Internal Audit Checklist

Board of Internal Audit and Management Accounting
The Institute of Chartered Accountants of India
(*Set up by an Act of Parliament*)
New Delhi

DISCLAIMER: The views expressed in this Guide are those of author(s). The Institute of Chartered Accountants of India may not necessarily subscribe to the views expressed by the author(s).

Foreword

The Internal Audit function has consistently evolved over time. Today, beyond the requirements specified by the Companies Act, 2013, the internal auditors are expected to ensure risk and governance aspects as well. Every organization adopts a unique approach to accepting certain levels of risk and applying measures to reduce these risks. The success of an organization is often closely linked to its proficiency in comprehending and managing its risk exposures. As a part of the company's risk control ecosystem, it is essential for the internal auditor to have the necessary skills to grasp the nature of risks and their corresponding controls.

I am happy to note that the Board of Internal Audit and Management Accounting of the Institute of Chartered Accountants of India(ICAI) has undertaken the project of revising its publication and issued 'Internal Audit Checklist (2024 Edition)' to provide step-wise guide to members to effectively conduct the Internal Audit Process. This checklist is illustrative in nature and is based on Risk Control Matrix. This checklist focuses on risk exposure and control effectiveness and data analytics for each process.

I congratulate CA. Rajendra Kumar P, Chairman, CA. Charanjot Singh Nanda, Vice Chairman and all other members of Board of Internal Audit and Management Accounting for bringing out this revised comprehensive publication.

I am sure that this publication will assist the members in discharging their responsibilities as internal auditors more effectively and efficiently.

February 1, 2024 **CA. Aniket S Talati**

New Delhi President, ICAI

Preface

The Board of Internal Audit and Management Accounting, ICAI has issued Internal Audit Checklist in 2017 to provide a step-by-step guidance to members on every aspect of internal audit. The Board has immense pleasure in placing before the members Revised "Internal Audit Checklist" that is drafted based on Risk Control Matrix for every aspect of Internal Audit. This checklist divides each process into sub processes and identifies risks for each process, controls to mitigate risks, sample size, test performed to check control effectiveness.

This Checklist has been divided into two parts: Part A and B. Part A contains Checklist Audit Planning, Entity Level Controls, Business Controls Diagnostic, Financial Statement Closure Process, Annual Operating Plan, Management Information system, Annual Operating Plan, IT Internal Controls, Standards on Internal Audit Compliances, Legal and Statutory Compliances, Operational and Administrative Expenses, Government Grants, Patents and Copyright, Business Continuity Plan, Related Party Transactions, Audit Conclusion. Part B contains checklist Order to Cash – Manufacturing and Services, Purchase to Pay – Material and Services, Capital Items, Fixed Assets and Capex, Project, Treasury and Inventory Management, Cash and Bank, Borrowings, Direct, Indirect Taxation and GST, Corporate Social Responsibility, Human Resources – Hire to Retire and Payroll Management, Foreign Currency Transactions. This Checklist is illustrative in nature and the internal audit team should review and update it based on systems and procedures of the Organizations. This checklist would help members to ensure the operating effectiveness of internal controls to mitigate key risks.

We are immensely grateful to all the members of study groups CA. K Vidyadharan, special invitee CA. A R Parthasarathy, CA, Aditya Kumar S, CA. Rekha Surana, CA. Narinder Jit Singh and CA. Amit Gupta, CA. Mohit Gupta, CA. Mohit Dhand, CA. Jitendra Prassad Indoriya, CA. Vineet Rathi, CA. Praveen Kaushik, CA. Chintan Pathak for sharing their experience and knowledge with us and contributing in preparation and review of this publication.

We would like to thank CA. Aniket Sunil Talati, President, ICAI and CA. Ranjeet Kumar Agarwal, Vice-President, ICAI for their continuous support and encouragement to the initiatives of the Board. We also thank the members of our Board who have always been a significant part of all our endeavors.

We also wish to express our sincere appreciation for CA. Arti Bansal, Secretary, Board of Internal Audit and Management Accounting, ICAI and team member CA. Gyanender Shokeen, Professional for their technical and administrative assistance in bringing out this Checklist.

We firmly believe that this publication would serve as a basic Guide for the members and other readers interested in the subject.

We will be glad to receive your valuable feedback at biama@icai.in. We also request you to visit our website https://internalaudit.icai.org and share your suggestions and inputs, on internal audit and Management Accounting.

CA. Rajendra Kumar P
Chairman
Board of Internal Audit &
Management Accounting

CA. Charanjot Singh Nanda
Vice-Chairman
Board of Internal Audit &
Management Accounting

January 22, 2024

New Delhi

Foreword to First Edition

The Chartered Accountancy profession, since its inception, is regarded as the trustee of public interest. In the last decade or so of financial turbulence, the role of Chartered Accountancy profession has become increasingly relevant and critical for sustenance of businesses. The CA profession has avowed duty to public interest and this can come through with increased impetus on ethics, trust and integrity in discharging professional assignments.

The Companies Act, 2013, has definitely shaped the way forward for internal audit function in India and has provided a strong legal mandate for the crucial role of internal auditors in the corporate governance structure.

Internal auditors should rise to the task and seize the opportunity of establishing high performing internal audit functions as per the new requirements. Internal auditors must be conscious that the current responsibilities come with new risks and new rewards. Continuous learning and timely application of relevant knowledge to create value will help in increasing the internal audit's credibility and confidence in their enhanced roles.

I am happy that the Internal Audit Standards Board is issuing this publication "Internal Audit Checklist" to provide updated guidance for helping internal auditors to stay at the cutting edge of best practices. This publication is quite comprehensive, providing a step-by-step guidance on every aspect of internal audit.

At this juncture, I wish to compliment CA. Mukesh Singh Kushwah, Chairman, CA. Anil S. Bhandari, Vice Chairman and other members of Internal Audit Standards Board, for their zeal towards bringing out comprehensive literature on internal audit.

I am sure that this publication would prove useful to the members in efficiently discharging their responsibilities as internal auditors.

February 7, 2017   **CA. M. Devaraja Reddy**

New Delhi   President, ICAI

Preface to First Edition

In today's dynamic environment organisations are constantly reinventing the way business is done, to meet the challenges of rapidly changing marketplace and regulatory framework. This makes it imperative for internal audit function to find innovative means to facilitate organizations to succeed and sustain their performance by imbibing/ integrating performance improvement in internal audit approach. The Companies Act, 2013, has also highlighted the important role of internal auditors in corporate governance framework.

The Institute is committed to continue its efforts in helping its members to understand, guide and shape the internal audit profession in the country. The Internal Audit Standards Board of ICAI has immense pleasure in placing before the members this publication on Internal Audit Checklist. It would serve as a simple step-wise guide intended to help internal auditors to effectively conduct the internal audit process. This checklist is illustrative in nature and the internal team should review and update it on the basis of systems and procedures of the organisations. It is divided into four main parts. Part I is Introduction, Part II deals with Internal Audit of Specific Function, Part III deals with Review and Reporting and Part IV covers Other Aspects. While each of the Parts is further divided into relevant sub topics, Part II contains, guidance on aspects such as Sales, Fixed Assets, Owner's Capital, Fixed Assets and Depreciation and Payables and Receivables, etc. This publication has therefore, a wider usage and appeal. This would also help to guide the members in maintaining proper internal audit documentation in accordance with SIA 3, *Documentation*.

At this juncture, I wish to place on record my sincere thanks to all the members of the Study Group formed under my convenorship at Delhi, *viz*., CA. Rakesh Garg (co-convener), CA. Anil Aggarwal, CA. Manoj Tayal, CA. Vidhya Jayaraman, CA. Vinod Gupta, CA. Prashant Chand, CA. Umesh Pandey, CA. Rajeev VD Gupta, CA. Vikas Agarwal, CA. Abhishek Jain, CA. Manoj Arora, CA. Rajiv Walia, CA. Manu Jindal, CA. Sandeep Goel, CA. Naveen Sharma for taking time out of their pressing preoccupations and contributing in preparation of this publication.

I would also like to thank CA. M. Devaraja Reddy, President, ICAI and CA. Nilesh Shivji Vikamsey, Vice President, ICAI for their continuous support and encouragement to the initiatives of the Board. I must also thank my colleagues from the Council at the Internal Audit Standards Board, *viz.,* CA. Anil Satyanarayan Bhandari, Vice-Chairman, IASB, CA. Tarun Jamnadas Ghia, CA. Mangesh Pandurang Kinare, CA. Dhinal Ashvinbhai Shah, CA. Babu Abraham Kallivayalil, CA. K. Sripriya, CA. M. P. Vijay Kumar, CA. Ranjeet Kumar Agarwal, CA. Sushil Kumar Goyal, CA. Debashis Mitra, CA. Shyam Lal Agarwal, CA. Kemisha Soni, CA. Sanjiv Kumar Chaudhary, CA. Sanjay Vasudeva, Shri Vithayathil Kurian and Shri Vijay Kumar Jhalani for their vision and support. I also wish to place on record my gratitude for the co-opted members on the Board *viz*., CA. Anil Kumar Jain, CA. Kartik Bharatkumar Radia, CA. Krishna Kumar T., CA. Vipin Gupta,

CA. Vishwanath K., CA. Yashwant Jaywant Kasar and special invitee *viz*., CA. Shobhit Dwivedi for their invaluable guidance as also their dedication and support to the various initiatives of the Board.

I am sure that the publication would be warmly received by the members and they would find it immensely useful in improving quality of their internal audit assignment.

New Delhi   **CA. Mukesh Singh Kushwah**
February 8, 2017   Chairman, Internal Audit Standards Board

MEMBERS OF THE COUNCIL [2022-25]

CA. Aniket Sunil Talati, President

CA. Ranjeet Kumar Agarwal, Vice President

CA. Rajkumar Satyanarayan Adukia

CA. Piyush Sohanrajji Chhajed

CA. Chandrashekhar Vasant Chitale

CA. Vishal Doshi

CA. Durgesh Kabra

CA. Dheeraj Kumar Khandelwal

CA. Purushottamlal Hukamichand Khandelwal

CA. Mangesh Pandurang Kinare

CA. Priti Paras Savla

CA. Umesh Sharma

CA. Dayaniwas Sharma

CA. Muppala Sridhar

CA. Prasanna Kumar D

CA. Rajendra Kumar P

CA. Cotha S Srinivas

CA. Sripriya K

CA. (Dr.) Debashis Mitra, Past President

CA. Sushil Kumar Goyal

CA. Rohit Ruwatia Agarwal

CA. Abhay Kumar Chhajed

CA. (Dr.) Anuj Goyal

CA. Gyan Chandra Misra

CA. Prakash Sharma

CA. (Ms.) Kemisha Soni

CA. Sanjay Kumar Agarwal

CA. Raj Chawla

CA. Hans Raj Chugh

CA. Pramod Jain

CA. Charanjot Singh Nanda

CA. Sanjeev Kumar Singhal

Shri Sanjay Kumar

Shri Ritvik Ranjanam Pandey

Shri Manoj Pandey

Shri Deepak Kapoor

Shri Rakesh Jain

Dr. P C Jain

Shri Vijay Kumar Jhalani, Advocate

Shri Chandra Wadhwa

MEMBERS OF THE BOARD OF INTERNAL AUDIT AND MANAGEMENT ACCOUNTING [2023-24]

Members from the Sitting Council

CA. Rajendra Kumar P, Chairman

CA. Prasanna Kumar D

CA. Charanjot Singh Nanda, Vice-Chairman

CA. Cotha S Srinivas

CA. Aniket Sunil Talati, President (Ex-officio)

CA. (Dr.) Debashis Mitra

CA. Ranjeet Kumar Agarwal, Vice-President (Ex-officio)

CA. Rohit Ruwatia

CA. (Dr.) Rajkumar Satyanarayan Adukia

CA. (Dr.) Anuj Goyal

CA. Chandrashekhar Vasant Chitale

CA. Prakash Sharma

CA. Vishal Doshi

CA. Sanjay Kumar Agarwal

CA. Durgesh Kumar Kabra

CA. Pramod Jain

CA. Priti Savla

CA. (Dr.) Sanjeev Kumar Singhal

CA. Piyush S Chhajed

Shri Deepak Kapoor

CA. Sridhar Muppala

Shri Chandra Wadhwa

Co-opted Members

CA. Mohit Bharti

CA. Sarda Satish Girdharlal

CA. Anil Kumar Jain

CA. Pankaj Soni

CA. Sharath Kumar D

CA. Nitin Hukumchand Agarwal

CA. Bhupal Sing Sulhyan

Special Invitee

Shri Avinash Sopan Jadhav

CA. Bisworanjan Sutar

CA. Krishnaswamy Vidyadaran

CA. Gavish Uberoi

CA. P K Manoj

CA. Pradeep Tyagi

CA. Savio Vincent Mendonca

CA. Tarun Kansal

CA. Sana Baqai

Contents

Introduction

The objective of this Internal Audit Checklist is to ensure that all relevant tasks and procedures are completed, and to ensure that the internal audit is done thoroughly and effectively. A checklist ensures that all necessary steps are taken and helps to identify the areas that may need improvement or further attention. Additionally, a checklist helps audit team to be organized and be focused and to ensure that all necessary information is collected and reviewed.

Scope

The Scope of checklists depends on both strategic and operational needs of the engagement. As part of the engagement, best efforts are done to identify areas where checklists are required.

About the Checklists

There are about 32 checklists which have been included in this publication can be customized as per requirements of the internal auditors. These checklists cover largely the common areas of an internal audit, however; the internal auditors may prepare additional checklists based on their engagement. The column against each of the line item in the checklist include:

- Process
- Sub-process
- Risk description
- Risk reference
- Controls
- Control reference
- Control owner
- Control frequency
- Design effectiveness
- Test perform
- attributes tested
- sample size
- work paper reference

- operating effectiveness

- exceptions

- data analytics performed

- results of data analytics and

- issue summary or observations.

- Process metrics

Need for Checklists

The Checklists is a tool which the professional can use to :

1. Help in giving direction to the team to cover specific areas of work with detailed action points;

2. Ensure completeness of the work by reviewing the critical points to be covered;

3. Documentation of the audit procedures carried out;

4. Consistency in the audit process especially in multi-team and multi-location assignments;

5. New team member need lesser amount of orientation since what needs to be done is covered;

6. The Internal Audit Checklist also covers Risk and Control Activities which would help the professional to fine tune the requirements based on the circumstance;

7. The Quality Reviewer of the engagement can also use the checklist to review the coverage, documents verified and other qualitative aspects of the engagement;

8. Helps the team to request for specific information from client based on the tasks to be done;

9. To document the granular levels of information on sample selection, data analytics.

Order of Checklists

Part A

1. Audit Planning Checklist

2. Entity Level Controls

3. Business Controls Diagnostic

4. Financial Statement Closure Process

5. Annual Operating Plan

6. Management Information system

7. IT Internal Controls

8. Standards on Internal Audit (SIAs) Compliances

9. Legal and Statutory Compliances

10. Operational and Administrative Expenses

11. Government Grants

12. Patents and Copyright

13. Business Continuity Plan

14. Related Party Transactions

15. Audit Conclusion

Part B

1. Order to Cash – Manufacturing

2. Order to Cash – Services

3. Purchase to Pay – Direct Material

4. Purchase to Pay – Indirect Material and Services

5. Purchase to Pay – Capital Items

6. Fixed Assets and Capex

7. Project Management

8. Inventory Management

9. Cash and Bank

10. Treasury Management

11. Borrowings

12. Direct and Indirect Taxation & GST

13.   Corporate Social Responsibility

14.   Human Resources – Hire to Retire

15.   Human Resources – Payroll Management

16.   Foreign Currency Transactions

PART A

Audit Planning

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
Overall Internal Audit Planning	Internal Audit Charter/ Terms of Internal Audit Engagement where it is an outsources engagement	Risk that internal audits are not in line with the objectives of the internal audit function, as per the internal audit charter of the entity (and terms of engagement, where it is an outsourced engagement) and also not in line with the overall objectives of the organisation.	A documented process, listing detailed process for preparing Annual audit plan keeping in view various facets of coverage required. It can be part of Audit Manual or a separate document.	1. Check the comprehensiveness of the Auditing plan, 2. Check the Adherence to the Annual Audit planning process as per document.	1. Whether documented process covers all the areas as listed in Audit Plan. 2. Step by Step adherence to the Annual audit planning process as per document.
	Developing / Enhancing Business Knowledge	Risk of leaving key elements of risk unattended due to lack of Business / regulatory environment knowledge.	Process of continuous engagement with stakeholders both inside and outside the organization.	Check the interactions Internal Audit has with inside and outside stakeholders and other research and documents as referred by the auditor.	Updation of overall business and regulatory knowledge.
	Audit Universe	Missing of Key Risk Area for coverage in Overall Internal Audit Plan	1. Having Audit Universe for Organisation / Auditable Entity. 2. Review of the Audit Universe at regular intervals.	1. Check the availability of Audit Universe for the Organisation/ Auditable Entity 2. How many areas added or deleted from Audit Universe. 3. See the risk rating of Various Audit Universe areas and any change in the risk ratings.	1. Audit Area Listing 2. Risk Rating of the Various Audit Areas 3. Updation of Audit Universe on regular basis
	Plan Linkages with	Lack of Audit Planning process linkage with Risk	Inputs from Enterprise Risk Management Team on key risk facing	Communication of inputs to and from Enterprise Risk	1. Usage of inputs in preparation of overall

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
	Enterprise Risk Assessment	faced by the Organisation	organisation and factoring the same in overall audit planning process	Management Team	audit plan
	Independent Risk Assessment for various Auditable units (i.e., locations, functions, business units and legal entities including third parties, wherever relevant).	Risk of not prioritising high risk area or missing them altogether.	1. Doing Independent Risk assessment of each auditable unit to arrive at correct risk attributable to each auditable unit. 2. Having adequate coverage in terms of scope/ frequency/ resource allocation to address the same.	1. Check Independent risk assessment along with methodology 2. See the coverage for scope/ frequency / resource allocation, etc.	1. Risk rating of each Auditable unit. 2. Scope/ Frequency and resources allocated to auditable unit.
	Resource and time allocation	Risk of inadequate resource allocation and available skill set	Allocation of resources and skill set depending upon criticality and complexity of the auditable unit along with proper time duration for the review	Assessment of resources and skill set allocation vis a vis criticality and complexity of the auditable unit. Sufficiency of the time duration to have adequate coverage of Auditable unit	1. Criticality and Complexity of Auditable unit 2. Skill set of resources allocated along with time duration for covering auditable unit
	Inputs for Audit plan for Executive Management	Risk of Audit Plan not in sink with Organisational realities/ Organisation objectives and strategies	1. Communication of Audit Planning process with executive management 2. Various meeting to capture inputs 3. Circulation of approved audit plan	1. Reviewing communication with executive management 2. Check various minutes of the meetings/ or other documents to capture inputs 3. Review approved and circulated audit plan	1. Audit Planning communication 2. Various inputs to the Audit Plan 3. Accuracy of communication of end result i.e. final audit plan
	Approval of Audit Plan with Audit	Risk of Audit Planning not aligned with those	1. Inputs from Audit Committee/ Board	Review of Audit Committee minutes to check inputs and	Inputs and approval of audit

8

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
	Committee / Board	charged with governance	2. Approval of Final Audit plan by Audit Committee	approval	committee
	Periodic review of Overall Internal Audit plan	Risk of derailment or non-alignment of Overall Internal Audit Plan	Review of the Overall audit plan on regular basis by Chief Audit Executive	Check the review performed by Chief Audit executive	Alignment of overall audit plan with stated objectives

Checklist 2

Entity Level Controls

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
Entity Level Controls	Ethics and Code of Conduct	Management does not demonstrate character, integrity and ethical values.	-The company has Codes of Conduct that provide guidance for ethical behavior for all officers, directors and employees, partners and consultants, as well as suppliers. The codes include guidelines to promote integrity, sound business practices, and legal compliance. -The codes are reviewed and modified on as needed. -Codes of Conduct are available on the company website. -Annually, all employees are asked to sign a Certification Form indicating that they have received, read, understood, and	Control evidence required: Signed Code of Conduct Declaration Define the criteria for evaluating compliance with the Code of Conduct. These criteria may include: Clarity and accessibility of the Code of Conduct. Effective-ness of communication channels used to disseminate the Code of Conduct. Employee awareness and understanding of the Code of Conduct. Reporting mechanisms for potential violations or	Documentation of Code of Conduct compliance/ undertaking	100%	Event Driven

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			agree to abide by the Code of Conduct -Annually, partners and consultants are required to provide acknowledgement that they have received and have been in compliance with the relevant policies The requirement to share the Code of Conduct with key and direct suppliers is documented in the Supplier Qualifications Procedures The Compliance team tracks the completion of employee training against the active employee headcount. The Compliance team also reviews the list of employees who have not completed the training and conducts timely follow-ups.	concerns. Actions taken in response to reported violations.			

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
Entity Level Controls	Corporate Governance Guidelines	The Constitutions of Board and other committee are not in line with the Companies Act/Regulator requirements	The Board and other committees under the Board are formed/ modified with the relevant statue requirements like Companies Act, IRDA requirements, RBI requirement etc. (As applicable to the relevant entity)	Control evidence required: Corporate Governance Guidelines

Ensure that there is a written Corporate Governance Guideline specifying details such as Board Independence, Committees, Qualification and expertise, executive compensation, board evaluation etc. Ensure that the board and other committees as required by the statutes are formed and the roles and responsibilities are clearly laid down. | Existence of Corporate Governance Guidelines | 100% | Yearly |
| **Entity Level Controls** | Board Oversight | Board does not clearly define authority to be exercised at Board level and authority | -Board powers are clearly defined. -Board powers are derived from | Control evidence required: Board composition, Corporate Governance | Appropriateness of Board oversight | 100% | Ongoing |

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
		delegated to other Directors.	Companies Act, Memorandum of Association (MoA) & Articles of Association (AoA.) -Also, for Directors appointed during the year, a Board Resolution has been passed to define general powers of a Director. -Board meeting has been held once every quarter and attendance records have been maintained.	Guidelines, Board Minutes, MoA & AoA of the Company Assess the effectiveness of the board of directors in providing oversight and governance to ensure that the organization's strategic objectives are met, risks are managed appropriately, and compliance with laws and regulations is maintained. -Review the Board Structure, Composition, meeting minutes, oversight (strategic, compliance, financial, risk) -Assess the effectiveness of board committees (e.g. Audit committee, Governance			

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				committee) in fulfilling their respective oversight responsibilities. -Verify that board members act independently -Compare the board's practices against industry best practices and corporate governance guidelines.			
Entity Level Controls	Board Oversight	Board does not have a mechanism to review Internal Control over Financial Reporting (ICFR)adequacy and performance.	Board of Directors review the performance of the company and adequacy of internal controls through regular interactions with the CFO. Monthly reporting is done by Senior Manager to the CFO who in turn reports to BOD. Minutes of Board Meetings where the Internal Audit reports are reviewed and adopted by the Board. There is	Control evidence required: Board Minutes, MIS for the month, ICFR. Ensure that there is a strong control environment that promotes ethical behavior and a commitment to internal controls. Ensure that minutes of meetings are reviewed and adopted by the Board.	Appropriateness of Board oversight	100%	Monthly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			an established process of monthly reporting on operations, performance and financial reporting. Monthly MIS prepared by the Senior Manager-Finance is reviewed by the CFO and Chairman & Managing Director.	Verify if monthly MIS is prepared and reviewed by the management.			
Entity Level Controls	Risk and Control Matrix	Financial Reporting and related application and information systems are not reliable.	On an annual basis, management performs a review of controls and processes including identification of risks and relevant financial statement assertions. The final version of the controls and process narratives and any changes made during the year are reviewed by the control/process owners to ensure they are accurate. The	Control evidence required: Risk and Control Matrix Check whether all significant risks related to each process or activity identified and included in the risk control matrix. Ensure that there is a clear and concise mapping of each risk to the corresponding control activities designed to	Verification of the Risk and Control Matrix and ensuring that the design and operating effectiveness of the controls are effective.	100%	Quarterly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			risk and control matrix, is maintained in the company's control management system.	mitigate or manage that risk. Verify that control procedures and protocols adequately documented for each control activity.			
Entity Level Controls	Risk Assessment Process	The Company does not carry out the risk assessment	On a quarterly basis, the Chief Risk Officer (CRO) reports to the Risk committee about the results of the risk assessment. The assessment includes Business risk, Solvency Position, Asset Liability Management, Industry position, etc.	Control evidence required: Quarterly Risk review presentation Ensure that the risk assessment process is well-defined and aligned with the organization's goals. Check whether relevant stakeholders, including management, department heads, and subject matter experts are involved in the risk assessment process.	Appropriateness of the Quarterly Risk review presentation.	100%	Quarterly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
Entity Level Controls	Whistle Blower Mechanism	The complaints received through Whistle blower policies are not enquired/ resolved.	The Management monitors/reviews the complaint received through whistle blower policy. The Ombudsman appointed enquire/ do a investigation of the complaints received and suitable action is taken if found guilty. On a quarterly basis, the report is provided to Managing Director & Company secretary and the same is reviewed and placed with Board.	Control evidence required: List of whistle blower Define the criteria for evaluating the effectiveness and efficiency of the whistle-blower mechanism, including: User access: The mechanism should be accessible to all relevant stakeholders. Anonymity: Whistle-blowers should be able to report without fear of identification. Confidentiality: The mechanism should safeguard the confidentiality of the reporter and the information provided. Acknowledgment and follow-up: The system	Adequacy of the whistle blower complaint process.	100%	Quarterly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				should acknowledge receipt of the report and allow for follow-up communication. Timeliness: Reports should be processed promptly. Resolution: The mechanism should facilitate appropriate investigations and resolution of reported issues.			
Entity Level Controls	Organizational Structure	Roles and Responsibilities not clearly defined	The company maintains an organizational structure with requisite positions supported by job descriptions that explain skill levels and responsibilities. Organizational chart is in place and maintained up to date to communicate lines of reporting. The company has set in place a succession plan	Check whether reporting lines are well-defined and clearly communicated throughout the organization and roles, responsibilities, and job descriptions are clearly outlined for each position within the organization. Review whether the succession plan for critical business	Existence of an approved Organizational Structure.	100%	Yearly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			(prepared by the HR Department) that identifies critical business operations and positions (designation with Managers & above level) and a back up plan is ensured to avoid impact on normal business operations.	operations and positions are clearly laid down and maintained.			
Entity Level Controls	Authorization Matrix	Roles, responsibilities, authorisation and approval levels not clearly defined.	Departmental policies and Management Guidelines outline responsibilities, authorization, and approval levels for transactions.	Role Definition: Verify that each role or position in the authority matrix has a clear and well-defined scope of responsibilities. Responsibility Assignment: Ensure that each task or activity in the organization is assigned to at least one responsible party in the authority matrix Accountabilities: Check that each task or activity has a	Existence of an approved Authorization Matrix	100%	Yearly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				single person or role designated as "Accountable" for its successful completion			
				Role Mapping: Validate that each individual's name or role listed in the authority matrix matches their actual position and responsibilities in the organization.			
				Approval Process: If there is an approval process defined in the authority matrix, verify that the steps and criteria for approval are clear and adhered to.			
				Delegation and Escalation: Assess whether the authority matrix includes provisions for delegation of responsibilities			

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				and escalation procedures for unresolved issues.			
Entity Level Controls	Segregation of Duties (SOD)	Duties and responsibilities are not appropriately assigned/segregated	Segregation of duties (SOD) controls are implemented throughout the sites where ERP has been implemented. SOD deficiencies are monitored, and management identifies compensating controls that are present and functioning to mitigate SOD risks.	Ensure that there is a well-documented policy and procedures manual regarding segregation of duties. Check whether there exists a mechanism to address conflicts identified during the transaction flow analysis. Check whether the SOD controls are reviewed and tested as part of internal and external audits.	Appropriateness of Segregation of Duties	100%	Yearly
Entity Level Controls	Strategic Plan	Strategic plans and objectives are not clearly defined.	Management periodically reviews entity-wide strategic plans and objectives. The Board of Director approves the entity-wide strategic plans	Control evidence required: Approved Strategic plans and objectives. Ensure that the strategic plan includes a clear	Existence of an approved Strategic Plan.	100%	Yearly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			and objectives.	and compelling vision statement that defines the organization's long-term aspirations and are aligned with the core values of the organisation.			
Entity Level Controls	Budget vs Actuals	The budget estimates are not prepared/set for the business teams. The Senior Management does not review the business operations on timely basis.	Management establishes business plans and budgets as well as measures results against plans quarterly. Analyses are independently reviewed for appropriate assumptions and methodology. Significant unusual relationships, variances, and exceptions are identified, investigated, and justified.	Control evidence required: Approved Budget and actuals. Ensure that the budget is accurate, reflecting realistic estimates of revenues and expenses and aligned with the organization's strategic objectives and operational plans. Check whether the assumptions and methodologies used in preparing the budget are	Appropriateness of Budget vs Actuals	100%	Yearly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				clearly documented and communicated. Verify whether the budget incorporates contingency plans to address unexpected events or changes in the business environment. Check whether unusual variances and exceptions are identified and justified.			
Entity Level Controls	Financial Reporting	Regulatory non-compliance and financial misstatements if suitable accounting principles, policies or rules not followed.	Management specifies financial reporting rules and standards which are consistent with accounting principles suitable and appropriate for the entity. Reviews by/consultations with the Statutory Auditors as required by the regulation (annual review)	Ensure that all employees and relevant stakeholders aware of the organization's policies and procedures Verify whether there is a process to monitor and assess compliance with policies regularly Check whether internal	Existence of Policies and Procedures (Including Financial Reporting Rules and Standards)	100%	As and when

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			or as considered necessary by the management, are done. Internal audit coverage extends to compliance review. Accounting policies and principles followed are stated in the 'Notes to accounts' in the financial statements. Circulars/email issued for closure of financial transactions are shared. Internal audit is done by professional firms and Internal Audit Reports identifies the issues observed. Annual review is done by Statutory Auditors.	controls in place to detect and prevent non-compliance with policies			
Entity Level Controls	Review of Related Party Transactions	Absence of an appropriate mechanism of related party transactions identification can lead to regulatory non-compliance and / or financial	Various compliances under different statutes in relation to transactions with a related party (transfer pricing related	Ensure that all related parties, including individuals, entities, and key management personnel, identified and	Appropriateness of disclosure of related party transactions	100%	As and when

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
		misstatements.	compliance and return filing) are verified. Audit Committee and Board approval are taken for related party transactions.	appropriately disclosed. Check whether related party transactions have been assessed for materiality and are material transactions adequately disclosed. Is audit committee approval and board approval obtained for related party transactions.			
Entity Level Controls	Internal Audit	A robust system of monitoring through periodic internal audits or control Self Assessments has not been established.	The Internal Audit function is led by and staffed with qualified, competent personnel with appropriate professional credentials and designations. For purposes of independence, Internal Audit reports functionally to the Audit Committee of BOD and administratively to the CFO, who approve the	Ensure that audit objectives aligned with the organization's goals and risks Verify whether scope of internal audit is adequately defined and documented Ensure that internal audit function is independent and free from undue influence or conflicts of interest Check whether	Appropriateness of Internal Audit	100%	Ongoing

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
			annual audit plan. Internal Audit completes an annual risk assessment and audit plan and provides periodic updates of its activities to executive management and the Audit Committee.	the auditor possesses the necessary skills, knowledge, and qualifications to perform their duties effectively			
Entity Level Controls	Information technology controls	Company infrastructure and IT systems being used for fraudulent activities thereby affecting the reputation and increasing the legal risks attached.	IT policies and practices are properly documented and communicated to achieve consistency across business units. Policies are communicated to users via the Company Intranet and policy updates are approved annually by management. Adequate measures are taken to protect sensitive information and data privacy.	Ensure that IT policies cover all relevant areas, such as information security, data privacy, IT governance, IT asset management, acceptable use, and disaster recovery. Verify if the IT policies in alignment with the organization's overall business objectives and risk appetite. Check whether the IT policies are in compliance	Existence of IT Policies and Procedures	100%	Quarterly

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				with relevant laws, regulations, and industry standards applicable to the organization's operations			
Entity Level Controls	Information & Communication-External Communication	In the absence of clear communicating channels for external parties, employee/ management malpractices may not come to light, may have a reputation risk with respect to third parties.	There are properly identified communication channels (email ids) for third parties under grievance mechanism.	Control evidence required: Dedicated email id created to register complaints; details available on company website. Ensure that email ids are created specifically for addressing third party grievance. Verify whether the email id is made available in the company website. Ensure that ethical considerations are prioritized in all external communication efforts.	Appropriateness of grievance mechanism for third parties	100%	As and when

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Control Frequency
				Verify whether key personnel are trained to handle crisis communication effectively;			
Entity Level Controls	Information & Communication-Management Oversight	Risk events, exceptional and unusual events remain unreported to the management and hence the risk management framework is not duly enhanced.	Formal communication process established for escalating disruption to operations, occurrence of risk events and any material exceptional event. Periodic MIS / Dash Boards, highlighting of all exceptions. Board meetings, management review discusses discuss unusual events. Monthly MIS prepared by the Senior Manager - Finance department is reviewed and approved by the CFO, Chairman & Managing Director.	Control evidence required: Procedure on Communication Protocol, MIS Ensure that a formal communication process is established for escalating disruption for operations. Verify whether there is an established communication protocol for different types of information (e.g., financial, operational, strategic). Ensure that the monthly MIS is reviewed and approved by the Senior management.	Existence of an approved MIS/Dashboard	100%	Monthly

Business Controls Diagnostic

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed
Business Controls	Respective sub-process	Risk of non-identifying 'what can go wrong' in each sub-process.	Whether the entity has prepared Risk Control matrix covering all risks (strategic, operational, financial, compliance, etc.,) and ensure that risk mitigation measures are operating effectively.	Business Head / Vertical or Segment Head.	Review of all the Risk Control Matrix and ensure its completeness and accuracy and critically evaluating the controls that is place and making effectively.
Business Controls	Controls	Risk of controls not being effective and efficient.	To review the control objectives critically and take steps to modify the control activity to make it more effective. with the approval of the appropriate authorities.	Each process-owner	Review all the controls critically and check whether it is sufficient to cover the risk envisaged.
Business Controls	Designing	Risk of ineffective designing or designing gap.	Process walkthrough of each sub-process and analyse whether there is any gap in internal control designing, then document the same.	Each process-owner	Walkthrough of all the processes and review design gap.
Business Controls	controls	Risk of ineffective controls not addressed.	There is tracker of all in effective controls and step has been taken to address it.	Internal Auditor	Follow up of all pending issues and corrective action
Business Controls	Policies and procedures	Risk of inconsistency in applying the policies and procedures.	There has to be a Standard Operating Procedure for all the sub-processes and the same needs to be	Each process-owner	To check whether all the steps given in the Standard Operating Procedure are followed.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed
			complied with.		
Business Controls	Standard operating procedure	Risk of Standard Operating Procedure being irrelevant and not in line with changed circumstances.	To ensure that Standard Operating Procedure is updated periodically	Each process-owner and Board of Directors	Periodicity of revision of standard operating procedure. Further, review the new risks and controls environment and check necessary changes are made to the SOP.
Business Controls	Ineffective controls	Risk of ineffective controls not being remediated.	All ineffective controls need to be reported to the management and a mitigation plan should be designed by the process owner and agreed upon with the internal auditors.	Process Owner	All the remediated Internal controls should be checked in the subsequent quarter to verify. operating effectiveness.
Business Controls	Manual controls	Risk of manual intervention at various control points.	Desirable to have more preventive and IT controls than manual interventions. To explore automation opportunities and check how the same can be implemented.	Process Owner	To review all manually tested or manually dependent controls to explore automation opportunities and provide a plan of action to the management.
Business Controls	Process Gaps	Risk of non-reporting of Gaps to the management by the process owners.	The internal auditor should have a comprehensive list of gaps in the processes and also suggest the mitigation plan.	Process Owner	All mitigation plans are to be approved by the Board of Directors for their compliance.
Business Controls	Action taken	Risk of non-compliances or gaps not being addressed to.	To ensure that the internal audit reports are discussed with Management for their action plan.	Process Owner	Review of the internal audit reports verify remedial action taken.

Financial Statement Closure Process

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size
Schedule of preparing financials	Closing Schedule	Risk of accounting remaining unclosed or not completed unless there is a formal process for formal closing of accounts at the month end/ Quarter end.	The Management should come out with a schedule of closing the books of accounts: illustrative list: a. All month end activity - by 7th of the next month; b. All Quarter end activities - by 10th of the next quarter beginning month. To also ensure that the closure of accounts period is aligned to regulatory requirements like SEBI LODR Requirements for listed companies or Group company norms.	Whether a proper communication is done by the Management say Director (Finance) or CFO Office to all the Finance and Accounts division or to service provider about the closure process.	Existence of communication	4 for monthly activities, 2 for Quarter activities, 1 for semi-annual and 100% for Annual activity.
Schedule of preparing financials	Closing Schedule	Risk of ledger balances not being updated and Risk of material misstatement of financial results.	1. Obtain reasonable assurance about whether the Financial Statements as a whole are free from material misstatement,	a. Whether there is list of reconciliations required to be prepared. b. Whether the reconciliations are reviewed (maker-checker	Correctness / Accuracy of the ledger balances.	4 for monthly activities, 2 for Quarter activities, 1 for semi-annual and 100% for Annual

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size
			whether due to fraud and error. 2. Preparation and Review of Reconciliation statements relating to (illustrative list is given as under): a. Bank Reconciliation Statement; b. Reconciliation GST. c. Reconciliation of inter-company transactions within the Group; d. Stock Reconciliation.	concept) with delegated authority. c. Whether there is an action plan for the items pending in the reconciliation and appropriate accounting treatment has been provided.		activity
Schedule of preparing financials	Closing Schedule	Risk of non-compliances with applicable financial reporting framework.	To ensure whether the Financial Statement is prepared and presented, keeping in mind all the material aspects, as per financial reporting frameworks as applicable. To do an assessment whether considering the requirement of relevant financial reporting frameworks:	Checking of disclosures and alignment to financial reporting framework.	Compliance with financial reporting framework	100%

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size
			That such Financial Statements appropriately disclose the important accounting policies that are selected and subsequently applied.			
			That the accounting policies which are selected and subsequently applied are in conformity with the relevant financial reporting framework.			
			That the accounting estimated which are made by management are rational.			
			That the information presented in financial statement is reliable, relevant, understandable, and comparable.			
			That the Financial Statement disclosure allows the users of the Financial			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size
			Statement to property understand the impact of material event and transaction on the information that is conveyed in Financial Statements.			
Schedule of preparing financials	Closing Schedule	Risk of non-compliances with regulatory requirements on specific disclosures.	The checklist can be used to conduct self-audits and identify areas where they are not compliant with regulations. The checklist can be updated periodically to reflect changes in laws and regulations.	Checking of disclosures and alignment to regulatory requirements like SEBI LODR.	Compliance with regulatory requirements	100%
Review of the financial Results	Material Transaction	Risk of a material transaction not being reported or reported incorrectly.	Review by CFO of the financial performance and position including cash flows and noting down significant issues and taking corrective action.	Review of the CFO notes and action being taken to take corrective action.	Completeness and accuracy of the financial results.	100%
Review of the financial Results	Variance Analysis	Risk of a material transaction not being reported or reported incorrectly.	Review of the Variance Analysis (on Quarterly / Monthly / Annually basis / Budget Vs.	Review of the CFO notes and action being taken to take corrective action.	Completeness and accuracy of the financial results.	100%

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size
			Actual) to enable to understand major transactions.			
Approval for publishing the results	Approval process	Approval of the financial results without being reviewed by management.	The Financial statement may be reviewed at various levels by CFO/Director, Statutory Auditor, CEO/ MD, Audit Committee and Board of Directors.	Whether the reviews have been done with respective authorities and the discussions are recorded in minutes.	Ensuring review is comprehensive and approved before the results are declared.	100%
Compliance with guidelines on Unpublished Price Sensitive Information (UPSI).	Protecting the financial information which is classified as price sensitive.	Risk of non-compliance with SEBI Regulations on UPSI and Prevention of Insider Trading Regulations (PIT).	a. All staff to be sensitised on UPSI and PIT Regulations and obtain confirmation from them in writing that no price sensitive information will be disclosed to anybody, and if done they are personally liable. b. Ensuring that price sensitive information is handled by senior executives and documented in a structured manner. c. Not permitting electronic or hard copies of the information to be	Whether steps have been taken to protect UPSI and PIT regulations.	Ensuring compliance with UPSI and PIT Regulations.	100%

35

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size
			circulated or transmitted unless. approved by appropriate authority.			

Annual Operating Plan

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
Annual Operating Plan	Collection of Data for preparation Annual Operating Plan	Risk of inaccurate data considered or incomplete data taken into account for preparation of annual operating plan. Risk of non-consideration of economic factors / current and future market conditions while considering the requirements in the annual operating plan.	Business objectives for the organisation are clearly defined while considering the data to be requested for preparation of annual operating plan. Correctness of various factors considered are verified and any modifications to be made to the plan are verified and approved. Realistic expectations are set for the organisation to achieve its objectives. Inputs are requested in a pre-defined format, for preparation of annual operating plan for every financial year.	Check whether the data considered for preparation of annual operating plan is adequate and accurate. Check whether the factors in the operating environment in which the entity operates have been considered and current and future market conditions have also been taken into consideration while preparing annual operating plan.	1. Annual Operating Plan Template. 2. Projected Annual Revenue Plan. 3. Projected monthly expenditure budget. 4. Annual Manpower Cost. 5. Projected Interest Cost.
	Preparation of Annual Operating Plan	Risk of inaccurate preparation of annual operating plan i.e. preparation done	Summarise the annual operating plan prepared to the teams and leaders in the	Check whether opinions and inputs of every department heads have been taken into account	1. Draft Annual Operating Plan.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
		based on collection of inadequate or inaccurate information. Risk of not considering the basic and main objectives of the organisation in preparation of annual operating plan. Risk of setting unrealistic goals and expectations while preparing annual operating plan which lead to not meeting those expectations. Risk of not taking into account the expertise of department heads in the preparation of annual operating plan.	organisation to ensure everyone is on track. While outlining the annual operating plan preparation process, take special note of potential roadblocks that might hinder the process. Consider the time constraints that might affect the annual operating plan process. Communicate the information acquired to the respective department heads for preparation of annual operating plan.	while preparation of annual operating plan. Check whether annual operating plan is prepared and communicated to every department for achievement of objectives.	
	Review of Annual Operating Plan	Risk of not reviewing the basis and validity of assumptions made in preparation of annual operating plan. Risk of not reviewing the data considered in the preparation of annual operating	Unified collaboration with stakeholders is a key step in the preparation of annual operating plan process and stakeholders should review the annual operating plan prepared. Strategic plans	Check whether annual operating plan prepared is reviewed by the key stakeholders in the organisation. Check whether basis and validity of the data is reviewed while preparation of annual operating plan.	1. Reviewed Annual Operating Plan. 2. Minutes of the meeting in which the Annual Operating Plan is reviewed periodically.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
		plan. Risk of not reviewing whether objectives of the organization as a whole have been considered in preparation of annual operating plan.	should align with annual operating plan without being redundant. Set up parameters to track and measure and review the achievement of objectives of organisation as per the annual operating plan prepared.	Check whether assumptions made in preparation of annual operating plan is adequate to functioning of the organisation.	
	Approval of Annual Operating Plan	Risk of annual operating plan being not approved or presented before audit committee or board of directors. Risk of not completing the preparation of annual operating plan before beginning of next financial year including approval of the same. Risk of non-approval of annual operating plans lead to lack of awareness among the audit committee members or board of directors about the plan being	The Chief Financial Officer (CFO) and the Chief Executive Officer (CEO) reviews and presents the Draft Annual Operating Plan for approval to the Audit Committee and Board of Directors, who reviews the major assumptions considered in the preparation of annual operating plan. Based on Draft Annual Operating Plan being prepared the Audit Committee or Board of Directors suggest revisions or changes, if any, for achievement of	Check whether the annual operating plan is reviewed and vetted before the Audit Committee and Bboard of Directors for consideration. Check whether any revisions or changes suggested by the Audit Committee or Board of Directors have been made. Check whether the annual operating plan for the financial year after all necessary changes as communicated have been duly reviewed and approved. Check whether the final approved annual operating	1. Final Approved Annual Operating Plan. 2. Minutes of Audit Committee where annual operating plan have been presented for approval. 3. Minutes of the meeting with the Board of Directors where approval of annual operating

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
		prepared and achievement of objectives. Risk of unapproved or unauthorised annual operating plan lead to material omissions in the plan being prepared or leading to unplanned expenditures during the year and financial strains. Risk of department head not aware of the approved annual operating plan	objectives of the organisation. Audit committee and Board of Directors approve the Final Annual Operating Plan though a board resolution. The approved annual operating plan shall be communicated to the department heads.	plan is in line with the overall objectives of the organisation.	plan have been made. 4. Changes communicated by the Board of Directors to be made to the annual operating plan.
	Monitoring and Review of Annual Operating Plan	Risk of not monitoring the annual operating plan periodically, lead to non-achievement of objectives stated in the annual operating plan. Risk of not preparing variance analysis with the objectives set out in the annual operating plan and what have been achieved. Risk of not addressing the unanticipated	On a monthly basis as part of Monthly Information System (MIS), the Annual Operating Plan should be reviewed and monitored for the objectives which are achieved and which are yet to be achieved. Annual Operating Plan should be periodically reviewed to factor in unanticipated occurrence of events in the organisation that lead financial	Check whether annual operating plan prepared is being periodically monitored and reviewed by the management. Check whether variance analysis is prepared for monitoring deviations and analysing the same in the annual operating plan prepared. Check whether unanticipated events in the business during the period is	1. Final Approved Annual Operating Plan. 2. Variance Analysis prepared. 3. Deviations identified from the Annual Operating Plan during the period and implementation of corrective actions.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
		expenditure occurring during the year which are not part of annual operating plan may lead to adverse effects on the organisation. Risk of not monitoring the annual operating plan periodically may lead to operational difficulties.	strains in the organisation and act as hindrance to achievement of objectives set out in the initial annual operating plan. The CFO and CEO monitor and review the annual operating plan and presents the same to the Audit Committee and Board of Directors for their review and advice. Variance analysis should be prepared for deviations from the annual operating plan and should be addressed for effective achievement of objectives.	factored in the annual operating plan prepared and necessary approvals have been received for the same. Check whether annual operating plan is being reviewed and presented to board of director for review and their advice. Check whether corrective action is taken for variances identified.	

Management Information System

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested
Management Information System	System Governance and Strategy	Absence of formally laid down policy for MIS.	There is a well-defined MIS governance framework with clear roles and responsibilities The organization has an MIS strategy aligned with its business goals and objectives. Policies and procedures for managing the MIS lifecycle is clearly documented.	Check whether: i) There is a well-defined MIS governance framework with clear roles and response-bilities. ii) The MIS strategy is aligned with its business goals and objectives. iii) Policies and procedures for managing the MIS lifecycle is documented.	Existence of a well - defined MIS
Management Information System	MIS Design and Development	MIS does not meet the organization's requirement	The MIS system is designed to meet the organization's reporting and analysis requirements and user's requirements, and it is well-documented (including the data flows and processing logic).	Ensure that: i) The MIS system is designed to meet the organization's reporting and analysis requirements. ii) User requirements are-documented, and was there user involvement during the designing phase. iii) The data flows and processing logic is clearly	Appropriateness of the MIS

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested
				defined and documented. iv) Adequate controls are embedded in the system design to prevent errors and fraud.	
Management Information System	Reporting and Analysis	Inaccurate/Untimely MIS Reporting	Templates and Timelines for MIS Reporting are standardized. MIS reports cover the overall organization and each function.	Check whether: i) The required reports are generated accurately and on time. ii) Reporting templates are standardized and consistent across the organization. iii) There is a process for validating report results against source data. iv) The MIS covers the overall business and each business function.	Accuracy of the MIS
Management Information System	User Training and Support	Effective use of MIS	Training are provided to users on using the MIS system. The details of the helpdesk or support channel are available for addressing user's issues and is also communicated to	Check whether the users are provided with training on using the MIS system effectively and there is a helpdesk or support channel available for	Effectiveness of the MIS

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested
			users.	addressing user's issues.	
Management Information System	Compliance	MIS System is not align with to the relevant laws and audit trail of user's activities is not tracked.	There is an up-to-date documentation of all applicable laws, regulations, and standards applicable and clear documentation of how the MIS aligns with each requirement and control. Regular training is provided to employees about the importance of compliance and data protection. Logging and tracking user actions, periodic audit trail reviews and restricted access to audit logs are also ensured.	Verify whether: i) The MIS system align with relevant laws, regulations, and industry standards. ii) Audit trails are maintained to track user activities and system changes. iii) Security assessments or vulnerability tests are conducted regularly.	Appropriateness of the MIS

IT Internal Controls

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
Governance, Management & Technical Controls	Policies, Standards and Procedures	Absence of IT controls at the Governance level would lead to loss of effective information management and security principles, policies, and processes deployment in the organisation.	Do corporate policies and standards that describe the need for IT controls exist	1. Identify the IT control environment of the organization, Whether Policy, Standards and Procedures existing the Organisation. 2. Check for IT Security Policy document including Values, Philosophy, Management style, IT awareness, Organisation, Policies, Standards. 3. Check for evidence of performance and compliance metrics that demonstrate ongoing support for IT Security framework.			
Governance, Management & Technical	Policies, Standards and Procedures	The Board of Directors have the primary responsibility	Determine whether the Board of Directors have reviewed and	1. Examine how Governance controls, IT Policies and			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
Controls		as keepers of the Governance Framework of which IT Controls are a part.	approved IT policies	Standards are mandated in the organisation - either by the entire Board of Directors or a Board committee in conjunction with the organization's executive management.			
Governance, Management & Technical Controls	IT Security Management	Information Security Management System needs to be top driven, there needs to be adequate Leadership and Top Management support	Does the organisation have Information Security Management System (ISMS)	Establish the existence of the ISMS document availability within the organisation and review it in detail			
Governance, Management & Technical Controls	IT Security Management	Lack of alignment between ISMS and Organisation Goals & Objectives will lead to non-fulfilment of business needs in an effective manner	IS Policy established in line with Org obj, int with Org processes, resources, supporting, comms, CI, etc)	Alignment between ISMS and Organisational goals and objectives need to be checked with respect to: 1. Internal business objectives and requirements: 2. Requirements specified in contracts and			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				service level agreements (SLAs) of the Company 3. Compliance requirements defined in legislation and regulations.			
Governance, Management & Technical Controls	Regulations & Compliance	Compliance to legislation of the country where the organisation is situated is a mandatory requirement that cannot be compromised	What legislation exists that impacts on the need for IT controls and has the Management taken steps to ensure compliance with this legislation?	1. Check for compliance with industry specific laws and regulations and compliance with Digital Personal Data Protection Act, 2023 or General Data Protection Regulation (GDPR) that require protection of personal data that detail specific information security requirements2. Check for telecommunications regulations that specify regulations to be complied with. 3. Examine laws that relate to relate to the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				admissibility of electronic evidence that organisations should be aware of regarding the collection of evidence during a security incident.			
Governance, Management & Technical Controls	Technical Controls	Absence of standards and methodology adoption for Software Life Cycle Management will affect reliability and integrity of information assets	Examine how IT management has defined standards and adopted a methodology governing the process of developing, acquiring, implementing, and maintaining information systems and related technology.	Examine the overarching set of standards & methodology the organisation adopts for Software Project Management and Software development. Examples include Prince2, traditional Waterfall methods, Agile methodology, Rapid Application Development, etc. Compliance with ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection (Refer Rule 8: Reasonable Security Practices			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				and Procedures).			
Governance, Management & Technical Controls	Technical Controls	Absence of standards, methodologies and procedures for Software Life Cycle Management will affect reliability and integrity of information assets	Determine if IT management has adequate standards and procedures for: Systems development Program change control Data Centre operations Data Base administration Direct Access Storage Devices (DASD)management (Disk Subsystem) Performance monitoring Capacity planning Network administration Information security Contingency planning/disaster recovery	The standards and procedures should cover all aspects of IT, viz., Organisation & Management, Physical & Environment Control, System Software & Infrastructure Controls, System Development Controls and Application-based controls			
HR Roles & Responsibilities	Segregation of Duties	Lack of oversight or the lack of segregation of duties rules within an organisation will increase the risk of fraud, as in the case when a single person	1. Check whether all the relevant responsibilities for IT controls been allocated to individual. 2. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or	1. Is the allocation of responsibilities compatible with the need to apply division of duties? 2. Are IT responsibilities documented? 3. Are IT control responsibilities communicated to the whole			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		performs every financial function.	unintentional modification or misuse of the organization's assets.	organization? 4. Do individual role holders clearly understand their responsibilities in relation to IT controls? 5. Does internal auditing employ sufficient IT audit specialists to address the IT control issues?			
HR Roles & Responsibilities	Information security roles and responsibilities	Inadequate mapping of roles with the organisational structure creates overlapping and confusing execution of activities	All information security responsibilities shall be defined and allocated.	- Each function or department being assessed should be checked for availability of a well-defined Org Structure and Roles & Responsibilities definition. - Special checks should be performed to see whether there is any duplication of work pointing to improper segregation of duties, especially in Quality Assurance, Procurement, Finance, Supply Chain, etc.,			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				functions.			
Mobile & Teleworking	Mobile Device Policy	Absence of a mobile device security policy can lead to security incidents and other potential costly problems that may lead to data breaches if employees aren't aware of the risks when using technologies improperly.	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. Bring Your Own Device (BYOD) policy may be laid down to given employees to use personal devices for work related activities.	There is a need to check the following: 1. Acceptable use policy for mobile devices; 2. BYOD, CYOD (choose your own device), etc policies and restrictions of use. 3. Mobile security policy related to user registrations, regular updates, etc.			
Mobile & Teleworking	Teleworking	Several risks associated with Teleworking / Remote working include: Accessing Sensitive Data Through Unsafe Wi-Fi Networks, Using Personal Devices for Work, Ignoring Basic Physical Security Practices in Public Places, Email Scams,	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Check the policy and implementation thereof. -If any discrepancies and report thereto.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		Cyberattacks on Remote-working Infrastructure, etc. A robust policy addressing these risks would lead to safe working operations for all types of employees.					
Access Control	Policies and Procedures	Poor access control can expose the organization to unauthorized access of data and programs, fraud, or the shutdown of computer services.	Access control policy - An access control policy shall be established, documented and reviewed based on business and information security requirements. Access to networks and network services - Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	1. Verify that Access Control policy limits access to information systems and network systems to authorised personnel only 2. Verify that IT and facility personnel are aware of the applicable policies.			
Access Control	User Access Management	Risk of information being accessed without the	1. User registration and de-registration - A formal user registration and de-	- Ensure that terminated users are promptly removed. Obtain a current user			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		appropriate authorisation, unlawfully and the risk of a data breach.	registration process shall be implemented to enable assignment of access rights. 2. User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. 3. Management of privileged access rights - The allocation and use of privileged access rights shall be restricted and controlled. 4. Review of user access rights - Asset owners shall review users' access rights at regular intervals. 5. Removal or adjustment of access rights - The access rights of all employees and external party users to information and information processing facilities	account list for all systems and cross reference it with current payroll or human resource data. Any users not found in the payroll or human resource files. -Check User profiles are defined in system.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.				
Access Control	User Responsibilities	Poor management or improper allocation of authentication information may result in unauthorised access to information systems and in loss of confidentiality.	Use of secret authentication information - Users shall be required to follow the organization's practices in the use of secret authentication information.	Secret authentication information is a gateway to access valuable assets. It typically includes passwords, encryption keys etc. so needs to be controlled through a formal management process and needs to be kept confidential to the user. This is usually tied into employment contracts and disciplinary processes. Verify : 1. Documentation of Management process, 2. Maintenance of confidentiality 3. Disciplinary processes			
Access Control	System and Application Access	lack of System and Application	1. Information access restriction - Access to	1. Determine the application and system level Login			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
	Control	Access Controls can result in risks like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, information extortion and many others.	information and application system functions shall be restricted in accordance with the access control policy. 2. Secure log-on procedures - Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. 3. Use of privileged utility programs - The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. 4. Access control to program source code - Access to program source code shall be restricted.	procedures. 2. Determine the user data and roles assigned for admin and privileged access and how the user id/passwords for these types of access are maintained and kept confidential. 3. Examine how granular are application and transaction level controls and how they are implemented and whether the process is reliable.			
Physical Security	Physical Security	Physical security represented by the security of personnel,	1. Physical security perimeter - Security perimeters shall be defined and used to protect areas that	Are the following access procedures in place: - Appropriate			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		hardware, programs networks, and data, if not protected can result in severe losses or harm to an enterprise, agency, or organization in terms of: 1. Tailgating 2. Theft of documents 3: Unaccounted visitors 4: Stolen identification 5: Social engineering There is a need to Measure, mitigate and monitor this risk. Physical security components connected to the Internet, such as RFID key card door locks, smartphones, and video surveillance cameras, are	contain either sensitive or critical information and information processing facilities. 2. Physical entry controls - Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. 3. Securing offices, rooms and facilities - Physical security for offices, rooms and facilities shall be designed and applied. 4. Protecting against external and environmental threats - Physical protection against natural disasters, malicious attack or accidents shall be designed and applied. 5. Working in secure areas - Procedures for working in secure areas shall be designed and applied. 6. Delivery and loading areas -	granting and discontinuance of authorizations? - Control over passkeys, keys? - Do post-emergency re-entry procedures exist? - Do controls over entry by time of day exist? - Are there specific exclusions to policy? - Observe and inquire about the physical security of the Computer Systems room. - Are alarm events logged and routinely reconciled to actual events? - List any network monitoring packages used along with the manufacturer and version. Obtain a list of the authorized users. Determine that any unauthorized network monitoring software is strictly			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		common targets for hackers and need to be protected	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	prohibited and that access to authorized software is approved by IT management. - Determine whether adequate segregation of duties exists between those responsible for the day-to-day network operations and those responsible for the network monitoring software and access controls. - Assure that access authorization procedures are used for all persons (employees, contract workers, security staff and visitors) requiring access to sensitive areas. (Are photo ID cards or electronic key cards required for entry?) - Analyze the potential threat posed by fires in			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				adjacent buildings and areas. - Are alarms installed at all potential entry and exit points of sensitive areas? - Determine that the physical components of the network are properly secured. This includes wiring closets, demarcation blocks, patch panels, cabling, terminals and LAN stations, as well as the communications processors. - Review access point control. Are entry/exit logs maintained? Does electronic and/or video surveillance equipment exist? - Is the LAN file server housing locked or otherwise secured to prevent removal of boards, chips, and the computer system? - Determine if the plant utilizes a			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				"Certificate of Understanding" for all employees with access to Personal Computers as required by Policy. This document should be distributed by the LAN Administrators at the plant to all personnel.			
Physical & Environment Security	Equipment Security	Lack of controls for equipment security can lead to several risks associated with equipment malfunction, breach of contractual relations, industrial espionage, interruption of business processes and other threats that can damage an organisation's ability to perform and function.	1. Equipment siting and protection - Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. 2. Supporting utilities - Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. 3. Cabling security - Power and telecommunications cabling carrying data or supporting information services	1. Clear desk and clear screen policy - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. 2. Review placement of water and drainage pipes to ensure they are routed away from operations areas. Assess the potential for storage tanks to flood electronic equipment and the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			shall be protected from interception, interference or damage. 4. Equipment maintenance - Equipment shall be correctly maintained to ensure its continued availability and integrity. 5. Security of equipment and assets off-premises - Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises. 6. Unattended user equipment - Users shall ensure that unattended equipment has appropriate protection. 7. Clear desk and clear screen policy - A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities	susceptibility to external flooding. 3. Review smoke detection and automatic fire extinguishing equipment to ensure that it is functional and that it provides adequate protection. (i.e. ensure that fire extinguishing equipment is not a sprinkler placed over each server.) 4. 6. Is there scheduled preventative maintenance on the components, either by the LAN administrator or by the vendor under a maintenance contract? Do these procedures meet the manufacturer's recommendations ? 7. If a maintenance contract exists for routine cleaning, verify that the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			shall be adopted.	vendor has honoured the contract.			
Operations security	Operational procedures and responsibilities	Standard operating procedures provide the policies, processes and standards needed for the organization to succeed. They can benefit a business by reducing errors, increasing efficiencies and profitability, creating a safe work environment and producing guidelines for how to resolve issues and overcome obstacles. Lack of SOPs would lead to inconsistency in operations of each of the above areas	1. Documented operating procedures - Operating procedures shall be documented and made available to all users who need them. 2. Change management - Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled. 3. Capacity management - The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance. 4. Separation of development, testing and operational	Verify that Standard Operating Procedures exist for each of the functions and production, non-production departments and that people are aware of the documents and process steps. Also verify that the SOPs are maintained under strict document and version control and that latest versions, duly authenticated are available for use.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			environments - Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.				
Operations security	Protection from malware	Malware viruses piggyback on existing programs and can only be activated when a user opens the program. These viruses can corrupt or delete data, use the user's email to spread, or erase everything on a hard disk. Some of the risks associated with malwares can be one of the following: 1. Viruses and worms. are malicious	Controls against malware - Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. Controls against Virus Protection 1. Determine the level of virus protection established on servers and workstations 2. The monitoring of infection being done by IS administration. 3. Virus Application should be updated on a monthly basis.	1. Check whether the organisation regularly conducts 3rd Party Vulnerability Assessment and Penetration Testing (VAPT) and takes remedial actions on the VAPT test report recommendations for reducing external threats 2. Check also how the system software and application software versions are kept updated 3. Check how 3rd Party Application Development or outsourced application			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		software programs (malware) aimed at destroying an organization's systems, data and network 2. Botnets 3. Drive-by download attacks 4. Phishing attacks. ... 5. Distributed denial-of-service (DDoS) attacks 6. Ransomware 7. Exploit kits 8. Advanced persistent threat attacks		development work are checked for Security vulnerabilities before these are deployed in the production environments 4. Check the methods of Virus Protection software installation, tracking and resolution adopted in the organisation.			
Operations security	Backup/Recovery	Risk of major disruption of business operations in case of business will not be able to recover the data.	1. Whether the organisation has adequately documented backup and recovery procedures/plans/schedules for critical sites. 2. If procedures exists, backup copies of information, software and system images shall be	1. Verify: LAN is supported by an uninterruptible power supply (UPS). 2. Verify: Has the UPS been tested in the last year (to test the batteries)? 3. Verify: Has the UPS been tested in the last year (to test the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			taken and tested regularly in accordance with an agreed backup policy	batteries)? 4. For disaster-recovery purposes, have LAN applications been prioritized and scheduled for recovery based on importance to the operation? Also determine if the recovery sequence is proper so that key applications can be restored. 5. Are LAN files backed up at appropriate intervals to ensure the need to re-enter data is minimized? 6. To ensure that the backups are good and can be used to recover the system have the System Administrator: Restore a file or files from the backup media. (Restore a file to a different location and then check the file) 7. Verify:			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				a) Backup tapes are properly labelled and organized. b) Backup tapes are stored securely in a fireproof safe and not left in the open. c) Backup tapes are secured off-site. 8. Obtain a copy of the insurance policy that applies to the LAN facility. With the assistance of computer insurance specialists, determine the adequacy of the LAN facility insurance coverage.			
Operations security	Logging and monitoring	Centralised Automated Event logging allows an organization to track and understand all the processes that occur within a network of IT	1. Event logging - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. 2. Protection of log information -	1. Verify the Security Event Log Monitoring process followed in the organisation. 2. Conduct an electronic audit of the logs for indications that unauthorized			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		servers and systems deployed. The log of information ensures that valuable information is preserved to avoid the efforts of cybercriminals and potential deletions due to a lack of storage space. Security incidents related to external or internal threats could be mitigated with proper log collection and monitoring.	Logging facilities and log information shall be protected against tampering and unauthorized access. 3. Administrator and operator logs - System administrator and system operator activities shall be logged, and the logs protected and regularly reviewed. 4. Clock synchronisation - The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	security-related activities have been attempted or performed on a system or application that processes, transmits or stores confidential information. 3. Verify the security incidents on a sample basis, if any, and check of documented root cause analysis and Corrective and Preventive actions taken to mitigate future risks 4. Check the process of Clock Synchronisation through the organisation's information systems.			
Operations security	Control of operational software	Automation of system and operational software is necessary as outdated software might not be able to withstand an	Procedures shall be implemented to control the installation of software on operational systems.	1. Check for availability of Software Deployment tools in the organisation and the associated Group Policy for software deployment.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		up-to-date cyber-attack. Systems will become more vulnerable to ransomware attacks, malware and data breaches if automated procedures for software installation on operational systems are not implemented		Examples include Microsoft SCCM, AWS Code Deploy, Google Cloud Deployment Manager, or any other remote deployment tools. 2. Validate the updates on the software tool and check whether latest versions are being used.			
Operation Security	Technical vulnerability management	Risk of fraudulent activities and external threats(Malware, SQL Injection, Denial of Service, etc) to the organisation .	1. Management of technical vulnerabilities - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. 2. Restrictions on software installation - Rules governing	1. Check whether the organisation regularly conducts 3rd Party Vulnerability Assessment and Penetration Testing (VAPT) and takes remedial actions on the VAPT test report recommendations for reducing external threats. 2. Check whether the organisation restricts software installation through policies and use of tools			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			the installation of software by users shall be established and implemented.	like VMware Airwatch, or any other similar tool that allows IT to automate, control, and secure administrative policies on laptops, tablets, or any other device connected to the organization's network.			
Operation Security	Information systems audit considerations	Risks of poorly designed business processes, IT security risk, integrity and ethical risk, human errors and fraud risk.	Information systems audit controls - Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	1. Check for availability of formal Internal Audit Schedules within the organisation. 2. Check validity of the scope of Internal Audit - whether the organisation periodically conducts ITGC and/or ISO 27001 audits 3. Review Strengths, Opportunities for Improvements (OFIs) and non-conformities and whether appropriate actions have been initiated from the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				last audit.			
Communication security	Network security management	Risks of widespread cyberattacks and degrade network performance due to inability of restricting the number of users in specific zones.	1. Network controls - Networks shall be managed and controlled to protect information in systems and applications. 2. Security of network services - Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. 3. Segregation in networks - Groups of information services, users and information systems shall be segregated on networks.	1. Check whether the IT department of the organisation has implemented preventive measures like Network Segmentation & Network Zoning based on Zero Trust Architecture (ZTA). 2. Check the policy and deployment of Firewalls, whether the organisation makes use of latest Firewall technologies (For example, from Palo Alto Networks, etc.). 3. Check whether the company has made Documentation and Network Diagrams for all segments and locations making maintenance and traceability of malfunctioning devices easier. 4. Check whether the organisation			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				has provided for redundancy in the network to avoid single point of failures. For example, use of Multi-Protocol Label Switching (MPLS) and Internet Lease Lines (ILL) to provide redundancy to the Fibre based WAN services, etc.			
Communication security	Information transfer	Risks involved in relation to the confidentiality, integrity and availability of the information and this will need to take into account the type, nature, amount and sensitivity or classification of the information being transferred.	1. Information transfer policies and procedures - Formal transfer policies, procedures and controls shall be in place to protect the transfer of information using all types of communication facilities. 2. Agreements on information transfer - Agreements shall address the secure transfer of business information between the organization and external parties. 3. Electronic messaging - Information involved	Check for availability of Policies on: a) Information transfer policies and procedures. b) Information & data flows and the classification system used. c) Agreement on information transfer addressing the secure transfer of business information between the organisation and external parties. d) Electronic messaging and protection of			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			in electronic messaging shall be appropriately protected. 4. Confidentiality or nondisclosure agreements - Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	messages. e) Confidentiality or non-disclosure agreements.			
Vendor Management	Information security in supplier relationships	Risk from suppliers and vendors. Absence of an adequate Supplier Policy may lead to financial, environmental, operational, and legal risks.	1. Information security policy for supplier relationships - Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented. 2. Addressing security within supplier agreements - All relevant information security requirements shall	1. Whether vendor reliability is considered before purchasing LAN hardware and software. 2. Whether a service log is maintained to document vendor support servicing. 3. Whether a service log is maintained to document vendor support servicing.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. 3. Information and communication technology supply chain - Agreements with suppliers shall include require-ments to address the information security risks associated with information and communications technology ser-vices and product supply chain.				
Vendor Management	Supplier service delivery management	External risks like Process disruptions, Intellectual property theft and Non-compliance with regulatory security standards.	1. Monitoring and review of supplier services - Organizations shall regularly monitor, review and audit supplier service delivery. 2. Managing changes to supplier services - Changes to the provision of services by	1. On a sample basis, select LAN hardware and software contracts. Whether vendor support requirements are clearly defined. Whether product licensing restrictions is clearly identified.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	2. Obtain the service log and look for software or hardware that has been subject to numerous problems and vendor-assisted support. Whether management and the users can support or justify the activity. 3. From the sample of LAN hardware and software contracts, determine if the vendor is reliable. Such information can be obtained from trade periodicals, financial reporting services (e.g. Standard & Poor's), trade associations, and MIS management. 4. Obtain a copy of the negotiated service level agreement from the IS department noting specific performance requirements. Compare the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				agreement with the performance reports.			
Asset Management	Asset Responsibility	Improper IT Asset Management can drive up insurance costs, can lead to inability to identify potential savings, enhance performance and prevent data breaches as a result of outdated inventory information. Also, it will become difficult to remotely manage IT infrastructure.	1. Inventory of assets - Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. 2. Ownership of assets - Assets maintained in the inventory shall be owned by the entity. 3. Acceptable use of assets - Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented, and implemented. 4. Return of assets - All employees and external party users shall return all the organizational assets in their possession upon termination of their	1. Determine: Whether there is a complete inventory of the following: Hardware: Computers, File Servers, Printers, Modems, Switches, Routers, Hubs, etc. Software: all software for each PC is logged with licenses and serial numbers. 2. Check availability of Information Asset Register with records of all assets 3. Verify: a) Written procedures for keeping asset inventory. b) The inventory procedures identify who (title) is responsible for maintain-ing the inventory report. c) The inventory			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			employment, contract or agreement. 5. Disposal of assets - a) Whether there is a policy regarding disposal of obsolete or badly damaged asset. b) Does the policy require management approval of disposal of the equipment. c) Obtain a copy and determine if it has been reviewed and approved by management.	procedures require regular updating of the inventory report. 4. Unused equipment is properly and securely stored. 5. Copies of the software and hardware inventory reports are stored at another secure location. 6. On a sample basis, match the inventory report to actual hardware devices (Inventory Record Accuracy Checks-IRA), All of the hardware present is properly identified/tagged, and located in the proper place.			
Asset management (Data)	Information Classification	Improper Information Asset Classification can impact Confidentiality, Integrity and Availability related to organisational operations,	1. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. 2. Labelling of information - An	1. Check whether the organisation has adopted a formal Information Asset Classification method. The classification method may include: a) Identification of			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		assets, and individuals. Poor classification systems can lead to loss of information in areas like Health and Safety, Financial Loss, Company's Mission/Programs and Public Trust.	appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. 3. Handling of assets - Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	information assets (labelling), b) Classification of information assets; by Confidentiality, Integrity, and Availability ("CIA"); c) Determining controls identified and handling methods adopted based upon the classification. 2. Check availability of Information Asset Register with records of all assets.			
Asset Management (Data)	Media Handling	Risk of both reputational damage and financial losses. Errors in physical media transfer could also lead to cyber-attacks using the social engineering route	1. Management of removable media - Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. 2. Disposal of media -Media shall be disposed of securely when no longer required, using formal procedures. 3. Physical media	1. Management of removable media : check documented procedures and records related to a) authorization for the removal of media from the company and a record of these removals maintained in order to preserve the audit trail, b) Media storage : In compliance with			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			transfer - Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	manufacturers' standards, all media should be kept in a secure and safe environment; c) Where confidentiality or integrity of data is important, whether cryptographic techniques for securing data on removable media is used, d) whether Multiple copies of important data is stored in different media to further reduce the possibility of accidental data damage or loss; e) Process for Registration of removable media 2. Disposal of Media : Check documented procedures and records related to : a) Whether Confidential media is disposed safely through, e.g. by incineration or shredding, or data			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				erasure b) Procedures to identify the items that need safe disposal c) If opting for media collection and disposal services; care must be taken to select a suitable external party with adequate controls and experience; d) In order to maintain an audit trail, the disposal of confidential items is being logged. e) Whether contents of reusable media that are to be removed from the organization should be made unrecoverable; 3. Physical Media Transfer: Check documented procedures and records related to : a) Reliable transport or the use of authorized couriers;			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			b) Packaging to safeguard the content from any physical damage likely to occur during transit and to protect the content against environmental factors such as exposure to heat, humidity, or electro-magnetic fields which could reduce media recovering efficiency. c) Logs to be maintained with details of the media content, date/ time of transfer to location and receipt at the destination.				
System acquisition, development, and maintenance	Security requirements of information systems	Lead to the development unreliable software prone to external threats and vulnerabilities.	1. Information security requirements analysis and specification - The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information	Check for the SDLC methodology adopted with specific inclusion of application security needs. Check how the documentation of security requirements have been carried out			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			systems. 2. Securing application services on public networks - Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. 3. Protecting application services transactions - Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.				
System acquisition, development and maintenance	Security in development and support processes	Vulnerable to external threats and lead to likely disruption of business	1. Secure development policy - Rules for the development of software and systems shall be	Check and validate the following: 1. Examine how the security requirements			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		operations.	established and applied to developments within the organization. 2. System change control procedures - Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. 3. Technical review of applications after operating platform changes - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security. 4. Restrictions on changes to software packages - Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	captured in the Analysis or Initial phases have been addressed in the design, development, testing and implementation processes. Special attention to be given on how the organisation has included preventive measures to block SQL Injection, Denial of Service threats, etc. from the external environment 3. Check whether 3rd Party VAPT testing has been formally carried out on the developed system and remedial actions initiated and closed before Go Live 4. Assess the Change Management process to ascertain how changes have been carried out during			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			5. Secure system engineering principles - Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts. 6. Secure development environment - Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. 7. System security testing - Testing of security functionality shall be carried out during development. 8. System acceptance testing - Acceptance testing programs and related criteria shall be established for new information	development and post implementation phases ensuring security reliability. 5. Examine the procedures related to Infrastructure and operating system changes during the life cycle of the project implementation. Ensure that the organisation tracks and control the changes in a systematic manner for the complete infrastructure environment comprising of Development, Test and Production servers.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			systems, upgrades and new versions.				
Information Security Incident Management	Management of information security incidents and improvements	Risk of security issues within an IT infrastructure.	1. Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. 2. Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible. 3. Reporting information security weaknesses - Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services. 4. Assessment and	1. Check for availability of procedures on management of Information Security Incidents, events and weaknesses with emphasis on: - Responsibil-ities & Procedures: Planning and preparing incident response, Monitoring, detecting, analysing and reporting information security events, Logging incident management activities, Handling forensic evidence, Assessing and deciding on information security events and weaknesses, Responding to a security incident, both internally and externally - Reporting Information			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			decision on information security events - Information security events shall be assessed, and it shall be decided if they are to be classified as information security incidents. 5. Response to information security incidents - Information security incidents shall be responded to in accordance with the documented procedures. 6. Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. 7. Collection of evidence - The organization shall define and apply procedures for the identification, collection, acquisition and preservation of	Security Incidents - Reporting Information Security Weaknesses - Assessment & Decision on Information Security Events - Response to Information Security Incidents - Learning from Information Security Incidents - Collection of Evidence 2. Check sample security incidents in the past and check compliance to the incident management processes			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			information, which can serve as evidence.				
Business Continuity Management	Information security continuity	Absence of a rigorous Disaster Recovery and Business Continuity Plan could result in a - Complete Loss of Data, which is critical to business operations - Business Interruption - Loss of Clients, - Damaged Reputation, and / or - Business Failure.	1. Planning information security continuity - The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. 2. Implementing information security continuity - The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. 3. Verify, review and evaluate information security continuity - The organization shall verify the established and implemented information security	1. Check whether the Organisation has appointed a Top Management driven Disaster Recovery / BCP Task Force to implement the plan 2. Review how the organisation has implemented or is in the process of implementing DRP/BCP with focus on - Project Planning - Country Risk/Analysis Review - Business Impact Analysis - Recovery Strategy (RTO, RPO guarantees) - Plan Development - Testing -Training - Business Continuity Plan - Maintenance			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. 4. Redundancies - Availability of information processing facilities - Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.				
Review of Information System Security	Monitoring Processes, Performance Evaluation	Risk of Non-compliance with all relevant legislation and internal policies and standards.	1. t Processes exist to monitor compliance with all relevant legislation plus internal policies and standards. 2. Monitoring processes are carried out by management.	Examine the Performance Management and Monitoring process with special emphasis on metrics identification, measurement and reporting. Also review how actions have been initiated looking at metrics trends or targets not getting achieved.			
Review of Information	Management Review	Risk of progressive	Top management shall review the	Validate how the Management			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
System Security		degradation of Security measures.	organization's information security management system at planned intervals to ensure its continuing suitability, adequacy, and effectiveness.	Review process is carried out in the organisation - either directly by the Board of Directors or by Audit Committee Check for appropriate review records and action points.			
Review of Information System Security	Internal Audit	Absence of a formal Internal Audit function and not having adequate and competent staff in the internal audit activity are a risk that exposes the organization to inadequate evaluation of the effectiveness of risk management, control, and governance processes.	The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system: a) conforms to: 1) the organization's own requirements for its information security management system; and 2) the requirements of this International Standard; b) is effectively implemented and maintained.	1. Check the Internal Audit policy, standard and procedure within the organisation 2. Check for evidence of Internal Audits conducted by the Organisation, the Audit schedules, and the results of the Audit. 3. Check how the recommendations of the Internal Audit have been Implemented.			
Information & Communications	Information & Communications	Risk that the Security policies are not working	1. Metrics are provided to the Board of Directors, its committees and	1. Check the IT Security Management Reports that are			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		effectively.	management in relation to IT security. 2. Additional reports are provided to the Board of Directors and to management on a regular basis. 3. Management is always provided with reports when there are IT control failures. 4. The Board of Directors and its committees receive similar reports of IT control failures.	prepared and circulated to the Board of Directors. 2. Examine the content and records of the Board Review / Audit Committee review and the actions taken.			
Cryptography	Cryptographic Controls	exposes sensitive application data on a weak or non-existent cryptographic algorithm.	1. Policy on the use of cryptographic controls - A policy on the use of cryptographic controls for protection of information shall be developed and implemented. 2. Key management - A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	In case the Organsiation's business environment requires, 1. Review the Cryptographic Control policy and procedures adopted in the organisation. 2. Review that robust Key Management procedures are in place to protect sensitive information.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
Compliance	Compliance with legal and contractual requirements	Risk to non-compliance	1. Identification of applicable legislation and contractual requirements - All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented, and kept up to date for each information system and the organization. 2. Intellectual property rights - Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. 3. Protection of records - Records shall be protected from loss, destruction,	Review and validate how the organisation has identified and recorded its legal, regulatory, and contractual obligations; the responsibilities for meeting such requirements and any necessary policies, procedures and other controls required for meeting the controls.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. 4. Regulation of cryptographic controls - Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.				
Compliance	Information security reviews	Risk of not in keeping current policies and standards changing with business needs and regulations.	1. Independent review of information security - The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant	1. Check that Independent Reviews are being conducted periodically of the Information Security Policy with a focus to improve the organisation's approach to information security, including The information security policy. Topic-specific policies. Related controls.			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			changes occur. 2. Compliance with security policies and standards - Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. 3. Technical compliance review - Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	2. Check whether the persons who have conducted the reviews have been independent, possess relevant operational competence and have no vested interests. 3. Check whether the organisation also conducts Ad-hoc reviews due to amendment of laws/regulations, post security incidents, major changes to business, introduction of new products, organisational changes, etc.			

Standards on Internal Audit (SIAs) Compliances

This Checklist on Standards on Internal Audit is illustrative in nature. Members are advised to suitably modify the same as per the facts, circumstances, and nature of the entity under internal audit. This document neither supersedes nor is a replacement of any guidance/ pronouncements/ Standards issued by ICAI. Members are advised to read or use the Checklist in conjunction with the Standards on Internal Audit. Members are also advised to exercise the professional judgement while using the Checklist on Standards on Internal Audit.

Particulars	Standards on Internal Audit	Response (Yes/No/ NA)
Planned internal audits are in line with the objectives of the internal audit function, as per the internal audit charter of the entity (and terms of engagement, where it is an outsourced engagement) and in line with the overall objectives of the organisation.	SIA 220, Conducting Overall Internal Audit Planning	
Confirm and agree with those charged with governance the broad scope, methodology and depth of coverage of the internal audit work to be undertaken in the defined time-period.		
Overall resources are adequate, skilled and deployed with focus in areas of importance, complexity and sensitivity.		
Audits undertaken conform at all times with the applicable pronouncements of the Institute of Chartered Accountants of India.		
The Internal Auditor shall gather all the information required to fully understand the entity's business environment, the risks it faces and its operational challenges.		
Key element of planning involves extensive discussion and deliberation with all stakeholders, including executive management, risk owners, process owners, statutory auditors, etc.		
Prior to defining the scope of internal audit, a complete identification of all the Auditable Units (locations, functions, business units, legal entities, including third parties where relevant) of the organisation shall be made.		
To confirm compliance of audit procedures with the SIA, all key		

steps undertaken in the planning process shall be adequately documented to confirm their proper completion.		
A risk-based planning exercise shall form the basis of the Internal Audit Assignment Plan. The Internal Auditor shall undertake an independent risk assessment exercise to prioritise and focus audit work on high risk areas and processes, with due attention given to matters of importance, complexity and sensitivity.	SIA 310, Planning the Internal Audit Assignment	
To confirm compliance of audit procedures with the SIA, all key steps undertaken in the planning process shall be adequately documented to confirm their proper completion. Essential documentation shall be as follows: (a) Planning Process documentation (or Checklists) and any tools used in the planning process. (b) Documentation supporting the information gathered about the Auditable Unit's business and operations, systems and processes and past or known issues. (c) Summary of meetings and communication with key stakeholders, with a summary of their inputs. (d) Risk Assessment documentation and a Summary of risk mitigating controls deployed. (e) Summary of available resources, their competencies and the proper matching of their skills with the audit requirements. (f) Detailed Internal Audit Programme (IAP) which lists the specific testing procedures to be conducted for each audit objective. (g) The final Internal Audit Assignment Plan duly approved by the Chief Internal Auditor.		
The Internal Audit Charter and the Engagement Letter shall be reviewed periodically by the Chief of Internal Audit and the Engagement Partner to ensure its relevance to the changing times or circumstances (e.g. change in scope). If found necessary, the proposed amendments to these documents shall be put up to the approving authority for their review and approval.	SIA 230, Objectives of Internal Audit	

All internal audits are conducted with certain fundamental features designed to:
 	
• establish the credibility of the Internal Auditor
 	
    o Independence
 	
    o Integrity and Objectivity
	Basic Principles of Internal Audit	

o   Due Professional Care
 	
    o   Confidentiality
 	
    o   Skills and Competence
 	
•   outline the elements essential for performance of internal audit activities
 	
    o   Risk Based Audit
 	
    o   System and Process Focus
 	
    o   Participation in Decision Making
 	
    o   Sensitive to Multiple Stakeholder Interest
 	
    o Quality and Continuous Improvement		

The Chief Internal Auditor has the overall responsibility to ensure the achievement of the objectives of the internal audit function through a well-documented internal audit process.	SIA 210, Managing the Internal Audit Function	
To confirm compliance with the Standard, all key activities which form part of the internal audit process shall be documented to confirm their timely completion.		
Where the findings of the Expert will form part of the assurance report to be issued by the Internal Auditor, the Internal Auditor shall participate in defining the scope, approach and work to be conducted by the Expert. Otherwise, the Internal Auditor shall not incorporate the finding of the Expert in his Internal Audit report.	SIA 240, Using the Work of an Expert	
The Internal Auditor shall perform an evaluation of the work completed by the Expert to ensure that the work completed constitutes appropriate and reliable evidence to support the overall conclusions to be reported.		
The Internal Auditor shall retain ultimate responsibility for internal audit conclusions and opinions which are incorporated in his internal audit report, unless specifically mandated otherwise by the Assurance User (the recipient of the Internal Audit Report). Hence, the Internal Auditor shall not refer to the work of an Expert in his Internal Audit Report.		
An effective communication relationship is established and maintained with Those Charged with Governance.	SIA 250, Communi-cation with Those Charged with Governance	
The matters to be communicated, the form and manner, and periodicity of communication are best established between the Internal Auditor and Those Charged with Governance. In this regard, a formal communication process shall be pre		

agreed with TCWG, and include the following (indicative list): (a) form and content of communication (the "what"); (b) manner and protocol of communication (the "who" and "how"); and (c) timelines and periodicity of communication (the "when")		
Certain matters which the Internal Auditor should consider as essential matters for communication may include the following (indicative list): (a) Annual Internal Audit plan, covering the scope, timing, methodology of audit assignments to be undertaken, along with resources and budgets of the internal audit department; (b) Outcome of the risk assessment exercise conducted to develop the Internal Audit Plan; (c) Periodic update on significant observations, with corrective action plans, as agreed with the auditee; (d) Details of the functioning of the internal audit department and a continuous update on their progress, status of performance and any resource or budget constraints; (e) Status update of prior audit issues, their timely closure with an Action Taken Report; and (f) Any other matters as per Standards on Internal Audit, laws and regulations and the professional judgement of the Internal Auditor.		
Maintain all the documents as required by the Standard on Internal Audit (SIA) 330, Internal Audit Documentation. Oral communications with TCWG may be documented for records through written communication or as the minutes of meetings.		
The Internal Auditor shall obtain sufficient and appropriate audit evidence which can form the basis of audit findings and allow reliable conclusions to be drawn from those findings. Evidence collected through various audit procedures shall be complementary and relevant to the objectives of the audit procedure conducted	SIA 320, Internal Audit Evidence	
The evidence shall be obtained from reliable sources with consistency between various evidence collected		
All audit evidence collected shall be recorded and the internal audit function shall maintain a written process explaining the		

manner in which audit evidence is to be gathered, reviewed, documented and stored as per Standards of quality and in conformance to the Standards on Internal Audit.		
The internal auditor shall record the nature, timing and extent of completion of all internal audit activities and testing procedures in the form of reproducible documents.	SIA 330, Internal Audit Documentation	
Documentation shall be complete and sufficient to support the analysis conducted on the audit evidence, the identification of findings, the formulation of audit observations and the drafting of the internal audit reports based on the findings. Documentation shall clearly state the purpose of the procedure, the source of evidence, the outcome of the audit work and also identify the performer and reviewer.		
The internal audit function shall maintain a written process explaining the manner in which documentation will be prepared, reviewed, stored and finally discarded, to ensure quality and conformance to Standards on Internal Audit.		
The internal audit work paper files shall be completed prior to the issuance of the final internal audit report. Any pending administrative matters shall also be completed within sixty days of the release of the final report.		
The ownership and custody of the internal audit work papers shall remain with the Internal Auditor.		
The audit work is executed in accordance with the Internal Audit Programme and Audit Procedures are completed effectively and timely to help achieve overall objectives of the audit assignment.	SIA 350, Review and Supervision of Audit Assignments	
The extent of the documentation reviewed is based on the professional judgement of the reviewer, and can include checking the name of preparer, date of preparation, relevance and reliability of audit evidence, conclusions formed, audit observations drafted, the sufficiency of documents, etc. The adequacy of the documentation is tested on the basis of the requirements of the applicable Standards on Internal Audit.		
A review of the audit workpapers shall be carried out to ensure that these are sufficient and appropriate to allow the reviewer to arrive at the same conclusions and formulate similar observations, as done by the audit staff. The documentation shall record the evidence of the supervision and review conducted, including the performance of any audit procedures subsequent to the review.		

The Internal Audit function (or out-sourced Firm) shall maintain a written process explaining the manner in which review and supervision shall be performed to ensure conformance to the quality as per Standards on Internal Audit.		
All communication with management shall be clear, appropriate and in line with the agreed process and timelines.	SIA 360, Communication with Management	
The process documentation shall outline the various modes and channels of communication, the periodicity and timelines for communication, and also cover certain essential information required to be communicated. Where essential matters are concerned, any verbal communication should subsequently be confirmed in writing and maintained as audit documentation.		
To confirm compliance of audit procedures with this SIA, the list of documents required is as follows: (a) Written Communication process and protocol, as part of the Internal Audit Manual. (b) Written details of essential exchange of information, as required by other SIAs, cross reference to the Internal Audit Program, where appropriate.		
On the basis of the internal audit work completed, the Internal Auditor shall issue a clear, well documented Internal Audit Report which includes the following key elements: (a) An overview of the objectives, scope and approach of the audit assignments; (b) The fact that an internal audit has been conducted in accordance the Standards of Internal Audit; (c) An executive summary of key observations covering all important aspects, and specific to the scope of the assignment; (d) A summary of the corrective actions required (or agreed by management) for each observation; and (e) Nature of assurance, if any, which can be derived from the observations.	SIA 370, Reporting Results	
The nature of assurance, if any, to be provided shall be in line with Standard on Internal Audit (SIA) 110, Nature of Assurance as pre agreed with the auditee at the planning stage.		
The content and form of the Internal Audit Report is to be established by the Internal Auditor based on his best professional		

judgement, in consultation with the auditee and, if necessary, with inputs from other key stakeholders. No internal audit report shall be issued in final form unless a written draft of the report has previously been shared with the auditee.		
The internal audit report shall be issued within a reasonable time frame from the completion of the internal audit work.		
Where the internal audit is conducted in compliance with the Standards of Internal Audit, (within the Framework governing Internal Audits), and the internal auditor can substantiate the same with supporting evidence and documentation, the internal audit report shall include a statement confirming that "the internal audit was conducted in accordance with the Standards of Internal Audit issued by the Institute of Chartered Accountants of India".		
The manner in which the internal audit report is drafted and presented is a matter of professional judgment and choice and could be influenced with preferences of the recipients. The SIA does not mandate any particular format or list of contents since the Internal Auditor is expected to exercise his best professional judgement on matters regarding how and what to report. Where some level of assurance is being provided, the form and content of the report shall be as per SIA 380, "Issuing Assurance Reports".		
To confirm compliance of audit procedures with this SIA, the list of documents required is as follows: (a) Copies of draft and final internal audit reports to be maintained, appropriately cross referenced to specific observations. (b) If appropriate, management action plans may be counter signed by respective management personnel		
The Chief Internal Auditor is responsible for continuously monitoring the closure of prior audit issues through a timely implementation of action plans included in past audits. This shall be done with a formal monitoring process, elements of which are pre-agreed with management and those charged with governance. The responsibility to implement the action plans remains with the management	SIA 390, Monitoring and Reporting of Prior Audit Issues	
For critical or sensitive issues (e.g., those rated high risk or with fraud risk), follow-up audit procedures shall be performed to ensure that the risk has been mitigated to an acceptable level. For		

medium risk issues, documentation proof of the implementation of the audit recommendations may be acceptable. For low-risk issues, a written note confirmation from management may be sufficient. However, the documentation for all the three categories of risks shall be maintained as per the Standard on Internal Audit (SIA) 330, "Internal Audit Documentation".		
When the Internal Auditor observes delay in the agreed time schedule for implementation, the Internal Auditor shall intimate the auditee and agree to a new time schedule.		
The Internal Auditor shall document the working papers according to the Standard on Internal Audit (SIA) 330, "Internal Audit Documentation", which shall include: (a) The monitoring plan as agreed with management, including escalation procedures and protocol to be followed in case of delays. (b) Auditee's confirmation of either complete implementation of agreed actions, or reasons for part/non-implementation and thereby, acceptance of risks. (c) The documentary evidence and working papers to support additional audit procedures performed to confirm effective closure of prior issues. (d) Escalation communication with corresponding management responses. (e) Periodic status reports (ATR) issued to the management and those charged with governance.		
The internal auditor shall periodically report to the management, and the Audit Committee, the status of prior issues (generally in the form of an "Action Taken Report"), including providing a confirmation of closure based on additional procedures, ageing of issues pending closure and reasons for any delays.		
Audits are undertaken after due study and understanding of the Organisation's ITE, which covers the IT strategy, policies, operating procedures, the risks and governance mechanism in place to manage the ITE.	SIA 520, Internal Auditing in an Information Technology Environment	
An independent risk assessment, along with an evaluation of the controls required to mitigate those risks, forms the basis of the audit procedures.		
The audit procedures, as designed and executed, are sufficient to allow an independent assurance, especially in the areas of		

(indicative list): • Security and reliability of information. • Efficiency and effectiveness of information processing. • Analysis and reporting of the information. • Continuous access and availability of the information. • Compliance of the IT related laws and regulations.		
The overall objective of performing an internal audit in an ITE is to provide independent assurance and help in making improvements in the ITE, thereby enabling the achievement of business objectives.		
Audit documentation shall include IT environment understanding and scoping, IT risk assessment, IT Audit planning, IT risk and controls matrix, IT test work papers, system generated reports with the supporting documents, evidence gathered and so on. Modern audit documentation tools may be used by the Internal Auditor to make the audit more efficient and effective.		
The Internal Auditor shall review both, the Pre-engagement and Post engagement due diligence undertaken by the User Entity, including an assessment of the control environment at the TPSP.	SIA 530, Third Party Service Provider	
A periodic independent risk assessment of each third-party arrangement shall be conducted by the management and reviewed by the Internal Auditor to ensure adequate mitigation steps and control activities are designed, implemented, and operated effectively.		
In case, the Internal Auditor is not performing an independent audit but obtains TPAA reports, the review of the TPAA reports shall be undertaken in compliance with Standard on Internal Audit (SIA) 240, Using the Work of an Expert.		
The Internal Auditor provides a written report expressing an opinion that conveys the assurance obtained about the Subject matter. Standard on Internal Audit (SIA) 380, "Issuing Assurance Reports" establish the basic elements, form and content of assurance reports. In addition, the Internal Auditor considers other reporting responsibilities, including communicating with those charged with governance (SIA 250) when it is appropriate to do so. Standard on Internal Audit (SIA) 370, "Reporting Results" covers those assignments where no formal assurance report is required,	SIA 110, Nature of Assurance	

and the Internal Auditors' report is, generally, in the form of a Summary of Findings or Observations.		
The Internal Auditor shall review the risk assessment exercise undertaken at the time of planning the audit assignment to establish a basis of evaluating whether adequate and appropriate Internal Controls are in place to address the risks identified.	SIA 120, Internal Controls	
Where the Internal Auditor is required to provide an independent opinion over the presence, design, implementation and/or operating effectiveness over Internal Controls, this shall be consistent with the requirements of SIA 110, Nature of Assurance, especially with regard to the need to have a clear understanding of the Internal Controls Framework which shall form the basis of the assurance.		
In situations where the Statutory Auditor is expected to rely on the work of the Internal Auditor as per Standard on Auditing (SA) 610, Using the Work of Internal Auditors, issued by ICAI, regarding their audit of Internal Financial Controls over Financial Reporting, the Internal Auditor shall document the objectives and agreed scope and approach of the internal audit, over which the reliance is to be placed by the Statutory Auditor.		
Where the independent assurance requires the issuance of an audit opinion over the design, implementation and operating effectiveness of risk management, this shall be undertaken in line with the requirements of SIA 110, "Nature of Assurance", especially with regard to the need to have a formal Risk Management Framework in place, which shall form the basis of such an assurance.	SIA 130, Risk Management	
The Internal Auditor shall not assume any responsibility to manage the risks or to execute risk management decisions. It is not responsibility of the Internal Auditor to mitigate or resolve the risks.		
"Basic Principles of Internal Audit" on Risk Based Audits, requires the Internal Auditor to conduct the audits based on a risk assessment exercise. SIA 220, "Conducting Overall Internal Audit Planning" and SIA 310, "Planning the Internal Audit Assignment" mandate the Internal Auditor to conduct risk-based audit planning to ensure that due attention is given to matters of importance, complexity and sensitivity. Similarly, SIA 370, "Reporting Results" expects the auditor to consider the risk of the observations in deciding the matters to be reported.		

Where a written assurance report is being issued, the Internal Auditor shall also consider the following as a basis for audit opinion: (a) The linkage of the risk management framework with the system of CEO and CFO certification on Internal Controls; and (b) Certificates of self-compliance from owners of key risks to support a system of continuous compliance.		

Legal and Statutory Compliances

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed
Control Environment	Legal and Statutory	Non-compliance with legal and statutory requirements	The Board of Directors should clearly have a policy on 'Compliance with legal and statutory requirements' and demonstrate the same by oversight periodically.	Board of Directors	Review of the Legal and Regulatory Compliance policy. Review of the minutes of the meeting discussing. Audit of legal and statutory compliances.
Compliances	Legal and Statutory	Risk of Non-compliance with a particular statute	To have a 'compliance calendar' which enlists all the compliance requirements during the period / year and then circulated to the department. At the due date, the legal team has to ensure that the requisite compliances are done. Compliance calendar to be approved by Board and periodically reviewed by the Directors.	Legal team and Board of Directors	a. Legal compliance calendar; b. Details of returns filed and compliances carried out; c. Minutes of the Board Meeting.
Compliances	Legal and Statutory	Risk of Legal Compliance calendar not updated.	The Head of Legal should ensure that any amendments to law, to the extent applicable, is also reflected in the compliance calendar.	Legal team	To review the amendments made to law (reference to website, authoritative pronouncements of the Government, expert advice, etc.) and see whether the amendments are carried out.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed
Compliances	Legal and Statutory	Risk of incorrect interpretation of statutes	To take legal opinion for critical issues and advise the management accordingly. To discuss with CFO and make necessary entries / disclosures in financial statements.	Legal team	To review the advice received by the legal experts and how the same have been addressed.
Compliances	Legal and Statutory	Risk of no response given to the notice of the statutory authorities	All the statutory notices should be sent to CFO or Chief Legal or Chief Counsel as decided by the Board. All communication should be tracked with a tracking number and responded to within the timeframe given by law.	Legal team and Board of Directors	To review all the legal notices received and their response is submitted within the timeframe.
Compliances	Legal and Statutory	Risk of defending a case or contesting demand without legal advice.	No case or demand be contested without the legal advice.	Legal team	Legal team should obtain written advice from experts before any claim is contested. On basis, legal team should hire an advocate to represent them.
Compliances	Legal and Statutory	Risk of hiring a consultant or legal expert who does not have experience.	Due diligence of the legal team (including their expertise known with peers of the same industry, known associates / affiliates etc.,) and also to ensure that there is no dependency on one legal expert.	Legal Team, Board of Directors	Board to evaluate different legal firms and choose the one that meets the requirements of the entity including their expertise, geographical spread, history of handling similar cases and their reputation.

Operational and Administrative Expenses

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
Operational and Administrative Expenses	Expense Budgeting and Planning	Risk of poor expense budgeting and planning process lies in inaccurate projections, underestimated or overestimated costs, inflexibility, misalignment with objectives, incomplete analysis, and communication gaps, which can lead to financial strains.	The organization establishes comprehensive controls for expense budgeting and planning, including data accuracy validation, multi-level review, alignment with strategic objectives, flexible contingency planning, regular monitoring, technology utilization, and continuous improvement to mitigate risks and ensure accurate resource allocation.	CFO	Perform tests including data accuracy, assumption validation, scenario analysis, alignment with objectives, budget vs. actual variance analysis, multi-level review, contingency planning, collaboration assessment technology functionality, documentation review, continuous improvement evaluation, and policy adherence to ensure the effectiveness and accuracy of the expense budgeting and planning process.	Budget Documents Policies and procedures Email Correspondence Meeting Minutes Actual expense reports Financial statements Budget revisions Approval Logs
	Expense Approval Workflow	Risk of non-compliance, with policy segregation of duties issues, inconsistent	The organization implements controls such as enquiry, quotation	Procurement	Perform tests including policy adherence checks, segregation of duties verification,	Expense approval records Expense reports Approval

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		approvals, approval delays, bias, limited visibility, errors, inefficient processes, lack of documentation, insufficient training, regulatory compliance concerns, audit trail gaps, system vulnerabilities, and scalability challenges.	comparison and lease cost service engagement with clear approval guidelines, segregation of duties, automated workflows, documented policies, training, multi-level reviews, electronic signatures, audit trail logging, transparency, real-time visibility, compliance reviews, and regular audits to ensure the integrity, accuracy, and efficiency of the expenses approval workflow for operational and administrative expenses.		electronic signature validation, real-time visibility assessment, compliance reviews, accuracy evaluations, training effectiveness assessments, and regulatory compliance verification to ensure the effectiveness, accuracy, and compliance of the expenses approval workflow process for operational and administrative expenses.	workflows Approval threshold and levels Audit trail logs Exception handling documentation Manager training records
	Expenses Tracking and Recording	Risk of inaccurate data entry, missing documentation, policy non-compliance,	The organization implements a comprehensive expense policy with clear	CFO	Perform tests including policy compliance, service receipt verification, authorization checks, and	Expenses policies and procedures Authori-zation

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		duplicate entries, misallocation, human error, fraud, and technology failures, highlighting the need for robust controls and standardized procedures to ensure accurate financial reporting and decision-making.	procedures, proper authorization, thorough documentation, and regular reconciliations to ensure accurate and transparent expenses tracking and recording while preventing fraud and errors.		reconciliation testing to ensure accurate, complete, and efficient expenses tracking and recording for both operational and administrative expenses.	records Expenses documentation Expenses reports Audit trails Recon-ciliation records
	Invoice processing and Approval	Risk of wrong invoice processing and approval processes encompass issues such as duplicate or fraudulent invoices, unauthorized approvals, data entry errors, manual processes, complex approval hierarchies, and inadequate compliance checks, necessitating robust controls and automation to mitigate	The organization implements comprehensive controls for invoice processing and approval in operational and administrative expense processes, including 3-way matching, verification, segregation of duties, automated processing, compliance checks, and documentation, to ensure accuracy, prevent fraud,	Accounts Payable	Perform comprehensive tests including verification, segregation of duties, authorization, compliance checks, automated processing, and documentation to ensure the accuracy, security, and effectiveness of the invoice processing and approval process in operational and administrative expense workflows.	Invoices and supporting documentation Approval records Segreg-ation of Duties records Audit trails and logs Vendor master data records Automated system records

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		potential financial, operational, and reputational impacts.	and maintain compliance.			
	Expense Reimbursement	Risk of expenses reimbursement processes include inaccurate submissions, policy violations, fraudulent claims, delayed submissions, lack of documentation, inadequate review, and non-compliance with regulations, necessitating strong controls, policy adherence, automation, and regular audits for risk mitigation.	The organization implements a range of controls including policy adherence, documentation requirements, segregation of duties, automated systems, compliance checks, auditing, and timely reimbursement to ensure accurate, compliant, and secure handling of expense reimbursement within operational and administrative expenses.	Accounts Payable	Perform tests including policy adherence, authorization, compliance checks, timely reimbursement, data security, and system functionality to ensure accuracy, compliance, and efficiency in the expense reimbursement process.	Reimbursement requests Receipts and supporting documentation Reimbursement policy Pre-Approval records Compliance check records Audit trails and logs
	Vendor Management	Risk of vendor management encompass issues such as vendor reliability, quality control,	The organization implements comprehensive controls in vendor	Accounts Payable	Perform tests and assessments throughout the vendor management process, including	Vendor Documentation Financial records Quality

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		financial instability, compliance challenges, data security, contractual disputes, and overdependence, necessitating comprehensive processes to ensure reliable supply, compliance, quality, and financial stability while minimizing disruptions and legal liabilities.	management to ensure vendor selection, contract agreements, performance monitoring, compliance checks, data security, risk mitigation, and continuous improvement, fostering reliable relationships while minimizing risks and disruptions.		due diligence, contract compliance, quality control, security, and regulatory adherence, to ensure vendors meet financial, contractual, quality, security, and legal requirements.	Assurance records Performance monitoring and reporting Security and comp-liance documentation Comm-unication records
	Expenses Analysis and Reporting	Risk of data inaccuracies, lack of documentation, compliance issues, manual inefficiencies, complex expense structures, reporting delays, technological limitations, change management challenges, third-party vendor issues, and insufficient oversight, all of which can impact	The organization implements controls such as expense approval processes, documentation standards, segregation of duties, automated systems, data reconciliation, audit trails, and training to ensure accuracy, compliance, and efficiency in expenses	Accounts Payable	Perform tests including expenses sampling, policy adherence checks, duplicate expenses detection, data reconciliation, budget compliance assessment, and verification of authorization levels to ensure accurate, compliant, and transparent expenses analysis and reporting for operational and administrative expenses.	Expenses documents Expenses reports and summaries Approval records Expenses management and system data Bank and financial records Expenses category documentation

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		financial accuracy and transparency.	analysis and reporting for operational and administrative expenses.			
	Expenses Reduction and Cost Control	Risk of operational disruption, employee morale impact, compromised quality, short-term focus, loss of competitive edge, unintended consequences, inadequate cost analysis, resistance to change, supplier relationship risks, over-reliance on automation, legal and compliance risks, lack of monitoring, misalignment with strategy, financial instability, and diminished customer experience.	The organization implements controls such as budgetary oversight, cost analysis, management approval, stakeholder communication, employee engagement, vendor management, technology utilization, Lean practices, strategic alignment, regulatory compliance, and audit monitoring to ensure effective and sustainable expense reduction and cost control for operational and administrative expenses.	CFO	Perform tests including variance analysis, cost-benefit assessments, vendor contract reviews, employee engagement evaluations, technology utilization assessments, regulatory compliance audits, and operational impact assessments to validate the effectiveness of expense reduction and cost control efforts while minimizing risks and ensuring alignment with long-term strategy.	Budget reports Financial statements Vendor contracts Process documentation Key performance indicators Opera-tional metrics

Government Grants

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
Government Grants	Understanding the business	Risk of eligible government grant not claimed	To understand the business carefully, including reading necessary materials and review of peers in the similar industry as to whether the particular business is eligible for government grant.	Auditor	To understand how the business is eligible for government grants and document how the Company has been assessed or evaluated that it is eligible for the grant.	Eligibility for the Grant	100%
Government Grants	Use of Government Grant	Risk of possible misuse of Grant or non-compliance with the conditions.	Periodically the CFO (designated employee) verifies compliance with grant terms, conditions, and reporting requirements and that grant funds are being used for their intended purposes and are in compliance with applicable regulations.	Corporate Accounts	Review of the conditions for the Grant and have an understanding of the compliance requirements and how the same is aligned to the client's business.	Eligibility for the Grant	100%

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
Government Grants	Classification of Government Grant	Classification of funds as capital funds or revenue receipts.	Classification is essential since the accounting treatment is fully dependent on this, a material error can misstate the financial statements.	Corporate Accounts	Whether the classification is based on the conditions prescribed in AS 12 or Ind AS 20.	Classification of Grant	100%
Government Grants	Capital Grant	Risk of misuse of Capital Grant	CFO (designated employee) to review the use of capital grant as mentioned in the conditions to the Grant.	Corporate Accounts	Review of the document prepared by CFO (designated employee) to indicate how the capital grant is expected to be used. Also to review whether there is any other audit / review done by an independent official or representative of the Government to ensure utilisation and documents like utilisation certificate is available for review.	Utilisation of the Grant	100%
Government Grants	Capital Grant	Risk of assets procured which is not	a) Management to approve the expenditure;	Corporate Accounts and Accounts	Review of the procurement process. Vouching of the	Actual procurement of assets	To be decided based on the

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
		related to the project for which Grant is obtained.	b) Select the vendors based on the quotations received; c) Receipt of assets and inspection of the assets; d) Acknowledging the receipt of asset; e) Ensuring this is put to use.	Payable	expenditure with underlying purchase orders, invoices, receipt of assets and acknowledgement from the Company. Reviewing the asset has been put to use.		project size.
Government Grants	Capital Grant	Accounting of Capital Grants	Review of the CFO (designated employee) to decide upon the accounting aspects including whether to choose the option to reduce the Grant received from the Overall cost of assets or show the same separately.	Corporate Accounts and Accounts Payable	Review of any note prepared by the CFO (designated employee) on the appropriate accounting treatment to be given.	Appropriateness of Accounting	100%
Government Grants	Revenue Grant	Risk of misuse of ~~Capital~~ Revenue Grant	CFO (designated employee) to review the use of revenue grant as	Corporate Accounts	Review of the document prepared by CFO (designated employee) to indicate how the	Utilisation of the Grant	To be decided based on the project size.

113

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
			mentioned in the conditions to the Grant.		revenue grant is expected to be used. Also to review whether there is any other audit / review done by an independent official or representative of the Government to ensure utilisation and documents like utilisation certificate is available for review.		
Government Grants	Revenue Grant	Risk of assets procured which is not related to the project for which Grant is obtained.	a) Management to approve the expenditure; b) Select the vendors based on the quotations received; c) Receipt of goods and inspection of the goods; d) Acknowledging the receipt of goods; e) Ensuring this is put to use.	Corporate Accounts and Accounts Payable	Review of the procurement process. Vouching of the expenditure with underlying purchase orders, invoices, receipt of assets and acknowledgement from the Company. Reviewing the asset has been put to use.	Actual procurement of assets	To be decided based on the project size.
Government Grants	Financial Controls and	Risk of Unauthorized	The transactions	Corporate Accounts	Assess the adequacy and	Accurate and Authorized	100%

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
	Expenditures	transaction	related to receipt and expenditure of Government grants are accurate, valid, properly authorized and supported by Invoices, Receipts, Payment records, etc.	and Accounts Payable	effectiveness of financial controls related to grant funds. Examine financial transactions and expenditures to ensure accuracy, validity, and proper authorization. Verify the documentation supporting financial transactions, such as invoices, receipts, and payment records.	transaction	
Government Grants	Budget and Expense Tracking	Risk of Expenditure exceeding the budget	Management periodically compares the approved budget with Actual expenses incurred during the Grant period. The Budget variances are analysed and significant deviation from original plan are investigated.	Corporate Accounts and Accounts Payable	Verify the process of formal review of budget vs actuals. Compare the approved budget with actual expenses incurred during the grant period. Analyze budget variances and investigate any significant deviations from the original plan.	Budget vs Actual Expenditure	100%
Government Grants	Revenue Grant	Risk of Inappropriate Accounting	Review of the CFO (designated	Corporate Accounts and	Review of any note prepared by the CFO	Appropriateness of Accounting	100%

115

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
			employee) to decide upon the accounting aspects ensuring that the Government Grant is accounted as revenue grant over a period of time.	Accounts Payable	(designated employee) on the appropriate accounting treatment.		
Government Grants	Project Management	Risk of Projects not being managed as per the plan.	Typically, large projects wherein the Government is giving the grant, could be towards building a new facility or procurement of an asset, etc., such projects needs to be monitored closely including (but not necessarily) have a separate team to monitor the progress and report to the CEO / Board as the case may be.	Project Manager	Review of how progress (including but not limited to even physical verification of the facility being constructed) and observe for any inordinate delays.	Existence of facility and timely completion.	100%
Government Grants	Reporting to Government	Risk of misstatement	Review of the reports being	CEO / CFO /	Review of the reports being	Accuracy of reporting to the	100%

116

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size
		or misreporting to Government.	shared with the Government with a higher authority along with supporting documents.	COO	shared with the Government with the project management reports and other documents. Assess the quality and accuracy of progress reports submitted to the funding agency. Check whether reporting timelines and requirements are being met.	Government.	

Patents and Copyright

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
Intellectual Property Rights	Patents and Copyrights	Risk of Patents and copyrights may be assigned to a third party.	Whenever the Company is hiring a consultant, or in an employment agreement or hiring sub-contractors where it is intended that the copyright in the work arising in the course of their engagement rests with the entity, are in the agreements with them and drafted with sufficient care to ensure that their legal Impact is considered.	Legal / CFO / Human Resource	To check the agreement has a clause mentioning about the ownership of any patents or copyrights arising of the work done .	Ensuring patents and copyrights are not used by a third party.
Intellectual Property Rights	Patents and Copyrights	Risk of patents and copyrights assigned to a third party.	Review of confidentiality clauses in the agreement, and no part of their work would include - existing patented or copyright material or if any copyright is included whether the permission is taken from the owner.	Legal / CFO / Human Resource	No case is filed against the company by third party for violating copyrights.	Non-compliance with patent and copyright law.
Intellectual Property Rights	Patents and Copyrights	Assignment of Copyrights may not be complete.	If the copyright has been acquired, to ensure that the	Legal	Registration and assignment of copyright is	Registration of acquired patent and copyright.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
			rights are assigned, and documented properly with copyright authorities.		complete in all respect.	
Intellectual Property Rights	Patents and Copyrights	Risk of third party claiming the patents and copyrights.	Proper patents and copyright notice should be given in all publicly distributed newspapers or media and on the literature wherever the company's work is communicated.	Legal	Company's official documents having reference of patents and copyrights are reviewed.	Declaration of ownership of copyrights
Intellectual Property Rights	Patents and Copyrights	Risk of infringements breached	To inquire whether any third party has filed a case against the company for infringing the patents and copyrights and if so, what action has the company taken to defend it.	Legal	Discussions with legal advisors and refer any advisory issued by them.	Risks of using copyrights of third party
Intellectual Property Rights	Patents and Copyrights	Risk of overstatement of value of Patents and copyrights.	To review the impairment workings, assumptions on how the business expected to get economic returns from the copyrights and whether the present value of returns are likely to be more than the carrying value of the patents and	Legal	Review of the impairment workings and the assumptions of cash flows, revenue, discount rate, tax impact, etc., Review of the valuation expert's report for the assumptions	Valuation of patents. and copyrights.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
			copyrights. Further, if required, the valuation been done by a valuation expert.		made and justification for the value (as to whether it is reasonable or not).	
Intellectual Property Rights	Patents and Copyrights	Risk of overstatement of value of copyrights.	Whether the cost of copyright is amortised over the useful life.	CFO	To review the amortisation workings and ensure that the amortisation is not beyond the legal life.	Valuation of patents. and copyrights.
Intellectual Property Rights	Patents and Copyrights	Non-compliance with agreements.	Review of all the agreements of acquisition, technology transfer, royalty, etc., to observe for any clauses on non-compliance.	Legal / CFO	Check Non-compliance clause in agreement and action how the same are being dealt with.	Ensuring there are no non-compliances of contractual obligations.
Intellectual Property Rights	Patents	Risk of Company's processes and copyrights being infringed by a third party.	To ensure that all IP Rights including Patents and Copyrights registered with the Government authorities.	Legal and Secretarial Team	To check copy of registered patents and copyrights and check if and infringement.	Possibility of any new product being developed which poses a risk of competitor or market using the same in an unauthorised manner.
Intellectual Property Rights	Patents	Risk of Company's IP Rights not being identified during any business acquisition.	To review the process of business acquisition as it is possible that the acquiree had certain intellectual property	Legal and Secretarial Team / CFO	To discuss with CFO and Legal team, how have they ensured that all the intellectual	Possibility of any intellectual property right not being accounted.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
			rights which were not identified or recognised during acquisition.		property rights have also been acquired and the legal status has been transferred to the acquiring business name.	
Intellectual Property Rights	Patents and Copyrights	Possibility of new products developed and launched in market without having Patents and Copyrights over them.	To ensure the registration of patents and copyrights after product is developed.	Legal / CFO	To check patents and copyrights registration is taken for all new products Developed and registered.	Risk of non-registration of new product patents and copyrights.
Intellectual Property Rights	Patents and Copyrights	Risk of non-compliances with specific industry regulations like Pharmaceutical, Software, Telecommunication and technology, consumer electronics, food products, etc.,	To a checklist of all compliance required as per all industry regulations is prepared.	Legal / CFO	To review the compliance requirements of all the industry standard regulations.	Compliance with local laws and regulations.
Intellectual Property Rights	Patents and Copyrights	Unauthorized access to patent/copyright documentation.	Secure document management system with access controls and implement non-disclosure agreements for external parties.	IT Department	To review that access permissions are properly configured in the document management system and NDA Compliance Testing is carried out.	Risk of unauthorized access to patent/copyright documentation.

121

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
Intellectual Property Rights	Patents and Copyrights	Unauthorized use leading to loss of licensing revenue.	Strong licensing agreements and tracking of usage.	Legal and Secretarial Team	To review logs and reports generated by software or systems that track usage of licensed software or intellectual property and ensure that the usage data is accurate and comprehensive, covering all licensed assets.	Risk of unauthorized use of licensed software
Intellectual Property Rights	Patents and Copyrights	Misplacement or destruction of patent/copyright records.	Backup and disaster recovery procedures for IP records.	IT Department	To test the frequency of data backups to ensure that critical IP records are backed up at appropriate intervals, verify the integrity of backup data to ensure that it is not corrupted or compromised during the backup process and perform data restoration tests to confirm that IP records can be successfully	Risk of destruction of patent/copyright records.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
					recovered from backups.	
Intellectual Property Rights	Patents and Copyrights	Lack of Intellectual Property Policies and Procedures covering aspects such as ownership of and right to use the IP, Procedures for identification, evaluation, protection and management of IP, procedures for cooperation with third parties, guidelines on the sharing of profits from successful commercialization, etc.	Develop and implement clear IP policies and procedures and ensure employees are aware of and trained on IP policies.	Legal / CFO / Human Resource	To review IP policies and procedures to ensure they are well-documented, up-to-date, and comprehensive and verify that the policies comply with relevant intellectual property laws and regulations.	To ensure that there are policies and procedures for Intellectual Property

Business Continuity Plan

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Preparation, Review and Approval	Risk of not having a BCP and DRP document	The organization has a formally reviewed and approved BCP and DRP document	Information Technology Department.	Perform a comprehensive series of tests including evaluation of risk assessment process, business impact analysis, scope and dependency verification, alignment with business objectives, threat scenario simulation, documentation review, dependency mapping, personnel training, backup and recovery tool testing, communication plan validation, testing of recovery procedures, data integrity verification, alternate site activation testing, testing frequencies determination, third-party vendor testing, user acceptance	1. Risk assessment reports. 2. Business Impact analysis (BIA) Documentation. 3. Scope and dependency documentation. 4. Alignment with Business objectives 5. Threat scenario test results. 6. Documentation of plans.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
					testing, incident handling simulation, recovery documentation validation, and regulatory compliance checks to ensure the effectiveness, accuracy, and feasibility of BCP and DRP.	
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Testing of BCP and DRP	Risk of inadequate stakeholder engagement, misalignment with business objectives, lack of technical expertise, incomplete documentation, version control issues, overly complex plans, lack of accountability, scope changes, insufficient testing, limited review time, bias and conflict of interest, overlooked dependencies,	The organization's mitigation strategies encompass stakeholder involvement, regular updates, technical input, clear documentation, version control, ownership clarity, scope coverage, testing, unbiased review, compliance checks, effective communication, and change management approaches to ensure plan	Information Technology Department.	Perform tests including stakeholder engagement, business alignment validation, technical expertise assessment, documentation accuracy and completeness checks, version control verification, clarity and understandability evaluation, ownership assignment, scope consistency verification, effectiveness testing, adequate review time assessment, unbiased review evaluation, dependency mapping	1. Stakeholder feedback 2. Business alignment records. 3. Technical expert assessment reports. 4. Documentation completeness. 5. Version control records. 6. Regulatory compliance documentation. 7. Testing scenarios and plans. 8. Test scripts and procedures. 9. Test results. 10. Communicatio

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		regulatory compliance gaps, communication breakdown, and resistance to change. Risk of disruptions to production systems, inadequate test scenarios, failure to identify weaknesses, operational impact, data privacy violations, incomplete recovery, resource constraints, testing complexity, unpredictable outcomes, inaccurate assumptions, data corruption, lack of stakeholder involvement, insufficient documentation, and challenges with testing	quality and alignment. The organization plan carefully, involve stakeholders, ensure compliance, balance thoroughness, document processes, validate recovery strategies, analyse outcomes, and continually refine the plans based on testing results.		validation, regulatory compliance audit, communication effectiveness assessment, and change management testing to ensure the quality, accuracy, and alignment of BCP and DRP. Perform tests including tabletop exercises, functional testing, full-scale simulations, data recovery tests, communication tests, alternate site activation tests, load balancing/failover testing, performance testing, user access testing, resource availability tests, integration testing, data integrity testing, Recovery Time Objective (RTO) testing, documentation review, training assessment, scenario variability	n records. 11. Data Recovery documentation. 12. Backup and restoration records.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		complexity.			testing, management involvement testing, lessons learned analysis, and post-test evaluation.	
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Review and periodic updated of BCP and DRP	Risk of outdated information, incomplete documentation, unaddressed risks, non-compliance, lack of stakeholder involvement, inaccurate dependencies, unrealistic recovery objectives, complexity increase, time/resource constraints, inadequate testing, inconsistent version control, scope creep, change management challenges, and lack of awareness.	The organization's mitigation strategies involve structured review processes, ownership assignment, stakeholder involvement, thorough testing, regulatory alignment, resource prioritization, version control, clear communication, and continuous assessment of plans' relevance to evolving business needs and risks and ensured that the BCP and DRP document has been	Information Technology Department.	Perform tests including document review, scenario validation, dependency check, regulatory compliance, recovery objectives assessment, stakeholder involvement, risk assessment, testing plan review, communication protocol assessment, resource allocation test, training and awareness evaluation, change management assessment, version control check, complexity review, scalability assessment, business impact analysis update, lessons learned integration, and communication	1. Updated Documentation. 2. Documentation review logs. 3. Scenario Validation results. 4. Dependency verification 5. regulatory compliance documentation. 6. Stakeholder feedback records.

127

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
			aligned and updated periodically with version controls.		test to ensure the effectiveness, accuracy, and alignment of updated BCP and DRP processes with the organization's evolving needs.	
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Backup Policies and Procedures	Risk of Backup Policies and Procedures formulated are not in line with business requirements, leading to backup failures and loss of financial data.	The organization's Backup Policies and Procedures are formalized after formal risk assessment of Information Security (IS) threats and adhered for compliance. Business Process Owners and Information Technology (IT) functional heads are involved in determining what backup resources are required. Backup of all critical servers (application and database) are taken on a daily / weekly /	Information Technology Department.	Testing of backup policy and schedule within a BCP has to be performed, which is essential for ensuring the reliability of data recovery processes during disruptions. This involves regular tests like backup and restoration simulations, full system recovery trials and partial data restoration assessments. Additionally, the backup frequency, retention, offsite storage, encryption and notification procedures should be systematically tested. Incorporating scenario-based testing, documentation review and	1. Backup Policies and Procedures. 2. Policy Approval records. 3. Backup configuration records. 4. Testing records. 5. Backup notification records. 6. Backup Infrastructure documentation.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
			monthly basis. Backups are taken in a centralised server (primary server) or on a third-party infrastructure (cloud).		performance assessments, these tests validate the effectiveness of backup strategies under diverse circumstances.	
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Backup Schedules	Risk of financial data loss and resource strain due to frequent failures in backups, potential gaps in recovery points, and challenges in managing complex schedules. Risk of not balancing the need for data protection with resource limitations as longer backup intervals could increase the risk of significant data loss, while frequent backups might impact system performance and require	The organization implements robust controls for executing the backup schedule within a BCP which is imperative for ensuring data protection and efficient recovery. Automation tools are employed to schedule backups at defined intervals, reducing the risk of errors and ensuring consistency.	Information Technology Department.	Regular testing of backup integrity and recovery processes to be initiated and detailed documentation combined with a change management process helps track adjustments to the schedule. Aligning the backup schedule with recovery time objective and recovery point objective requirements are to be ensured for timely recovery without excessive data loss. Additional strategies involve implementing redundancy, offsite backups, encryption and monitoring storage capacity to support	1. Backup Logs. 2. Timestamps 3. Backup Reports. 4. Data Integrity checks. 5. Notification emails 6. Backup retention records.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		additional resources.			effective backup processes.	
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Monitoring of Backup failures and Action Taken	Risk of undetected backup failures, inadequate alerting, human error, and incomplete monitoring that could compromise data protection.	The organization's mitigation measures include implementing automated monitoring tools with proper alert configurations, regular training for personnel, comprehensive coverage of monitored systems, and well documented procedures for responding to failures and should implement fine-tune thresholds and tiered alerting.	Information Technology Department.	Preparation of detailed documentation of incidents and cross-training personnel mitigates risks of dependency and confusion. Technical glitches are managed by testing the monitoring tools and introducing redundancy. Perform tests to verify the accuracy and efficiency of backup failure monitoring and response processes within the BCP, including alert configuration, notification, escalation, coverage, personnel training, documentation, backup remediation, technical glitch handling, backup validation, dependency scenarios, alert fatigue assessment,	1. Alert Log and Reports. 2. Notification records. 3. Alert escalation records. 4. Personnel Actions Log 5. Incident Reports. 6. Documentation of procedures. 7. Training records.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
					performance impact analysis, incident trend analysis and audit trail review.	
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Re-run of Backup Job	Risk of data inconsistency, backup window overruns, resource overutilization, dependency on personnel, versioning and compatibility issues, increased risk of failure, overwriting existing backups, impact recovery point objectives, notification and monitoring challenges, documentation and auditing concerns and data privacy and security considerations.	The organization implement controls such as change management, version compatibility testing, data validation, resource allocation, testing environment, personnel availability, backup log review, verification, notification and monitoring, data retention, documentation, security measures, audit trails and regular testing to effectively manage risks associated with the "Rerun backup job" process in a BCP.	Information Technology Department.	Perform tests to verify the compatibility, data validation, backup verification, resource utilisation, notification, personnel availability, change management, documentation review, data retention, security and privacy, audit trail creation, personnel training, overwriting protection, impact assessment and incident handling tests to ensure effectiveness and reliability of the "Rerun backup job" within a BCP.	1. Rerun documentation. 2. Compatibility test results. 3. Data Validation reports. 4. Backup verification reports. 5. Resource utilisation reports
Business	Storage of	Risk of	The	Information	Perform tests to	1. Physical

131

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Backup Tapes - Onsite and Offsite	physical damage, single points of failure, limited accessibility, human error, transportation vulnerabilities, security concerns at offsite facilities, vendor reliability issues, longer recovery times, data privacy and compliance challenges, and the potential for unnoticed deterioration.	organization implements controls to secure physical data storage both onsite and offsite within a BCP. For onsite storage, utilizes fireproof storage, control access, ensures redundancy, and maintains proper labelling. For offsite storage, prioritizes secure transportation, assesses vendors rigorously, encrypts during transit, tracks the access, conducts audits, establishes data privacy agreements, defines retrieval protocols, and ensures redundancy.	Technology Department.	review general measures such as documentation, regular monitoring, testing restoration, personnel training, incident response plans, and physical security to safeguard data integrity and facilitate efficient recovery in alignment with the BCP.	Security Measures Documentation. 2. Climate Control Records. 3. Access control logs. 4. Vendor Agreements. 5. Secure transportation records. 6. Access logs.
Business	Restoration	Risk of data	The	Information	Perform	1. Restoration

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	of Backed up Data	integrity issues, data inconsistency, extended recovery times, application compatibility challenges, dependency complications, inadequate documentation, human errors, personnel unavailability, testing gaps, technical glitches, insufficient bandwidth, and security / compliance concerns.	organization's mitigation control involves robust testing, comprehensive documentation, personnel training, data validation, dependency management, redundancy planning, regular validation, technical resilience, and adherence to security and compliance protocols to ensure effective data recovery and minimized disruptions.	Technology Department	comprehensive tests including full and partial restoration, cross-system dependencies, data integrity checks, application compatibility, recovery time objectives assessment, documentation review, user acceptance, personnel availability, testing gap identification, technical glitch simulation, data volume evaluation, security/compliance validation, incident scenario simulation, and backup validation to ensure the reliability and effectiveness of data restoration within a BCP.	Test Reports. 2. Data Integrity verification. 3. Partial Restoration records. 4. Dependency test results. 5. Application compatibility reports.
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Evaluation of Restoration of Backed up Data from Offsite Storage	Risk of data integrity issues, inadequate testing, unreliable restoration, storage facility vulnerabilities, location	The organization implement controls to mitigate, ensure regular testing and updates, accurate documentation	Information Technology Department	Perform tests including data retrieval, integrity, restoration time, documentation review, facility access, environmental simulation, vendor assessment,	1. Testing plans. 2. Test results. 3. Data Retrieval logs. 4. Data Integrity verification. 5. Restoration time data.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		challenges, outdated documentation, untrained personnel, third-party dependency risks, communication gaps, lack of regular review, unplanned costs, data privacy concerns, loss of control, resource limitations, and testing constraints.	, due diligence with vendors, proper communication, geographical considerations, compliance review, personnel training, contingency planning, and integration with overall recovery testing.		personnel training evaluation, communication testing, documentation update verification, cost analysis, data privacy compliance check, contingency planning assessment, resource allocation test, and full recovery simulation to evaluate and ensure the effectiveness of the offsite storage process in a BCP.	6. Documentation assessment results.
Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)	Training and Awareness	Risk of including inadequate content, lack of customization, infrequent sessions, poor engagement, communication breakdown, personnel changes, overreliance on key individuals, misinterpreted procedures, lack of testing, resistance to change,	The organization's mitigation control ensures relevant, engaging, and regular training, effective communication, diverse participation, realistic scenarios, management endorsement, and continuous improvement based on feedback. The organization	Information Technology Department	Perform tests including knowledge assessments, scenario simulations, communication drills, role play exercises, tabletop exercises, evacuation drills, technology failure simulations, response time assessments, feedback collection, post-training surveys, documentation reviews, crisis communication	1. Training Attendance records. 2. Training materials. 3. Knowledge assessment results. 4. Scenario-based exercise reports. 5. Communication drill records. 6. Evacuation drill records.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested
		cultural / language barriers, unrealistic scenarios, inadequate management support, technology challenges, and incomplete evaluation.	implement controls such as customized training content, frequent sessions, engaging methods, clear communication, personnel change plans, diverse participation, crisis simulations, multi-language / cultural considerations, senior management involvement, feedback collection, training evaluation, documentation.		tests, leadership evaluations, decision-making assessments, and adaptability tests to thoroughly assess employees' preparedness and understanding within the training and awareness process of the BCP.	

Related Party Transactions

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested
Related Party Transactions	Entity level controls	Risk of non-identification of Related Parties	The Company Secretary (or equivalent in absence of a company secretary) should have a policy on identifying related parties including obtaining declaration from directors regarding their interests in companies and other business entities and the position they hold as directors or otherwise in other business entities.	Obtaining copies of the declaration by the Directors and whether the same have been discussed at the Board. Further, whether the list of related parties already existing are updated with any new updates from the directors.	a. Declaration given by Directors; b. Review by the Board of Directors through the Minutes of the Meeting; c. Updated list of Related Party
Related Party Transactions	Entity level controls	Risk of non-identification of Related Parties - Subsidiaries	A list of related parties-subsidiaries is prepared, and other documents related thereto. Transactions carried out with subsidiaries are properly recorded.	Review of the notes prepared by the Corporate Accounts Team to understand how they have identified entities as subsidiaries and the tests applied under AS 21 or under Ind AS 110 as the case may be.	Relationship with other entities.
Related Party Transactions	Entity level controls	Risk of non-identification of Related Parties - Associates	A list of related parties-Association is prepared, and other documents related thereto. Transactions carried out with Associations are properly recorded.	Review of the notes prepared by the Corporate Accounts Team to understand how they have identified entities as associates and the tests	Relationship with other entities.

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested
				applied under AS 23 or under Ind AS 28 as the case may be.	
Related Party Transactions	Entity level controls	Risk of non-identification of Related Parties - Jointly controlled entities or joint ventures	A list of related parties- Jointly controlled entities or joint ventures is prepared, and other documents related thereto. Transactions carried out with Jointly controlled entities or joint ventures are properly recorded.	Review of the notes prepared by the Corporate Accounts Team to understand how they have identified entities as associates and the tests applied under AS 27 or under Ind AS 28 as the case may be.	Relationship with other entities.
Related Party Transactions	Entity level controls	Risk of non-identification of Related Parties	Identification of related parties including as per Regulation 23 of SEBI LODR Guidelines	Review of the notes prepared by Company Secretary's team on applicability of SEBI LODR Guidelines and identification of additional related party transactions. Review of the minutes of the audit committee and Board of Directors.	Relationship with other entities.
Related Party Transactions	Transaction level	Risk of non-identification of Key Managerial Personnel (KMP) as	Identification of Key Managerial Personnel (KMP) as related parties.	Review of the appointment letters of the KMP, their roles and responsibilities	Nature of responsibilities

Final	Sub-process	Risk Description	Control	Test Performed	Attributes tested
		related parties		and conclusion drawn on whether they are related parties or not.	
Related Party Transactions	Transaction level	Approval for transactions with related parties	Ensuring compliance u/s 188 and Regulation 23 of SEBI LODR Guidelines	Review of the approvals by audit committee and Board of Directors.	Basis and copy of approvals.
Related Party Transactions	Transaction level	Transactions with related parties which are not approved	Review of the contracts (with copies of PO / Invoice / any other document) with related parties and ensuring that the contract terms are approved by the Board.	Review of the approvals by audit committee and Board of Directors.	Basis and copy of approvals.
Related Party Transactions	Transaction level	Transactions which are not at arm's length price.	Whether the company has reviewed the transactions with related parties and has done transfer pricing study to ensure that the prices charged are at arm's length price? To observe whether there are transactions which are abnormally over or under priced (Risk of Fraud and non-compliance).	Review of Transfer Pricing Study report and comparing the same with the contracts.	Pricing of the transactions with related parties.
Related Party Transactions	Transaction level	Transactions for Services rendered by family members.	Whether the transactions disclosed are as per AS 18 / Ind AS 24 (as the case may be)?	Review of the disclosures made in the financial statements / information submitted to regulatory authorities.	Disclosure required as per AS 18 / Ind AS 24 and as per financial statements / information.

Audit Conclusion

Final	Sub-process	Test Performed
Audit Conclusion	Review Audit Objectives and Scope	a) Verify whether the audit objectives set at the beginning of the audit have been met. b) Ensure that the audit scope was adhered to and any deviations are documented appropriately.
Audit Conclusion	Verify Audit Work	a) Cross-reference workpapers, evidence received, and audit documentation to ensure accuracy and completeness. b) Validate that audit procedures were performed are in accordance with the established standards and methodologies.
Audit Conclusion	Assess Materiality	a) Determine the thresholds for materiality used for assessing findings and their impact on the audit report. b) Confirm that identified issues and discrepancies meet the defined materiality criteria.
Audit Conclusion	Evaluate Internal Controls	a) Review the effectiveness of internal controls relevant to the audit objectives. b) Identify any weaknesses or deficiencies in internal controls and assess their impact on audit findings.
Audit Conclusion	Analyse Audit Findings	a) Summarize the audit findings, including significant issues and exceptions. b) Categorize findings based on their severity and potential impact. c) For each finding, identify the root cause and provide recommendations (based on industry best practices) to address the root cause.
Audit Conclusion	Obtain Management Responses	a) Communicate audit findings and recommendations to management personnel. b) Obtain management's responses to the audit findings, including any corrective actions planned or taken. c) Obtain the target timeline for corrective actions.
Audit Conclusion	Review Corrective Actions	a) Evaluate the adequacy of proposed/implemented corrective actions to address audit findings. b) Ensure that management's responses are aligned with the identified issues.
Audit Conclusion	Finalize the Audit Report	a) Compile audit findings, management responses, and supporting evidence into a comprehensive audit report. b) Ensure the report follows the organization's prescribed format and

			includes required sections.
		c)	Address any feedback or revisions required by the reviewer of the audit report.
		d)	Ensure that the audit report is clear, concise, and free of errors.
		e)	Circulate the finalized audit report to relevant stakeholders, including management, audit committee, and regulatory bodies as required.
Audit Conclusion	Review for Objectivity and Accuracy	a)	Verify that the audit report is unbiased, factual, and objective in its presentation.
		b)	Confirm whether all findings and conclusions are accurately portrayed and supported by evidence.
Audit Conclusion	Archive Documentation	Safely store all audit documentation, workpapers, and evidence for future reference and potential follow-up audits.	
Audit Conclusion	Post Audit Review	a)	Conduct a post-audit review to identify areas for improvement in the audit process.
		b)	Document findings to enhance future audit engagements.

PART B

Order to Cash – Manufacturing

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
Order to Cash	Customer Management	Customer chosen is not appropriate to complete the contract obligations resulting in bad debts.	Defined process to check the customer worthiness and approval from marketing head is needed for finalising customer. Credit worthiness process should include the following: Analysis of customers' latest available financial statements. Understanding customers' management and business. Personal guarantee. te visit. Reference Check. Evaluation of 4 C's of Credit	Check whether credit worthiness of all new credit customers has been evaluated by and documented for approval.	1. Credit Worthiness Supporting 2. Approval for customer.	Whether there are any customers where the credit worthiness is deteriorated after the contract.
		Proper documents not taken from customer at the time of onboarding.	Authorised Person approves onboarding of a new customer after reviewing data input with the supporting's attached with customer form. Documents needed with customer form- • GST Certificate • PAN card • E-mail ID	1. Check the customer hard file to test Customer form and other required data for onboarding	1. Customer Hard file	How many data fields or critical points in the customer file are empty or are not filled up for any reason?

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			• Contact Details • Bank details • Other details as required in Customer KYC Form Without necessary documents, no customer is onboarded.			
		Inaccurate/ Incomplete updation of customer master	1. Authorised person approves onboarding of a new customer after reviewing the data input with the supporting's attached with customer form. 2. Recorded changes to the customer master file are compared to authorized source documents to ensure that they were input accurately. 3. Customer master file data is periodically reviewed by management for accuracy and ongoing pertinence.	1. Check that the information so entered is reviewed by Authorised person. 2. Check with the supporting documents that the information has been completely & accurately entered.	1. Supporting documents 2. Approvals	
		Risk of inadequate screening viz. an employee being a customer.	Every employee is mandated to inform concerned division head/ Superior where conflict of interest exists. Employees are required to certify compliance with the	1. Check the employee declarations	Declarations by the employees. Check whether requirements of code of conduct and Companies Act, 2013 are fulfilled.	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			policy on an annual basis.			
		Unauthorised modifications/alterations made to customer master.	Customer master can be updated (modifications / Alterations) only with the approval of authorised person. Also, the access to make modification / alteration to the customer master is restricted to personnel authorised as per approval matrix.	1. Check that the person making the addition / alteration is authorised to do so 2. Check approval as per approval matrix.	1. Approvals for addition / alteration	Check whether log of changes is available.
		Inactive/ fictitious customers are not blocked.	Customer with no transactions for a period specified as per organisation policy are blocked in ERP/Accounting Package for further sales with approval of authorised person	1. Check the customer master for blocked customers.	1. Customer Ledgers 2. Customer Master	
		Unauthorised reopening of customer blocked earlier.	Block customer accounts can only be opened again after taking approval as per approval matrix.	1. Check list of blocked customer account reopened 2. Verify proper approvals have been taken.	1. Customer Master 2. Approval logs	
	Annual Target	Annual Targets are not prepared, no proper planning leading to loss of revenue.	An annual target is developed for defining the sales for each year. Targets are duly approved by	Check whether annual sales budget is prepared and approved as per	Approved Sales Budget	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			the authorised personnel management/ Board.	the authority matrix		
		Annual targets are not being achieved.	Every month, meeting of Division head with Marketing team is held to keep the annual sales target on track. At period end, reasons are identified for variances in actual sales with budgeted sales and same is considered while formulating plan for the next year.	Review Minutes of Meeting	Minutes of meetings	
	Order Manageme nt	Product prices catalogue is not approved by authorized person.	The pricing of each product is decided by the Management with Division heads considering costing and other factors and the same is defined in the ERP/ Accounting Package. Also, the prices are reviewed by the management on a regular basis, and changed, if required.	Check approved price list Verify changes made are properly authorized.	Price List	
		Unauthorized quotations send to customer.	Authorised personnel prepare and record the quotation in the ERP/ Accounting Package, the quotation is approved by Approving authority as per	Check whether the quotations are approved properly as per the authority matrix	Quotations	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			authority matrix and shared to customer.			
		Unauthorized discount allowed to the customers	Data validation is done in the ERP/ Accounting Package so that the personnel inputting days cannot enter the price below than allowed limit Further Approval as per approval matrix is required to quote a rate/price to customer.	Check whether the pricing of sales orders is according to the price list. Verify discounts have been approved from as per approval matrix.	Price List Sales orders Approvals for discount	
		Quotations not shared with customer within time	Customer inquiry for quotations is input by sales team in ERP/Accounting Package. Delayed quotation is time flagged in ERP/Accounting Package. Quotations as made are required to be, approved and shared to customer within 2 Days of receipt of inquiry of quotations.	Verify quotations are being with time specified as per Organisation policy.	Quotations Listing	
		Signed purchase order/agreement not obtained and sales process started	The sales executive shall ask for the customer to share the approved purchase order/ agreement, or in absence of P.O, he shall prepare the Performa invoice after onboarding of	Check proper supporting attached with sales order raised. Also, check the sale order is not issued until PO/agreement/ Performa	Purchase order/ agreement received from customer	

147

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			customer into ERP/Accounting Package and get it signed & stamped by the customer. Further, work is not started until sales order is made.	invoice not received.		
		Sales order is not entered or incorrectly entered in the system with respect to rate, quantities & other terms or duplicates orders are entered.	Sales orders are to be reviewed (with respective purchase order/agreement) and approved as per authority matrix. Further, Invoices are linked to sales order, invoices can't be issued without sales order.	Check sales orders are approved as per authority matrix.	Authority Matrix Approvals for sales order	
		Sales order/agreement does not prescribe the correct technical specifications of goods required resulting in procurement of incorrect goods	Specifications are mandatory field in the sales order and cannot be circumvented (in ERP/Accounting Package). Sales agreement is approved by approving authority after proper review.	Check sales orders are prepared with all specifications necessary and match the sale order specification with customer's purchase order	Sales order	
		Delay in approving sales order	The sales order created should be approved within time specified as per organisation policy. Unapproved sales order are time flagged on dashboard of approving authority.	Verify sales orders are approved within time limit specified.	Authority Matrix Organisation policy Approvals for sales order	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		Unauthorized modification/cancellation of sales order/agreement	Request for modification/cancellation of sales order/agreement is raised in ERP/ Accounting Package, and after approval as per authority matrix, the request is closed.	Check sales orders are modified/ cancelled as per authority matrix	Authority Matrix Approvals for sales order	
		No process of closing/ blocking the old sale order in the ERP automatically	In case, sales order has not been completed within time agreed, the sales order is closed. Customer has to apply to the Organisation for new order for the unexpired quantity.	Check sales orders are closed after time limit specified in sales order has passed.	Listing for Sale orders	
	Credit Management	Credit policy is not in place / Unapproved credit policy is formulised	Approved credit policy is in place and all the customers are given credit as per the policy only. Same is also mentioned on invoice.	Check whether credit policy is formulated	Approved Credit Policy	
		Unauthorized changes in credit limit, period and terms of a customers	Credit limits are defined in ERP/Accounting Package, any modifications made are to be approved as per authority matrix	Check changes in credit limit are authorised as per authority matrix	Authority Matrix Approved Credit Limit	
		Unauthorized credit allowed to customers.	Credit Limit Matrix have been defined for allowing credit period to the clients in Credit Policy.	Check credit limit matrix is prepared and approved	Approved Credit Limit Matrix	

149

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		Delivery order has been generated by the system and the customers trade debts exceed their credit terms/ limits.	Credit Limits are linked to customer account in ERP/ Accounting Package, for exceeding credit limits, prior approval has to be taken as per authority matrix	Check whether credit limits are breached during the year. If exceeded, Check whether prior approvals were taken.	Data for credit given to customer during the year	
	Order Fulfilment	Quality of the goods delivered not in line with the requirement of the customer	1. Person responsible shall regularly follow-up with the production team for the purpose of quality of goods to be delivered. 2. Before loading of material, the quality team and sales team shall check the quality of material on a random basis and shall share the quality inspection report to the dispatch/document team.	Check reports of quality team issued during the year.	Quality Reports	
		Delivery not made to customer within time	Sales order validity is mentioned in the sale order at the time of creation of sale order and the same is monitored by the authorized personnel to make all deliveries timely.	Check whether sales are made to customer within time specified in sales order.	Outward Register E-Way Bails Sale Orders	
		Customers do not receive dispatched products leading to customer dispute	1) Delivery challan to be taken from transporter. 2) Goods receipt note / material	Check whether acknowledgeme nts has been received from customers and	Acknowledgemen t from customer. Delivery Challan. Invoice.	Customer confirmation obtained where Acknowledgem ent from

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			receipt note as confirmation is taken from respective customer through mail.	delivery challans are available.		customer is not available
	Order Shipping	Goods are dispatched more than sales order quantity	a. Items are dispatched on the basis of sales order issued by sales and marketing department. b. Inventory Personnel ensure that items are not issued more than the sales order quantity of customer. c. Goods are loaded in the vehicle in the presence of security, marketing executive, and inventory personnel.	Verify dispatch order/packing list with sales order	Dispatch order/packing list Invoice Sale order	
		Shipping is made without obtaining advance payment	Sale order is not generated until advance is not received as per PO/agreement/proforma invoice.	Verify advances have been received as per the sale agreements/sale order. Also check that no sale order is generated until advance received.	Bank Statement Sale order/Agreement	
		Invoicing & dispatch documents are generated but products are not dispatched	Invoice and dispatch documents are generated after the dispatch team has loaded the goods on vehicle.	Reconcile Invoices with E-way bills	Invoice E-way bills	

151

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		Invoice generated and goods dispatched are not in line with customer order	Based on marketing team communication, packaging list is prepared, and goods are identified and made ready for dispatch by stores team. Goods dispatched note is prepared by stores in charge and goods are loaded in vehicle in presence of stores in charge & security in charge. Based on packaging list and goods dispatch note, invoicing is done.	Match Invoice generated with sales order issued and PO/agreement to customer	Invoice Sale order	
		Delivery is made without sale order	Invoice is linked with sales order. Inventory team issues the inventory to dispatch team after recovering approved sales order form sales team.	check that Invoices have been linked to sales order	Invoice Sale order	
		Dispatched Goods have not been input/ incorrectly input in outward register maintained at factory/company gate	Security in charge checks outward registers are updated before dispatch of goods from gate. Security supervisor on regular intervals checks registers are updated timely and correctly.	Verify Dispatch goods have input in outward register	Invoice Outward register	
	Customer Invoicing	Dispatch is done without issuing invoice.	Goods are not exiting the factory gate before the issue of Invoice and other	Match the outward register with invoice and dispatch	Outward register Dispatch register invoices	

152

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			dispatch documents.	register.		
		Invoice is not as per dispatch order/packaging list.	Dispatch team and Security in charge scrutinises the dispatch order/packaging list with invoice and ensure both are in line.	Verify Invoices issued during the year with their respective dispatch order/packaging list	Invoices Dispatch order/packaging list	
		Invoicing is not in line with statutory requirements	Predefined format for invoice has been made in ERP/Accounting Package after approval of authorised personnel. The same is regularly reviewed by FP&A team.	Check the format of Invoice is in line with statutory requirements	Invoices Refer respective law	
		Invoice generated with incorrect statutory details (Like HSN, Place of supply, GST Rate, etc.)	Invoices are prepared by authorised person, and invoice is reviewed and approved by the authorised signatory	Check correct statutory details are filled for invoices issued during the year	Invoices Refer respective law	
		Invoices raised on unauthorized/incorre ct rates.	Invoices are linked with sales order (agreed earlier with the customer). Rates and other terms are pre-specified in invoices as per sales order.	Verify invoices are matching with sales order linked to it	Invoice Sale order	
		Invoices not generated and delay in generating the invoice.	For every sale, packaging list, goods dispatch note & invoice is created. Without packaging	Verify Packaging list/ Goods dispatch note/order with Invoice issued	Invoice Packaging list/ Goods dispatch Data	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			list & invoice, goods loaded vehicle is not allowed to exit factory gate.	during the Year.		
		E-way bill generated not in line (incorrect item, rates, quantity, etc.) with the invoice issued.	Dispatch team and Security in charge scrutinises the dispatch documents like invoice, e-way bill, etc and ensure all are matching with one-another.	Reconcile Invoices with E-way bills	Invoice E-way bills	
		Cash sales made not recorded/ under recorded.	Invoice/cash receipts are to be issued from ERP/Accounting Package for cash sales and monthly reconciliation is made of invoice generated with cash deposit by authorised personnel.	Check invoices is issued from ERP and monthly reconciliation is made or not	Invoices Cash Receipts Reconciliation	
		Cash received not deposited in bank within time as per Organisation policy.	Cash received should be deposited at the branch office as per the Organisation policy. Responsible Personnel should reconcile it with ERP/Accounting Package receipts and issue acknowledge-ment. Responsible Personnel should deposit the cash in bank daily basis/ next working day.	Check cash is deposited within time as per the Organisation policy and reconciliation is done for cash receipt at branch. Verify cash received for sales during year has been deposited in bank.	Bank Deposit Slips Cash Reconciliations	

154

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
	Sales Return and Refund	Policy has not been formulated for Sales return and refund.	Approved policy has been defined for Sales Return and Refund.	Check sales return and refund policy	Sales Return and Refund policy	
		Sales return request accepted without proper approvals	Authorised matrix has been defined for approval of sales return request	Check proper approvals have been taken for approving sales return request.	Approval for sales return	
		Unauthorised/ improper Credit notes is issued	1) Approval as per approval matrix is taken for issue of the credit note through mail/ERP/Accounting Package by personnel responsible. 2) After approval, the credit notes are prepared by personnel responsible and shared to customer.	Check approvals for Credit notes issued during the year	Credit Notes register/ledger	
		Sales returns are incorrectly recorded (Quantities, Rate etc.) or accounted without physically receiving goods	1) After arrival of vehicle at warehouse/factory, goods are checked by quality team. Report is issued and goods are forwarded to inventory team. 2) Inventory team inputs the goods in register and raises material receipt note. 3) After issue of MRN and approval from Division head, sales return entry is	Check Report issued by quality team for returned goods, MRN generated by Inventory team and approval of Division head for Sales Return.	Quality team report MRN for Returned Goods Approval as per approval matrix.	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			passed in books.			
		Refund of sales return made to incorrect customer	Bank account is updated in the ERP/accounting package. Before refund, approval as taken per the approval matrix.	Check approval received as per approval matrix	Approval	
	Accounts Receivable	No policy for periodical customer balance reconciliation / Incorrect customer balance reflected in books of accounts	Account statements for all customers has been obtained on quarterly basis and reconciliation is prepared by person responsible. Further, balance confirmations are obtained from all customers on yearly basis.	Check whether accounts statement are obtained as per Organisation policy.	Accounts Statements/Bala nce confirmations from customers	
		Identified discrepancies during reconciliation with customer are not adjusted correctly in the books of accounts	Identified deviations are reconciled by responsible accounting personnel and reviewed by approving authority. Adjustment is entered in Accounting Package after approved by approving authority.	Check whether there is any discrepancy between customer statements and Organisation ledgers. Check identified discrepancy are resolved and adjusted in necessary books after approvals as per authority matrix	Accounts Statements/Bala nce confirmations from customers Customer Ledgers Approvals for adjusting entries	
		Revenue is recorded in books for goods	Revenue for Goods sent on approval is	Check conditions as	Revenue Recognition	

156

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		sent on approval, but approval not received from customers.	recorded when i) The goods have been formally accepted by the buyer, or ii) The buyer has done an act adopting the transaction, or iii) The time period for rejection has elapsed or where no time has been fixed, a reasonable time has elapsed.	mentioned in Organisation policy are satisfied before booking revenue for "Goods Sent on Approval".	Policy Data for Goods Sent on Approval. Book entry	
		Provision for bad & doubtful debt is not made or made using incomplete and inaccurate data or not correctly accounted for in the books of accounts	Organisation has defined policy for creation of provision for doubtful debts. Ageing for debtors is prepared. Provision for doubtful debts is approved by Chief Financial Officer & provision is entered in accounting package by responsible accounting personnel and approved by approving authority to take legal advice for collecting the dues and filing suits.	Check whether policy is formulated for recording of doubtful debts and ageing is prepared regularly. Verify necessary approvals as per authority matrix have been received for recording provision for doubtful debts.	Policy for provisions. Customer Ageing. Approvals for recording provision for doubtful debts	
		Debtors written off without approval	The Accounts receivable team share the list of customers who have not made the payment to Division	Check the bad debts in the ERP with the share list by the authorised person.	Bad debts ledger Trail mail/Supporting's for bad debts by authorised person	

157

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			heads and CFO. Decision is taken to written off the balance and the same is shared to authorised personnel to pass the entry in the ERP/Accounting Package.			
	Payment Collections	Regular delay in collecting payments from customers.	Monthly aging is extracted from ERP/Accounting Package by marketing team and regular follow up is done with the customer whose payment is due.	Check that regular follow up is done with customer whose payment is due	Aging Follow up mail	
		Cheque received but not deposited in Bank	1) Cheques received are collected by the marketing team and forwarded to accounts department, and cheque is deposited in bank on the same day or next working day. 2) Monitoring of cheque deposit being done on regular basis.	Check the deposit slip with entry in the ERP	Receipts data Deposit slip	
		Cheque deposited in bank but not accounted	After receiving the cheque from the marketing team, entry is made in ERP/Accounting Package on the same day or next	Check organisation books are matching with bank statements, and daily bank	Bank Ledgers Bank Statements Reconciliation	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			working day. BRS is also prepared and monitored on daily basis,	reconciliation statements are being made		
		Collections are recorded incorrectly in the books with respect to amount, period or customer account.	Collection is recorded in ERP/Accounting Package and approved by authorised person after verification of supporting document. Further, reconciliation is performed for bank ledger & bank statement and deviations are recorded accordingly.	Check bank reconciliations are prepared, and appropriate journal entries are passed as per reconciliation	Bank Reconciliation Statements	
		Incorrect calculation is done for the interest accrued on the outstanding receivable balance.	Interest on defaulting companies is to be calculated on the basis of a fixed percentage as per approved policy and same is to be approved by the authorised person.	Check whether the sales proceeds have been realised within the time limit as per the as per credit given to customer. Obtain collection date & invoicing date for all invoice and verify interest has been charged on defaulting companies	Customer Ageing Invoice Receipts data interest working	
	Reporting and Data Manageme	Revenue is not recognized as per applicable AS /	Organisation has defined revenue recognition policy in	Ensure that an appropriate, consistent	Revenue Recognition	

159

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
	nt	organisation policy	compliance with applicable accounting standard.	revenue recognition policy is applied at the year end. Ensure that the policy adopted is in line with generally accepted accounting principles. Compare the Organization's policy for accounting sales with the significant accounting policies mentioned in the Notes to the Accounts.	Policy	
		Transactions have been recorded in incorrect period.	Monthly sales invoices, GST returns, e-way bill & sales data as per accounting package are reconciled by person responsible, to ensure no invoice is omitted to be recorded and recorded in the current financial period/ year. Reconciliation are approved by authorised person.	Check Revenue is recorded in correct period and apply cut-off procedures for testing.	Sales Data GST Returns Invoice Data Reconciliation	
		Fictitious /duplicate sales are recorded in	All invoices are to be authorised/ approved	Check that invoices are	Approved invoices	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		the books of accounts.	from Authorised Signatory. Further all entries are approved as per approval matrix.	approved from authorised signatory and entries are approved as per approval matrix.	Ledger of sale	
		Sales transactions are not properly classified in accounts	Sales entry is passed by person responsible, and it is approved by authorised person.	Scrutinise sales ledgers on overall basis, and check sales are recorded in correct ledgers.	Sales Schedule Sale leger	
		Benefits for export sales not availed/ under availed by the Organisation.	Export incentive working is prepared, and it is reviewed by authorised person.	Check trail mail/supporting's of approval as per approval matrix.	Working of export incentive Trail mail	
		Export sales are recorded at incorrect foreign exchange rate.	All export sales are recorded at same day prevailing CBEC website rate. Sales entry is passed as per accounting manual.	Check export sale made are recorded at rates as specified by accounting manual	Export sale ledger Invoice CBEC rates	
		Accounting for exempt sales is done incorrectly in books of account.	Separate expense and revenue ledgers are made related to exempt sales for compliance with applicable tax laws	Check accounting for exempt sale and taxable sale in books	Books of Account	
	Customer Evaluation	No policy has been formed for evaluation of customer.	Approved Policy for evaluation of customer has been formed.	1. Obtain policy of customer evaluation	Customer Evaluation Policy	
		Customer evaluations are not being performed regularly.	The Customer Evaluation is done as per policy. Marketing and Finance team is responsible for doing	Check whether customer evaluations are being performed, and	Customer Evaluation forms/report	

Proces s	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			the customer evaluation. Based on the same and subsequent discussions with the approving authorities, Sales depart-ment revises the approved customer list and block customers as per evaluations list.	approved customer list is updated as per the evaluations		
	Customer Complaints	No policy has been for handling of customer complaints.	Approved Policy for handling customer complaints has been formed.	1. Obtain policy of handling customer complaints	Customer Policy	
		Policy made for handling of customer complaints not complied.	Authorised levels are formulated for handling a customer complaint, regular monitoring is done to ensure customer complaints are handled as per policy by authorised personnel.	1. Check for compliance with the policy for handling customer complaints.	Customer Policy Complaint Log	
		Timely redressal of customer complaints not done.	Authorised person as per policy handles customer complaints and take appropriate action. Regular monitoring is done for status of customer complaints by authorised personnel as per company policy.	1. Check status of customer complaints. 2. Report complaints which have not been resolved in time specified as per Organisation policy	Complaint Log	

Order to Cash – Services

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
Order to Cash	Customer Management	Customer chosen is not appropriate to complete the contract obligations resulting in bad debts.	Defined process to check the customer worthiness and approval from marketing head is needed for finalising customer. Credit worthiness process should include the following: Analysis of customers' latest available financial statements. Understanding customers' management and business. Personal guarantee. Reference Check. Evaluation of 4 C's of Credit	Check whether credit worthiness of all new credit customers has been evaluated by checking company's financial heath, credit's history, edit rating report and documented for approval.	1. Credit Worthiness Supporting 2. Approval for customer.	
		Proper documents not taken from customer at the time of onboarding.	Authorised Person approves onboarding of a new customer after reviewing data input with the supporting's attached with customer form. Documents needed with customer form – GST Certificate PAN card E-mail ID	1. Check the customer hard file to test Customer form and other required data for onboarding	1. Customer Hard file	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			Contact Details Bank details Other details as required in Customer KYC Form Without necessary documents, no customer is onboarded.			
		Inaccurate/Incomplete updation of customer master	1. Authorised person approves onboarding of a new customer after reviewing the data input with the supporting's attached with customer form. 2. Recorded changes to the customer master file are compared to authorized source documents to ensure that they were input accurately. 3. Customer master file data is periodically reviewed by management for accuracy and ongoing pertinence.	1. Check that the information so entered is reviewed by Authorised person 2. Check with the supporting documents that the information has been completely & accurately entered	1. Supporting documents 2. Approvals	
		Risk of inadequate screening viz. an employee being a customer.	Every employee is mandated to inform concerned division head/ Superior where conflict of interest exists. Employees are required to certify compliance with the	1. Check the employee declarations	Declarations by the employees Check whether requirements of code of conduct and Companies Act, 2013 are fulfilled.	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			policy on an annual basis.			
		Unauthorised modifications/alterations made to customer master.	Customer master can be updated (modifications/ Alterations) only with the approval of authorised person. Also, the access to make modification/ alteration to the customer master is restricted to personnel authorised as per approval matrix.	1. Check that the person making the addition/ alteration is authorised to do so 2. Verify customer approval forms are approved as per approval matrix.	1. Approvals for addition/ alteration	
		Inactive/ fictitious customers are not blocked.	Customer with no transactions for a period specified as per organisation policy are blocked in ERP/ Accounting Package for further sales with approval of authorised person.	1. Check the customer master for blocked customers.	1. Customer Ledgers 2. Customer Master	
		Unauthorised reopening of customer blocked earlier.	Block customer accounts can only be opened again after taking approval as per approval matrix.	1. Check list of blocked customer account reopened 2. Verify proper approvals have been taken.	1. Customer Master 2. Approval logs	
	Annual Target	Annual Targets are not prepared, no proper planning leading to loss of revenue.	An annual target is developed for defining the sales for each year. Targets are duly approved by the authorised personnel	Check whether annual sales budget is prepared and approved as per the	Approved Sales Budget	

165

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			management.	authority matrix.		
		Annual targets are not being achieved.	Every month, meeting of Division head with Marketing team is held to keep the annual sales target on track. At period end, reasons are identified for variances in actual sales with budgeted sales and same is considered while formulating plan for the next year.	Review Minutes of Meeting	Minutes of meetings	
	Order Management	Service prices catalogue is not approved by authorized person.	Pricing of each service is decided by the Management with Division heads and the same is defined in the ERP/Accounting Package. Also, the prices are reviewed by the management on a regular basis, and changed, if required.	Check approved service price list Verify changes made are properly authorized.	Price List	
		Absence of pricing policy/review of pricing policy leading to sale of services below the incurred cost.	Pricing policy is maintained/updated regularly for all services offered by the organization.	Check whether the proper pricing policy for services has been made or not.	Pricing Policy	
		Unauthorized quotations send to customer.	Authorised personnel prepare and record the quotation in the ERP/Accounting Package, the quotation is approved by	Check whether the quotations are approved properly as per the authority matrix	Quotations	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			Approving authority as per authority matrix and shared to customer.			
		Unauthorized discount allowed to the customers.	Data validation is done in the ERP/Accounting Package so that the personnel inputting days cannot enter the price below than allowed limit. Further Approval as per approval matrix is required to quote a rate/ price to customer.	Check whether the pricing of sales orders is according to the price list. Verify discounts have been approved from as per approval matrix.	Price List Sales orders Approvals for discount	
		Quotations not shared with customer within time.	Customer inquiry for quotations is input by sales team in ERP/Accounting Package. Delayed quotation is time flagged in ERP/ Accounting Package. Quotations madeis required to be approved and shared to customer within 2 Days of receipt of inquiry of quotations.	Verify quotations are being with time specified as per Organisation policy	Quotations Listing	
		Signed purchase order/agreement not obtained and sales process started	The sales executive shall ask for the customer to share the approved purchase order/ agreement, or in absence of P.O, he shall prepare the Performa invoice after onboarding of customer into ERP/	Check proper supporting attached with sales order raised.	Purchase order/agreement received from customer	

167

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			Accounting Package and get it signed & stamped by the customer. Further, work is not started until sales order is made.			
		Sales order is not entered or incorrectly entered in the system with respect to rate, quantities & other terms or duplicates orders are entered.	Sales orders are to be reviewed (with respective purchase order/agreement) and approved as per authority matrix. Further, Invoices are linked to sales order, invoices can't be issued without sales order.	Check sales orders are approved as per authority matrix	Authority Matrix Approvals for sales order	
		Sales order/ agreement does not prescribe the correct technical specifications of services required resulting in rendering of incorrect services	Specifications are mandatory field in the sales order and cannot be circumvented (in ERP/ Accounting Package). Sales agreement is approved by approving authority after proper review.	Check sales orders are prepared with all specifications necessary and match the sale order specification with customer's purchase order	Sales order	
		Delay in approving sales order	The sales order created should be approved within the time specified as per organisation policy. Unapproved sales order is time flagged on dashboard of approving authority.	Verify sales orders are approved within time limit specified.	Authority Matrix Organisation policy Approvals for sales order	
		Unauthorized	Request for	Check sales	Authority Matrix	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		modification/cancellation of sales order/agreement	modification/cancellation of sales order/agreement is raised in ERP/ Accounting Package, and after approval as per authority matrix, the request is closed.	orders are modified/ cancelled as per authority matrix.	Approvals for sales order	
		No process of closing/ blocking the old sale order in the ERP automatically	In case, sales order has not been completed within time agreed, the sales order is closed. Customer has to apply to the Organisation for new order for the unexpired quantity.	Check sales orders are closed after time limit specified in sales order has passed.	Listing for Sale orders	
	Credit Management	Credit policy is not in place / Unapproved credit policy is formulized.	Approved credit policy is in place and all the customers are given credit as per the policy only. Same is also mentioned on invoice.	Check whether credit policy is formulated.	Approved Credit Policy	
		Unauthorized changes in credit limit, period and terms of a customers.	Credit limits are defined in ERP/Accounting Package, any modifications made are to approved as per authority matrix.	Check changes in Credit limit are authorised as per authority matrix.	Authority Matrix Approved Credit Limit	
		Unauthorized credit allowed to customers.	Credit Limit Matrix have been defined for allowing credit period to the clients in Credit Policy.	Check Credit limit matrix is prepared and approved.	Approved Credit Limit Matrix	
		Services has been performed and the customers trade debts	Credit Limits are linked to customer account in ERP/Accounting	Check whether credit limits are breached	Data for credit given to customer during	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		exceed their credit terms/ limits.	Package, for exceeding credit limits, prior approval has to be taken as per authority matrix.	during the year. If exceeded, Check whether prior approvals were taken.	the year	
	Order Fulfilment	Services provided not in line with the requirement of the customer	1. Engagement team is briefed at the commencement of a service. Regular reviews meetings are held to ensure the services are performed timely and as per customers requirement	Check reports of quality team issued during the year.	Quality Reports	
		Services not rendered to customer within time	Service order validity is mentioned in the service order at the time of creation of service order and the same is monitored by the authorized personnel to make all services timely.	Check whether services are provided to customer within time specified in Sales order.	Outward Register Service Orders	
	Customer Invoicing	Invoices not generated and delay in generating the invoice.	After service has been performed, Engagement team informs the Finance team and invoices is raised within 2 days.	Verify Invoices has been issued within approved time as per policy.	Invoice	
		Invoicing is not in line with statutory requirements	Predefined format for invoice has been made in ERP/Accounting Package after approval of authorised personnel. The same is regularly reviewed by FP&A team.	Check the format of Invoice is in line with statutory requirement.	Invoices Refer respective law	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		Invoice generated with incorrect statutory details (Like HSN, Place of supply, GST Rate, etc.)	Invoices are prepared by authorised person, and invoice is reviewed and approved by the authorised signatory.	Check correct statutory details are filled for invoices issued during the year.	Invoices Refer respective law	
		Invoices raised on unauthorized/ incorrect rates.	Invoices are linked with sales orders (agreed earlier with the customer). Rates and other terms are pre-specified in invoices as per sales order.	Verify Invoices are matching with sales order linked to it.	Invoice Sale order	
		Cash sales made not recorded/ under recorded.	Invoice/cash receipts are to be issued from ERP/ Accounting Package for cash sales and monthly reconciliation is made of invoice generated with cash deposit by authorised personnel.	Check invoices is issued from ERP and monthly reconciliation is made or not.	Invoices Cash Receipts Reconciliation	
		Cash received not deposited in bank within time as per Organisation policy.	Cash received should be deposited at the branch office as per the Organisation policy. Responsible Personnel should reconcile it with ERP/Accounting Package receipts and issue acknowledge-ment. Responsible Personnel should deposit the cash in bank daily basis/ next working	Check cash is deposited within time as per the Organisation policy and reconciliation is done for cash receipt at branch. Verify cash received for sales during year has been deposited in	Bank Deposit Slips Cash Reconciliations	

171

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			day.	bank.		
	Sales Return and Refund	Policy has not been formulated for issuing credit notes.	Approved policy has been defined for Credit notes.	Check credit notes policy.	Credit Note Policy	
		Credit note request accepted without proper approvals	Authorised matrix has been defined for approval of credit note request	Check proper approvals have been taken for approving credit note request.	Credit Notes	
		Unauthorised/ improper Credit notes is issued	1) Approval is taken as per approval matrix for issue of the credit note through mail/ERP/Accounting Package by personnel responsible. 2) After approval, the credit notes are prepared by personnel responsible and shared to customer.	Check approvals for Credit notes issued during the year.	Credit Notes register/ledger	
		Refund of sales return made to different customer	Before refund, approval as taken per the approval matrix.	Check approval received as per approval matrix.	Approvals	
	Accounts Receivable	No policy for periodical customer balance reconciliation / Incorrect customer balance reflected in books of accounts.	Account statements for all customers has been obtained on quarterly basis and reconciliation is prepared by person responsible. Further, balance confirmations are obtained from all customers on yearly basis.	Check whether accounts statement are obtained as per Organi-sation policy.	Accounts Statements/ Balance confirmations from customers.	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
		Identified discrepancies during reconciliation with customer are not adjusted correctly in the books of accounts.	Identified deviations are reconciled by responsible accounting personnel and reviewed by approving authority. Adjustment is entered in Accounting Package after approved by approving authority.	Check whether there is any discrepancy between customer statements and Organi-sation ledgers. Check identified discrepancy are resolved and adjusted in necessary books after approvals as per authority matrix.	Accounts Statements/Balance confirmations from customers Customer Ledgers Approvals for adjusting entries.	
		Provision for bad & doubtful debt is not made or made using incomplete and inaccurate data or not correctly accounted for in the books of accounts.	Organisation has defined policy for creation of provision for doubtful debts. Ageing for debtors is prepared. Provision for doubtful debts is approved by Chief Financial Officer & provision is entered in accounting package by responsible accounting personnel and approved by approving authority.	Check whether policy is formulated for recording of doubtful debts and ageing is prepared regularly. Verify necessary approvals as per authority matrix have been received for recording provision for doubtful debts.	Policy for provisions. Customer Ageing. Approvals for recording provision for doubtful debts.	
		Debtors written off without approval	The Accounts receivable team share the list of customers who have not made the	Check the bad debts in the ERP with the share list by	Bad debts ledger Trail mail/ Supportings for	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			payment to Division heads and CFO. Decision is taken to written off the balance and the same is shared to authorised personnel to pass the entry in the ERP/Accounting Package.	the authorised person.	bad debts by authorised person	
	Payment Collections	Regular delay in collecting payments from customers.	Monthly aging is extracted from ERP/Accounting Package by marketing team and regular follow up is done with the customer whose payment is due.	Check that regular follow up is done with customer whose payment is due.	Aging Follow up mail	
		Cheque received but not deposited in Bank.	1) Cheques received are collected by the marketing team and forwarded to accounts department, and cheque is deposited in bank on the same day or next working day. 2) Monitoring of cheque deposit being done on regular basis.	Check the deposit slip with entry in the ERP.	Receipts data Deposit slip	
		Cheque deposited in bank but not accounted.	After receiving the cheque from marketing team, entry is made in ERP/Accounting Package on the same day or next working day. BRS is also prepared and monitored on daily	Check Organisation books are matching with bank statements, and daily bank reconciliation statements are	Bank Ledgers Bank Statements Reconciliation	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			basis.	being made.		
		Collections are recorded incorrectly in the books with respect to amount, period, or customer account.	Collection is recorded in ERP/Accounting Package and approved by authorised person after verification of supporting document. Further, reconciliation is performed for bank ledger & bank statement and deviations are recorded accordingly.	Check Bank Reconciliations are prepared, and appropriate journal entries are passed as per reconciliation.	Bank Reconciliation Statements	
		Incorrect calculation is done for the interest accrued on the outstanding receivable balance.	Interest on defaulting companies is to be calculated on the basis of a fixed percentage as per approved policy and same is to be approved by the authorised person.	Check whether the sales proceeds have been realised within the time limit as per the Organisation's policy. Obtain collection date & invoicing date for all invoice and verify interest has been charged on defaulting companies.	Customer Ageing Invoice Receipts data Interest calculation.	
	Reporting and Data Management	Revenue is not recognized as per applicable Accounting Standards / organisation policy.	Organisation has defined revenue recognition policy in compliance with applicable accounting standard.	Ensure that an appropriate, consistent revenue recognition policy is applied at the year end.	Revenue Recognition Policy	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
				Ensure that the policy adopted is in line with generally accepted accounting principles. Compare the Organisation's policy for accounting sales with the significant accounting policies mentioned in the Notes to the Accounts.		
		Transactions have been recorded in incorrect period.	Monthly sales invoices, GST returns & sales data as per accounting package are reconciled by person responsible, to ensure no invoice is omitted to be recorded and recorded in the current financial period/ year. Reconciliation are approved by authorised person.	Check Revenue is recorded in correct period and apply cut-off procedures for testing.	Sales Data GST Returns E-Way Invoice Data Reconciliation	
		Fictitious /duplicate sales are recorded in the books of accounts.	All invoices are to be authorised/ approved from Authorised Signatory. Further all entries are approved as per approval matrix.	Check that invoices are approved from authorised signatory and entries are approved as per approval	Approved invoices Ledger of sale	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
				matrix.		
		Sales transactions are not properly classified in accounts.	Sales entry is passed by person responsible, and it is approved by authorised person.	Scrutinise sales ledgers on overall basis and check sales are recorded in correct ledgers are per Organisation policy.	Sales Schedule sale leger	
		Benefits for export sales not availed/ under availed by the Organisation.	Export incentive working is prepared and it is reviewed by authorised person.	Check trail mail/supportings of approval as per approval matrix.	Working of export incentive Trail mail	
		Export services are recorded at incorrect foreign exchange rate.	Export services are recorded at same day prevailing CBEC website rate. Sales entry is passed as per accounting manual.	Check export sale made are recorded at rates as specified by accounting manual.	Export sale ledger Invoice CBEC rates	
		Accounting for exempt sales is done incorrectly in books of account.	Separate expense and revenue ledgers are made related to exempt sales for compliance with applicable tax laws.	Check accounting for exempt sale and taxable sale in books.	Books of Account	
	Customer Evaluation	No policy has been formed for evaluation of customer.	Approved Policy for evaluation of customer has been formed.	Obtain policy of customer evaluation.	Customer Evaluation Policy	
		Customer evaluations are not being performed regularly.	Customer Evaluation is done as per policy. Marketing and Finance team is responsible for doing the customer evaluation. Based on	Check whether customer evaluations are being performed, and approved	Customer Evaluation forms/report	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Data analytics performed
			the same and subsequent discussions with the approving authorities, Sales department revises the approved customer list and block customers as per evaluations list.	customer list is updated as per the evaluations.		
	Customer Complaints	No policy has been for handling of customer complaints.	Approved Policy for handling customer complaints has been formed.	Obtain policy of handling customer complaints.	Customer Policy	
		Policy made for handling of customer complaints not complied.	Authorised levels are formulated for handling a customer complaint, regular monitoring is done to ensure customer complaints are handled as per policy by authorised personnel.	Check for compliance with the policy for handling customer complaints.	Customer Policy Complaint Log	
	Customer Complaints	Timely redressal of customer complaints not done.	Authorised person as per policy handles customer complaints and take appropriate action. Regular monitoring is done for status of customer complaints by authorised personnel as per company policy.	1. Check status of customer complaints. 2. Report complaints which have not been resolved in time specified as per Organisation policy.	Complaint Log	

Purchase to Pay – Direct Material

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
Procurement	Vendor Management	Risk of chosen of incompetent vendor and supply of inferior quality of goods.	Defined process for vendor evaluation and approval exists and includes the following: - technical and commercial evaluation by cross functional teams. - approval authority. - single vendor justification like for imports or critical items including development of new vendors.	1. Check the approval for technical evaluation and supporting documents thereof. 2. Check approval for commercial evaluation and supporting documents thereof. 3. Check justification for exceptions, if any.	1. Approvals for evaluations. 2. Support-ing for evaluations	30 new vendors	1. New vendors vis-à-vis existing vendors 2. Single vendors for non-critical items	-Number of certified suppliers. -Number of local and global suppliers. -Number of national contracts. -Number of rate contracts. -Supplier development programs.
		Risk of Unauthorised updates / alterations to vendor master.	Updates (Additions / Alterations) to the vendor master can be done only with the approval of	1. Check the ACL is as per approved authority matrix. 2. Check that person making the	1. Approvals for addition / alteration2. Acccess Control List	1. 30 vendor approval forms 2. Access Control	-	-

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			HOD (Commercial) and IT Head. Also, the access to make additions / alteration to the vendor master is restricted to personnel authorised as per approved Authority Matrix. The Authority Matrix is entered in the Access Control List (ACL) in the ERP systems.	addition / alteration is authorised to do so. 3. Verify vendor approval forms are approved by HOD commercial and IT Head.		List		
		Risk of Inaccurate updation in the vendor master.	Recorded changes to supplier master file are compared to authorized source documents by Manager (Commercial) or the designated authority to ensure that they were	1. Check that the information so entered is reviewed by Manager (Commercial) 2. Check with the supporting documents that the information has been Completely &	1. Supporting documents 2. Approvals	1. 30 vendor approval forms	check whether approvals are there for all the new vendor empanelment.	

180

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			entered accurately.	Accurately entered.				
		Risk of Critical vendor data is incomplete and not upto date.	Requests to change supplier master file data are logged; the log is reviewed to ensure that all requested changes are processed timely.	Check the requests log to ensure that there are no long pending requests for updation.	1. Outstanding Request log	1. Request log		
			Requests to change supplier master file data are submitted on prenumbered forms; the numerical sequence of such forms is accounted for to ensure that all requested changes are processed timely. In an ERP environment, the request for change can also be done in the system on the	1. Check the requests log to ensure that there are no missing request. Alternatively, there should be number cancellation note on the log.	1. Sequence of the request forms used	1. Request log		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			basis of chronology and numbering.					
			Supplier master file data is periodically reviewed by management	1. Check the evidence of the management review.	1. Management review			
			Recorded changes to the supplier master file are compared with authorized source documents by Manager (Commercial) or designated authority.	1. Check that the information so entered is reviewed by Manager (Commercial) 2. Check with the supporting documents that the information has been Completely & Accurately entered.	1. Supporting documents 2. Approvals	1. 30 vendor approval forms		
		Risk of inadequate screening	As per Company's Code of Conduct, the employees are mandated to inform the concerned HOD / Superior where conflict	1. Check the employee declarations for compliance with the ethical standards. 2. Check the vendor acknowledge	Declarations by vendors and the employees	1. Certifications of 30 employees 2. Acknowledgement from 30 vendors		

182

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			of interest exists. Employees are required as per Code of Conduct to certify compliance with the policy on an annual basis. Also, the vendors are required to inform as per the standard terms and conditions printed on the Purchase Order, if they have any relations employed with the organization.	ments in the Purchase Order.				
		Risk of not following screening procedures for one - time vendor	For ERP like Oracle, there is an option of ticking "One time flag" which needs to be updated at the time of vendor creation. As a result, the	1. Check by creating a dummy Purchase Order, if the vendor flagged off as One-time can be reused. 2. Obtain a list of One-	1. field validation	1. List of one-time vendors 2. PO dump		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			vendor gets deactivated after placing one PO.	time vendors and compare it with the PO dump to check whether one time vendors have been used more than once.				
		Vendor performance not reviewed periodically.	Performance Appraisal of vendor is done once in a year for long term PO / Contract and quarterly for short term PO / Contract. Based on the evaluation, Approved Vendor list is updated. Company is responsible for doing the vendor appraisals. Based on the same and subsequent discussions with the buyers / within the purchases group,	1. Verify whether the vendor appraisals have been done annually & quarterly. 2. Verify updation of the approved vendor list.	Timelines Quality approvals	1. for annual appraisal - check one sample, 2. for quarterly appraisal - check 3 samples		-Number of stock outs -Number of rejections -Number of warranty claims % of rework done

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			Purchases department revises the approved vendor list.					
		Riks of Dummy / inactive vendors exists	Suppliers that have not been used for a significant time period are reviewed by Manager (– Commercial) and marked for deletion by the application.	1. Compare the active vendor listing (VLOOKUP) with the PO listing for the year. 2. Scrutinise the vendor dump for vendors with common / dummy names or details.	Dummy/ Inactivity in vendors accounts	1. Active vendor listing 2. PO Dump		
	Procurement Planning	Risk of increased material cost or erratic inventory levels due to lack of planning.	An annual plan is developed for defining the material requirement for each of the departments. The plan is duly approved by the different HODs and CEOs. The plan includes the following factors (regarding	Check that there is compliance with defined process regarding identification of vendors, entering into agreement with the vendors for long term supplies, the plans are communicated to the vendors, etc.	Timeliness in updating the plan Completeness of defining material requirement Vendor identification Vendor communication Authorizations.	1. Annual Plan 2. All the activities to be checked for 30 items	-	-Type of items required - Quantities required -No of vendors

185

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			procurement): 1. type of material required 2. frequency of requirement 3. authorisation Based on the Annual plan, purchases department identifies the suppliers for the regular material, agreements with the suppliers, communication of the plan to the suppliers, lead time for delivery, periodicity of supply, etc. The company has defined procedure for undertaking the above activities.					
	Ordering	Risk of Inadequate number of vendors	Sufficient quotations, before approving the	1. Check for compliance with the purchase	Number of vendors vis-à-vis the requirement	Vendors for 30 items	-	-

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		are identified for Request for Quote (RFQ)	PO. Justification for deviation from purchase policy is mentioned as remarks, which is also reviewed by the approving authority before PO is approved.	policy for identification of vendors for RFQ. 2. Check whether incase the requisite number of vendors were not available; the due escalation procedure was followed.	of purchase policy.			
			All POs are required to be approved in accordance with the approved authority matrix. The Authority Matrix specifies the expenditure limits of the relevant personnel and has been entered into ERP package.	1. Check the approvals for the PO with the Authority Matrix. 2. In case, the approvals are not as per the authority matrix, ratification/ justification for the same needs to be checked.	Approval	30 Pos		
		Wrong quantity / rates / payment terms are	Purchase Order is prepared by the buyer which is	1. Check that the PO is supported with a duly approved	1. Quantity as per indent vis-à-vis PO. 2. Approval	30 items	-	-

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		raised in Purchase Order, etc.	reviewed and approved by the person so authorized as per Authority Matrix. The reviewer verifies the details in the PO with the supporting. Access to create and approve PO are with different users in ERP system.	indent. 2. Check that the PO is approved as per Authority Matrix.	for the PO.			
		Indent raised/ approved for purchase when there is no requirement for goods / services or goods are already in stock.	The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to procure material. The Authority Matrix is entered in the ERP system	1. Check that indent is approved in accordance with the Authority Matrix.	1. Approvals for indent 2. Access Control List	1. 30 indents 2. ACL		

188

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			in Access Control List (ACL).					
			Review of Monthly Budget *vs* Actual Expenditure is conducted encapsulating department budgets and major expenditures incurred. Any unauthorized expenditure or double processing of significant expenditure would be identified in the review meeting.	1. Check that all the indents which get converted into PO are reported as part of MIS for variance analysis (viz. budget vs. actual). 2. To review the progress/ minutes of the meeting and analyse the common / continuing issues.	1. Quantity reported in MIS.	1. MIS - 3 months		
		Unauthorised indents may be raised for purchases.	The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to procure	1. Check that the indents are approved in accordance with the Authority Matrix.	1. Approvals for indent 2. Access control list	1. 30 indents 2. ACL		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			material. The Authority Matrix is entered in the ERP system in Access Control List (ACL).					
			The ERP system does not allow changes to be made to the approved indents. They can either be cancelled or processed for PO. The amendment rights are available only to the Head of the Department (HOD). In case of any modification, if done, in a log which needs to be reviewed.	Check the access control list to see that no one other than HOD has modification access for indent and access to cancel indent is with Managers in respective user departments / Cost centers.	1. Approvals for indent 2. Access control list	30 indents ACL		
		Indent does not prescribe the correct technical	Specifications are mandatory field in the indent and	1. Check the exception report generated from ERP for	Rejections due to incorrect / missing specification	Exception report and Rejection report for	No of rejections vis-à-vis no of indents placed	-No of indents placed -No of rejections

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		specifications of goods/ services required resulting in procurement of incorrect goods/services.	cannot be bypassed (in ERP).	indents raised without any specification. 2. Check the rejection report for the material rejected due to incorrect specification.	s.	the period of audit.		-No of rejections due to specifications.
		Indent does not prescribe the correct technical specifications of goods/services required resulting in procurement of incorrect goods/services.	The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to procure material. The Authority Matrix is entered in the ERP system in Access Control List (ACL) Indents without the specifications are treated as incomplete since the	1. Check that the indents are approved in accordance with the Authority Matrix.	1. Approvals for indent 2. Access control list	1. 30 indents 2. ACL		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			quotations cannot be obtained for the same.					
			In case the goods are rejected by the Quality Control department or shop floor, reasons for the same are reviewed to ensure that the same were not due to incorrect specifications mentioned on indent. This is ensured by AM – Commercial.	1. Check the Material Rejection list and if they are due to incorrect specifications.	specifications	1. Rejection report		
		Indents / PRs are not used when purchasing goods or services.	All supporting documents (Indents/ vendor quote analysis sheet/ vendor quotes. etc) are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).	1. Check the PO review and approval process. Check that the PO is supported with a duly approved indent.	Supporting documents (including indents)	30 POs		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			All POs are required to be approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying correctness and accuracy thereof. The Authority Matrix is entered in the ERP system in Access Control List (ACL).	1. Check that the PO are approved in accordance with the Authority Matrix. 2. Check that the Purchase Order cannot be created without approval.	1. Approvals 2. ACL	30 POs		
		POs do not contain accurate information.	All supporting documents (Indents/ vendor quote analysis sheet/ vendor quotes, etc.) are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).	1. Check the PO review and approval process. 2. Check that the PO is supported with a duly approved indent.	Supporting documents (including indents)	30 POs		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			All POs are required to be approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying correctness and accuracy thereof. The Authority Matrix is entered in the ERP system in Access Control List (ACL).	1. Check that the PO are approved in accordance with the Authority Matrix. 2. Check that the PO cannot be created authorizer without approval.	1. Approvals 2. ACL	30 POs		
		PO prices are not competitive.	ERP system requires the PO approving authority to review vendor quotes at the time of approving the PO.	1. Check the Price fluctuations for same items. 2. Check that the PO is supported with a duly approved quotes. 3. Check that the PO is approved as per Authority Matrix.	1. Supporting documents 2. Price fluctuations	1. PO dump 2. 30 POs	1. Same Material from same vendor at different rates 2. Same material from different vendor at different rates 3. Foreign exchange fluctuations	Number of non-certified suppliers Commodity/ forex hedging Proportion of procurement from high rate vis-à-vis low-rate vendors Rising unit cost.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			The purchase policy of the company requires obtaining a certain minimum number of quotations before placing the order. In case the specified number of quotes are not available then escalation procedure specified in the purchase policy needs to be followed.	1. Check that specific number of quotes required as per purchase policy are obtained. 2. Check that in case of exceptions, escalation procedure as per the policy is followed.	1. quotes	30 POs		
		Price changes are not authorised.	If the terms of an approved Purchase Order are altered in ERP, it automatically sends PO in pre-approval stage.	1. Check by raising a dummy PO, getting it approved and then altering it. 2. Check by review of the audit trail report in ERP, if any PO has been modified after approval.	Price changes in PO	Audit trail report		

195

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			The purchase policy of the company requires that in case the approved price in a PO is changed, it needs to be re-approved / re-processed as if it is a new PO.	1. Check whether the PO wherein price has been altered has been re-approved as per the Authority Matrix.	Price changes in PO	30 POs		
		Unauthorized POs/Contracts	All POs are approved as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	1. Check that the PO is approved as per Authority Matrix 2. Check the ACL and confirm that the same is updated as per Authority Matrix	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 POs		
			All supporting documents (Indents/vendor quote analysis sheet/vendor quotes, etc.) are reviewed at the time of PO approval by authorised personnel (as	1. Check the PO review and approval process. 2. Check that the PO is supported with a duly approved indent.	Supporting documents (including indents)	30 POs		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			per the approved Authority Matrix).					
		-Terms of PO / contract are not suitable - contract terms not vetted by Legal Dept.	General terms and conditions, approved by legal are pre-printed on reverse of PO.	1. Check whether the standard terms and conditions are approved by Legal Department. 2. Check whether the standard terms and conditions are printed on reverse of PO.	Standard PO terms and Conditions; Approval	30 PO / Contracts		Vendor claims
			In case of unusual or non-regular contracts, the personnel authorised as per Authority Matrix to approve the contract are required to obtain the approval of personnel authorised to do so in Legal department.	1. Check whether the terms and Conditions of unusual or non-regular contracts are approved by authorised personnel in legal department	Approval of terms for customised contracts	30 PO / Contracts		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		Contracts are not stored / kept in a central / safe repository to safeguard company's interests and to prevent the use of the contract which might be detrimental to company's interests.	All PO / contract copies (active/ expired) are maintained with the buyer. Contracts on stamp paper are being stored centrally with Manager – Legal.	Check the existence of contracts with Buyers / Manager - Legal	Existence and storage	30 Contracts		
		Vendor, order details are not accurately input in the system.	At the time of PO approval, PO is printed, and the details of the order, vendor and terms of the order are checked for accuracy by the personnel authorised to approve the PO as per the Authoritiy Matrix.	1. Compare the approved PO with the supporting documents to ensure accuracy of data input.	Accuracy of data updation	30 POs		
		PO issued	Receipts for	1. Check by	Existence of	GRN and	GRN for	% of

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		after the goods have been received or goods / services may have been procured without raising a PO	the goods cannot be entered in the ERP system unless PO exists ,therefore in the system. i.e. GRN cannot be prepared in the absence of PO Reference in the ERP system.	raising a dummy receipt where PO does not exist. 2. Compare the GRNs with the PO to ensure that PO exists for all the goods receipt and the POs are dated prior to GRN.	PO for goods received	PO dump	which no PO reference PO date after GRN date	GRNs without POs
			Vendor invoices cannot be processed in ERP system in absence of a PO in system.	Compare the invoices recorded in vendors' accounts with the PO listing to ensure that PO is available for invoices booked.	Existence of PO for invoices booked	Vendor-wise Invoice listing	PO date after Invoice date	
		Orders not clubbed to save logistics cost.	Purchases Report is generated monthly and is reviewed by Sr Manager - Commercial to ensure that same location procurement requirements	1. Check the receipt of material vis-à-vis locations - date wise and quantity-wise. 2. Check the monthly purchases report for	Date, quantity, location, vendor, logistics provider.	GRN dump and PO dump	1. Same date same location different supplier. 2. Close range of dates same location different supplier.	Logistics cost per location/ delivery

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			are evaluated for scheduling deliveries so as to reduce logistics / freight and related costs.	evidence of Sr Manager's review.				
		Business share allocation amongst different vendors results in higher procurement prices	All POs are reviewed and approved as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	1. Check that the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 POs	Same material different suppliers Item cost Lead time for delivery of material for different suppliers.	Servicing time for each of the supplier for same material
			Purchases MIS is reviewed monthly by cross functional team of Heads of Purchases, Finance and Production and reasons / costs for or due to allocation of procurement among different	1. Check the monthly purchases MIS review for evidence of HODs review. 2. See the minutes of discussion and check whether the action points have been actioned upon.	Monthly MIS review	MIS for 3 months		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			vendors are analysed. Exceptions, if any are taken into account at the time of placement of subsequent orders.					
		Inadequate segregation of duties -- Vendor identified by the user and goods/services ordered directly by the user from the vendor (including determination of purchase price and other terms and conditions).	Adequate segregation of duties (SOD) exists for all purchases that are routed through the buying department which is different from the user department. The same is ensured in ERP system through updation of Access Control List (ACL).	1. Check that the user department does not have access to raise PO by creating a dummy PO with id of a buyer. 2. Check the ACL for existence of SOD.	SOD	ACL		
		Purchase against Invalid contracts	The majority of contracts are generated for a calendar year thereby facilitating timely	1. Check the validity of the contracts. 2. Check the time gap between date of expiry of	Timely renewal of Contracts	Contracts dump	No of contracts Periodicity of the contracts Time taken for renewal	Periodicity of the contracts

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			renewal. Details of each of these time-bound contracts are maintained in a Tracker. As and when contracts are shown due for renewal in Tracker, they are reviewed to assess whether fresh terms and conditions/contracts need to be drawn up.	contract and date of actual renewal.			of contracts.	
		Vendors not challenged on a regular basis to bring down the price of supply.	Negotiations are conducted with approved vendors on an annual and routine basis to reduce the cost of purchase. Also, the Quotes are compared for negotiations during the appraisal time of the vendors. This is done by the personnel	1. compare the approved PO with the subsequent reductions in the prices. 2. check the market rates for the bulk items / critical items and their movements during the period of audit.	Price fluctuations	PO dump	Movement in market price of items over a period. Movement in purchase price of the items over a period of time.	Acquisition price as compared to the market price.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			approved as the Authority Matrix.					
			MIS is reviewed by cross functional team of HODs for critical items and costs. Actionable, if any are flagged off for implementation.	1. Check the MIS for evidence of HODs review. 2. See the minutes of discussion and check whether the action points have been actioned upon.	Monthly MIS review	MIS for 3 months		
		Duplicate Orders	MIS is reviewed by cross functional team of HODs for critical items and costs. Actionable, if any are flagged off for implementation.	1. Check the MIS review for evidence of HOD's review. 2. See the minutes of discussion and check whether the action points have been actioned upon.	Monthly MIS review	MIS for 3 months		
			Exception report is generated at the time of processing of invoices for POs /	Check the linking of the attributes and the exception report generated for any duplicate	Quantities, PO numbers, PR reference, supplier name	Invoice / PO dump and link with PR dump	Difference in PO and PR quantity Check in supplier ledger for duplicate	

203

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			Invoices with certain same attributes such as supplier, quantity, PR reference and is reviewed by HOD Commercial.	orders. Sort the Invoice batch / PO dump on the attributes and check for the common information.			payments.	
			All POs are reviewed for accuracy and correctness and approved as per the Authority Matrix. Also, the same has been enteredinto ERP software in Access Control List (ACL).	1. Check that the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 POs		
		All POs are not recorded.	PO are sequentially pre-numbered. The sequence of PO processed is accounted for.	1. Check whether there are any missing serial numbers of the POs.	Serial control	PO dump	No of PO raised No of POs raised manually	
			In case of emergency purchases, the purchases	1. Check that there exists specific approval for	Approval	Invoice dump		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			made without indent / PO need to be specifically approved as per the Authority Matrix.	purchases without indent or PO as per the Authority Matrix.				
		Validity of the open POs / Contracts	The list of open POs / contracts is reviewed monthly by Sr Manager - Commercial. The redundant / expired PO are purged from the list.	1. Check the validity of open PO / Contracts.	Open PO dates	Open PO listing	Open PRs and POs Ageing – Periodic review and closure process.	Delay in receipt of materials as compared to PO date.
	Receiving	Stock outs due to delays in delivery of stocks ordered through open Pos.	Open PO list is prepared on a weekly basis by the Commercial department. This is used as basis for tracking timely deliveries by the buyers.	1. Check the instances of stock outs and review the justification / root cause for the same. 2. Check whether the buyers track deliveries against the Open PO list.	1. Open PO dates 2. stock outs	1. 10 weeks open PO list 2. Stock out event list	Open PRs and POs Ageing – Periodic review and closure process.	Delay in receipt of materials as compared to PO date.
		Goods received may not be recorded.	Statements received from vendors are reconciled to	1. Check that the vendor accounts reconciliation	Vendor Reconciliation	Vendor Reconciliation statemen		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			the vendor accounts in the accounts payable sub ledger quarterly and differences are investigated. This is reviewed by AM – Accounts,	is done on a periodic basis. 2. Check the differences, if any, are reconciled and are not carried forward.		ts		
			The stock is physically verified at least once a year by Accounts department /independent auditors. Variances, if any are reconciled with the books of accounts to ensure accuracy of the books of accounts.	1. Check the working papers of physical verification and see that the differences, if any were reconciled and accounted for.	Periodicity and Variances noted in physical verification.	Physical verification statements and reconciliation		
		Goods and services accepted without proper inspection and	The receiving personnel are required to match the goods received with the open	1. Check whether GRN can be raised for items without a PO or that do not meet the PO	specifications	30 GRNs		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		verification	purchase orders. In case, the goods received do not match with the quantities or specifications or exceed the purchase order quantity, the same are rejected.	specifications.				
			All receipts are reviewed and approved by the personnel as per the Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs		
		Quantity received in excess of ordered quantity.	The receiving personnel are required to match the goods received with the open purchase orders. In	Check whether GRN can be raised for items without a PO or that do not meet the PO specifications	specifications	30 GRNS		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			case, the goods received do not match with the quantities or specifications or exceed the purchase order quantity, the same are rejected.	.				
			All receipts are reviewed and approved by the personnel as per the Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs		
		Quantity received has not been ordered.	The receiving personnel are required to match the goods received with the open purchase orders. In case, the goods	1. Check whether GRN can be raised for items without a PO or that do not meet the PO specifications.	specifications	30 GRNS		

208

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			received do not match with the quantities or specifications or exceed the purchase order quantity, the same are rejected.					
			All receipts are reviewed and approved by the personnel as per the Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs		
		Quantity ordered but received before the due date.	The receiving personnel are required to match the goods received with the open purchase orders. In case, the goods are received before the	Check whether GRN can be raised for items received before the due date or without a PO or that do not meet the PO specifications.	specifications	30 GRNS		

209

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			due date or do not match with the quantities or specifications or exceed the purchase order quantity, the same are rejected.					
			All receipts are reviewed and approved by the personnel as per the Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Autho-rity Matrix 3. 30 GRNs		
		Unauthorized person can create receipts.	All receipts are reviewed and approved by the personnel as per the Authority Matrix. Also, the same has been entered into ERP software in Access	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Autho-rity Matrix 3. 30 GRNs		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			Control List (ACL).					
		Terms and conditions of acceptance of goods at the factory gate (before the goods have been approved by quality) may be detrimental to the interests of company.	The receiving stamp that is used to acknowledge receipt of goods at the gate on GRN, bears the inscription *'goods are being received subject to count and quality procedures'*.	Check that the GRNs are being marked with the stamp 'goods are being received subject to count and quality procedures'.	Appropriate stamp on the GRNs	30 GRNs		
		Inappropriate quality of material accepted.	Before the GRN is sent to Accounts for booking the liability or the goods are sent to store, quality department is required to certify the quality of material received in accordance with the set guidelines. The store clerk will not	Check whether the GRNs have been marked as approved by Quality Department. 2. Review exception report for the goods rejected due to quality constraints at the shop floor.	Post QC - rejections	1. 30 GRNs 2. Exception report raised for post QC - rejections	1. Number of Post QC Rejections 2. Number of items rejected during the period	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			accept the goods unless the "QC checked" is stamped on GRN. Also, Accounts will not book the liability and process the payment unless the QC checked stamped GRN is received by them. In the event, quality check is not required for any item, the same should be a part of QC exceptions list which is reviewed on a monthly basis.					
			Access to certify the quality of material is restricted as per Authority Matrix in ERP.	1. Review Access Control List for access to personnel other than those authorised for certifying	Access rights for certifying quality	Access Control List		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
				quality of the goods.				
		Delay in clearing and forwarding of imported goods.	The report on demurrage charges incurred due to delay in C&F of imported goods is reviewed by Sr. Manager - Receiving and Manager - Accounts monthly. Also, these charges are separately disclosed in the MIS for Sr. Management review.	Check the Demurrage charges paid and justification for the same.	Demurrage charges	Dump of demurrage charges ledger balance.	Demurrage charges and linking to receipt of goods.	
		Unauthorised or Inaccurate release of payments for transporter dues.	All transporter claims are authorised by the Sr. Manager - Stores prior to payment by Accounts. This is based on the agreements with the vendors / transporters.	Check the supporting for the claims viz. agreements, if any / rate contract	Transporter charges	30 transporter invoices		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		CENVAT not availed / Short / Excess availed	Monthly reconciliation of CENVAT account and CENVAT register is done jointly by Stores and Accounts.	Check the CENVAT reconciliation for long outstanding items and check justifications for the same.	Periodicity of reconciliation and reasons for outstanding items.	3 months reconciliation		
	Invoice Processing	Invoices may be booked incorrectly	Before any invoice is approved for booking, AM - Accounts performs a three-way match of the PO, GRN and Invoice.	Check that the invoice is supported by duly authorised PO and GRN.	supporting documents	30 invoices		
			In case of emergency purchases, the invoice is verified with the GRN and the subsequent approval obtained for the purchase from authorise personnel.	Check that the invoice is supported by GRN and post-purchase approval from the authorize personnel.	supporting documents	30 invoices		
		Same invoice may be booked more than	At the time of booking of invoice, invoice is defaced with	Check that the invoices are defaced at the time of booking.	Defacing of invoice	30 invoices		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		once.	the Stamp "Processed" by Booking Clerk.					
			Once a invoice is booked, the supporting documents *viz.* GRN, PO, Indent are attached with it. Invoices without these, cannot be processed.	Check that the invoice is supported by duly authorised PO and GRN.	supporting documents	30 invoices		
		Unapproved invoices are processed	The invoices before being processed are reviewed by AM - Accounts	Check the approval of AM - Accounts on the invoice.	Approval of AM - Accounts	30 invoices		
			Access rights to process the invoices are restricted to the authorised personnel and are entered in Access Control List (ACL) in ERP system.	Check the Access Control List for the access rights given to the authorised personnel.	Access rights	ACL		
		Delay in accounting	Statements received from	1. Check the periodicity of	Timeliness of booking	Reconciliation for	Time taken for booking	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
		of invoices	vendors are reconciled to the vendor accounts in the accounts payable subledger quarterly and differences are investigated. This is reviewed by AM – Accounts.	vendor reconciliation 2. Sample check the pending items in the reconciliations for invoices pending booking and confirm the reasons for same.	of invoices	30 vendors	of invoices from the date of receipt of material.	
			The list of Goods Received Not Invoiced (GRNI) and the items with Quality Control are reviewed monthly to ensure that there are no delays in booking the liability.	1. Check aging of the Temp GRN raised for the material with Quality Control department and the GRNIs. 2. Ensure that the same are accounted in the books as liability in the suspense accounts.	Aging of GRNI and material being held by QC.	Dump of GRNI and material with QC	1. Time taken for QC of material procured. 2. Time taken for booking of invoices from the date of receipt of material.	
		Delay in raising debit/ credit notes	Statements received from vendors are reconciled to the vendor accounts in	1. Check the vendor reconciliation for the periodicity of	Timeliness of raising Debit / Credit Notes	Reconciliation for 30 vendors	Time taken for issuing debit / credit notes from the date of	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			the accounts payable subledger quarterly and differences are investigated. This is reviewed by AM – Accounts.	reconciliation 2. Sample check the pending items in the reconciliations for debit / credit notes yet to be raised. Confirm reasons for the same.			booking of invoices or date of receipt of material.	
		Unauthorized debit/ credit notes may be raised.	The debit / credit notes are approved by the authorised personnel. The same entered in the Access Control List existing in the ERP system.	1. Check that the access control list defined in ERP system is as per the approved Authority Matrix. 2. Check that adequate back up / supporting documents exist for issuing debit / credit notes.	1. Approvals 2. Reasons for issuance	30 debit / credit notes	1. Number of debit / credit notes issued vis-à-vis number of purchases made. 2. Value of debit / credit notes issued vis-à-vis value of purchases made.	
	Accounting	Unauthorised payments	The payment voucher with required supporting is reviewed by authorised personnel. The authority	1. Check that the Access Control list in ERP is as per the Authority Matrix. 2. Check that	1. Access Control List 2. Supporting	1.Access Control List 2.Authority Matrix 3. 30 Payment		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			matrix is entered in the Access Control List (ACL) in ERP system. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved.	requisite supporting are attached with the payment voucher. 3. Check that the supporting are defaced for the approved vouchers.		vouchers		
			At the time of processing a vendor invoice for payment, AM - Accounts are required to identify and set off all the advances pending adjustment for such vendor.	1. Check that there are no amounts pending adjustment for vendors where all the invoices have been paid. See justification for exceptions. 2. Scrutinise the vendor accounts / party accounts to check the cases of segregation of amounts to avoid	1. unlinked amounts in vendor accounts pending adjustments .2. multiple payments on same or nearby date.	30 vendor accounts	Same Vendor-Same Date-More than one payment	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
				authority matrix.				
			The listing of vendor payments is reviewed prior to release of payment by the authorised person.	1. Check that the evidence of review on the vendor payment list.	review	30 vendor payment lists		
			The personnel making the payment (either through cheque / DD / wire transfer) are authorised person.	1. Check the approval for authority to make the payment. 2. Check whether the same has been communicated to the bank.	approval	Authority Matrix		
			Management periodically reviews the returned paid cheques for unauthorised signatures, alterations and / or alterations.	1. Check the evidence of the management review.	review	Returned cheques		
		Payments are made to incorrect vendors	The payment voucher with required supporting is reviewed by	1. Check that the ACL in ERP is as per the approved	1. Access Control List 2. Supporting	1.Access Control List 2.Authority Matrix		

219

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			authorised persons. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved.	Authority Matrix. 2. Check that requisite supporting are attached with the payment voucher. 3. Check that the supporting are defaced for the approved vouchers.		3. 30 Payment vouchers		
			The listing of vendor payments is reviewed prior to release of payment by the authorized person. Cheques / DD are restrict endorsed by the preparer to ensure that they are paid to specific payee.	Check that the evidence of review on the vendor payment list.	management review	30 vendor payment lists		
			Management periodically reviews the returned paid cheques for	Check the evidence of the management review.	management review	Returned cheques		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			unauthorised signatures, alterations and / or alterations.					
		Duplicate payments	The payment voucher with required supporting is reviewed by authorised person. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved.	1. Check that the Access Control list in ERP is as per the approved Authority Matrix. 2. Check that requisite supporting are attached with the payment voucher. 3. Check that the supporting are defaced for the approved vouchers.	1. Access Control List 2. Supporting	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers		
		Non receipt of material against advances	The listing of Open POs is reviewed monthly to check the cases of delayed supplies wherein advances have been	1. Check the due dates in the open PO / Contracts. 2. Check the reasons for delays in supplies.	1. Open PO dates 2. justifi-cation for delays	Open PO listing	Open PRs and POs Ageing – Periodic review and closure process.	Delay in receipt of materials as compared to PO date.

221

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
			released to the vendors.					
			Ageing of the party balances is reviewed monthly and account reconciliation is done on a quarterly basis.	1. Check the debit balances appearing in the supplier's account and ageing thereof. 2. Check whether any unauthorized advance has been given to the supplier. 3. Check whether the advances have not been adjusted correctly while accounting for receipt of goods.	1.Approvals, 2. Amount, 3. Receipt of material 4. Due date	Vendors Account and the Advances Aging statement	Advances ageing statement and due date for receipt of supplies.	Old outstanding items in ageing report
		Wrong Foreign exchange rates used for conversion of foreign currency invoices.	Weekly foreign currency rates are updated in the ERP system by the authorised person.	Compare the rates applied for invoice processing with the RBI rate.	Exchange rate applied	Forex rates in 10 weeks		

Purchase to Pay – Indirect Material and Services

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
Procurement of Indirect Material and Services	General and entity level control	Procurement policy and Authority matrix may not be prepared or approved by Board of Directors and thus leading to risk of procurement at unfavorable conditions to the organisation.	The organisation has clear and comprehensive (up to date) Indirect material and service procurement policy as approved by Board of Directors (BOD) or designated authority.	As per company policy	1. Check clear updated procurement policy approved by BOD or designated authority. 2. Check it addresses all attributes related to service procurement.	1. Approved procurement policy 2. Completeness	Approved procurement policy	NA
			1. The organization has clear and comprehensive (up to date) Delegation of Authority (DOA)/ Delegation of Power (DOP) and Authority Matrix. 2. Authority Matrix is approved by Board of	As per company policy	1. Check Indirect material and service procurement DOA/DOP is available and approved by BOD.	Approved DOA/DOP for purchase	Approved DOA/DOP from BOD	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Directors, defining the authorities for approving purchase transactions or performing various transactions during the purchase process.					
		Inadequate Segregation of Duties and access rights which may result in fraudulent / unauthorised transactions.	1. Document defining appropriate Segregation of Duties (SOD) is in place. 2. Access rights (Write / Read / Delete / Modify) to various people in the origination of reviewed periodically to ensure appropriate SOD and avoid any unauthorized transact-ions. 3. Periodic Review of Segregation of Duties and Access rights is conducted.	As per company policy	1. Check documented SOD and Access right list which are duly updated. 2. Verify same SOD and Access right also input in the system for approval of transactions 3. Verify evidence of periodic review of SOD and Access rights in ERP system.	1. Docum-ented SOD, Access right 2. Periodic review	1. SOD 2. Access right List 3. Half yearly review document	Analyse transaction carried out during the review period to identify the following: 1. Un-authorised users performing transactions. 2. Con-flicting transaction rights granted to same person. 3.Internal Auditor to review the circumstances of conflict of interest.

224

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		SOP may not be defined to ensure consistency and standardization of operations.	1. The organization has clearly defined Standard Operating Procedures and are in place. 2. SOP should define the sequence of activities, Roles and Responsibilities, Key Performance Indicators (KPIs), Timelines and Frequency of activities along with various documents to be maintained by the organization for procurement of Indirect material and service transactions.	As per company policy	1. Check SOP available and complete in all aspect of roles, KPIs, Timelines and frequency of activities, etc. 2. Check when SOP updated last and enquire the reason for not updating the SOPs in case, not updated for long time.	Approved SOP and completeness	Updated SOP	NA
		Review system to mitigate risk of inappropriate transaction may not be in	Review system is in place to mitigate risk in procurement	As per company policy	1. Review appropriateness of Management Information System	1. MIS 2. RSM 3. Fraud assessment activity	MIS for 3 months Action and step taken to identify and	Analyse various figures reported in MIS vis-a-vis the details

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		place.	of indirect material and services. 1. Management Information System (MIS) for monitoring of procurement of indirect material and services are in place. 2. Risk management system is in place to identify and mitigate risk related to procurement of indirect materials and services. 3. Fraud risk assessment activity conducted by management frequently.		(MIS) for regular monitoring of operations and financial activities by senior / top management, especially for any management override of controls. 2. Review appropriate Risk Management System is in place to identify and mitigate various risk related to procurement activities of the organization. 3. Review of Fraud Risk Assessment activity is conducted, and fraud risk are identified along with relevant controls to avoid any fraudulent transactions viz.		control fraudulent activity.	appearing in ERP system to identify instances of incorrect reporting. Risk management : To review the risks that are being mitigated and whether there is any risk not being mitigated. Risk being dynamic, whether emerging risks are also covered needs to be reviewed. Fraud Risk: Critical review of transactions from the possibility of fraud.

226

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					unapproved transactions, fictious invoices and payments, etc.			
	Annual procurement budget of indirect material and service	Procurement budget may not be prepared and monitored on regular basis to avoid deviation in future.	1. Base for preparing budget and Budget is approved by the BOD before start of financial year. 2. Monitoring of Budget Vs Actual is done on monthly basis and review of action plan wherever required.	As per company policy	1. Check Annual Procurement Budget is approved by the designated authority and agreed with / communicated to the ~~relevant authorities~~ delegated authority well in advance. 2. Review of periodic monitoring of deviations (variances) from the approved budget conducted along with reasons for deviations, if any. 3. Action plan is documented and adhered for avoiding such	Approved budget and subsequent monitoring	Approved Budget for the year Budget Vs actual MIS for 3 months and upto date	Verify the accuracy of the Budget vs Actual MIS from the independent data source e,g, transactions recorded in ERP to identify instances of incorrect monitoring or Budget overrides. to understand the reasons for variances and not limited to (a) incorrect preparation of budget (b) accounting and classification of errors (c) use of budgetary provision for other purposes, etc.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					identified variance in future.			
		Absence of formal planning policy may lead to increased material and service cost or increased inventory levels.	1. Approved procurement plan ~~is~~ is ~~existed~~ prepared ~~and prepared~~ based on the production plans or business plans. 2. Operations are conducted as per plan and process is in place to identify and report deviations. corrective actions are required to be taken where there are variances.	As per compan y policy	1. Check annual plan is developed for defining the material requirement for each of the departments. The plan is duly approved by the different HODs and CEO. The plan includes the following factors (regarding procurement) : a. type of material required in terms of units, price, source and other preferences b. frequency of requirement c. autho-rization 2. Check based on the Annual plan, purchase department	Approved budget and subsequent monitoring	Approved Budget for the year Budget Vs actual MIS for 3 months and upto date	Verify the accuracy of the Budget V Actual MIS from the independent data source e,g, transaction recorded in ERP to identify instances of incorrect monitoring or Budget overrides.

228

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					identifies the suppliers for the regular material, agreements with the suppliers, communication of the plan to the suppliers, lead time for delivery, periodicity of supply, etc.			
	Vendor Selection and Master Management	Vendor chosen is not competent resulting in inferior quality of goods being supplied.	Defined process for vendor evaluation and approval exists and includes the following: - technical and commercial evaluation by cross functional teams. - approving authority. - single vendor for imports or critical items including development of new vendors. Any regulatory requirements	As per company policy	1. Check the approval for technical evaluation and supporting documents for delegation of authority. 2. Check approval for commercial evaluation and supporting documents for delegation of authority. 3. Check justification for exceptions, if any, and reason there for. 4. See the	1. Approvals of plan evaluations 2. Supporting for evaluations	20% of new vendors or 20 whichever is higher	1. Analyse vendor list of current year vis-à-vis previous year to identify addition of new vendors to increase competition. 2. Analyse sufficient no. of vendor were for each type of service and material to get best competitive rates, 3. Check quotations were taken to find competent vendors on regular basis

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			to be fulfilled.		overall approval including that party is in approved vendor list.			to give contract to appropriate parties.
		Incomplete/ Inaccurate vendors records	1. Pre-defined / Pre-designed Vendor creation forms contains key details of vendor i.e. Name, PAN, Address, Contact Details, GST registration details, Bank Account, place of business, MSME certificate, Turnover details for e-Invoicing, etc. 2. Mandatory field are defined in the system without which vendor code is not allowed to be created in the system.	As per company policy	1. Check approved vendor format and all requests should be received in standard format only. 2. Complete details of vendors filled in format mentioning not applicable in case, any field is not applied. 3, Check system control to avoid duplicity at code level, PAN and GST level, address and contact level.	1. Approved format for creation/alteration 2. Completeness and accuracy	30% of new vendors or 10 whichever is higher	Analyse Vendor Database for any duplicate vendor records and corresponding purchase / payment transactions with such codes.
		Selection of inappropriate	1. Market research are	As per compan	1. Check the list of pre-	Management review and	Select 2 contractor	1. Analyse that vendor

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		material / vendor	carried out from time to time to specify the minimum timeline to identify prospective contractor for the required Service/ Material. 2. Appropriate due-diligence and financial /operational and technical background checks be performed as per approved checklist and the contractor be added to the approved list after due approvals. 3. Con-tractors who do not participate in bidding process, are reviewed and removed after obtaining NOC from them. 4. Con-	y policy	qualified contractor for different types of Service requirement of organization. 2. Check due diligence and financial / operational and technical background check performed as per checklist. 3. Frequency of updating of list and identify non-responding bidders. 4. Check approval from designated authority of selected vendor for quotation purpose.	approval mechanism to identify prospective vendors	from each major Service and material group Or as per business need	list are updated by company on frequent basis and should have sufficient vendor who actively participate in bidding. 2. Check company should not be dependent on some vendors for quotation purpose.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			tractor are selected on basis of pre-qualification and merit basis. After selection of vendor, list is approved by designated authority before asking for quotation.					
			1. Open tender system are followed for high value transactions or critical services / material as per the organization policy for inviting all possible vendors for indented procurement. 2. Limited tender requests for quotation are given to the pre-approved vendors for select category of service/material or value below the	As per company policy	1. Check open tendering used by the company for high value or critical service/ material transaction or for specific procurements. 2. For other services/ material limited tender request are sent to all approved vendors. 3. Check method used for open tender, i.e., no. of	Tendering as per policy of the company	PO Records	Analyse ERP Open tender, Limited tender data and verify that tendering is done as per policy of the company.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			define limit as per the organization policy.		advertisement in different newspapers, coverage area and in different languages to create competition among vendors. 4. Check NOC are obtained from vendors who did not send quote.			
			Standard request for Quotation / tender are prepared and circulated to all parties for inviting quotations as per the organization's policy.	As per company policy	1. Check standard format of request are approved and used by departments. 2. Check changes should be done by only by addendum after approval. 3. If quotation, not in standard format, should be rejected unless there is a chance to accept the	Standard format used for Tender /quotation	For 5 major tenders and 5 major RFQ process or cover 40% tender whichever is higher.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					quotation.			
			1. Technical criteria are defined in the bids as per the requirement of user department and approved by HOD (purchase). 2. Marks are allotted to bidders on the basis of technical qualification and no of deviations allowed.	As per company policy	1. Check technical criteria for selection of vendor are define in bids and matched with requirements as specified by user department and approved by HOD. 2. Check technical qualification document and mark is allocated to bidders based on it only. 3. Check for any deviation from technical qualification, verify approval of designated authority.	1. Defining of technical criteria 2. Deviation approval	for 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher.	Analyse tracker to verify technical qualification, details are obtained and considered for all bidders. Note: exception and check approval of deviation are obtained.
		Possibility of vendor preference	Same timelines and process are followed for all parties and deviation are approved	As per company policy	1. Check bidding document and process to verify timeline and process are	1. Same and timely process for all parties 2. Deviation approval	for 5 major tenders and 5 major RFQ process or cover 50% tender whichever is	Analyse time tracker of - Submission of technical, financial qualification

234

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			by designated authority except procurement of low value and selected category as per procurement policy.		common in case of all tendering parties 2. In case of deviation approval obtained from designated authority.		higher	document and approval thereof. - Submission of financial bidding and approval to verify all process are followed in time bound manner for all vendors. **Note** exception and check deviation for same to check tendering process is monitored properly.
		Selection of wrong vendor or high cost of procurement.	1. Comparative quotation analysis sheet drawn before purchases are approved. 2. If lowest quotation is not accepted, appropriate justification be documented and	As per company policy	1. Check whether comparative sheet of bids is prepared or not. 2. Check Justification for selection of other than lowest bidders and approval of the same. 3. Check whether quotation opened, registered	1. Approval on comparative sheet 2. Deviation approval 3. Sign off by tender committee	For 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher	Analyse ERP or other softwares for final comparison of rates for all vendors with original rates quoted by individual vendor to identify difference.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			approved by designated authority. 3. Quotations are opened and registered, and a comparative chart is prepared and authorised. 4. Quotations are opened in presence of tender committee only for the qualified bidders and rest bid may be rejected.		and comparative list is approved by authorised persons. 4. Check quotation opened in presence of tender committee for qualified bidders and sign off by them. 5. Check order given to lowest bidder but whether earlier project was performed by him within time and cost (Check history of vendor).			
			1. Approved note with all relevant justification is documented for selected vendor by designated authorities. 2. Adequate approval (as per	As per company policy	1. Check justification must be prepared and approved by designated authority. 2. Check justification must be supported by evidence, i.e., project	1. Approval note with Justification	for 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher	Check justification given in approval note with actual work performed by vendor or with previous work performed from ERP records.

236

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Companies Act,2013, SEBI) from Board of Directors is in place for purchase from related parties.		delivered in past. 3. Check justification given in approval note. Verify justification with actual work performed by vendor during audit period or record of previous work performed by same vendor.			1. Quality rejection 2. Timely delivery 3. Qualitative delivery
		Non-compliance to requirement of Companies Act and other regulations	1. Adequate approval from Board of Directors is in place for purchase from related parties. 2. Disclosure of related parties and purchased from it. 3. Adequate documentation is in place to justify price of purchases from related	As per company policy	1. Check BOD approval obtained in case of purchase from related party. 2. Check disclosure note given in financial statement. 3. Justification documented for purchase from related parties. 4. In case of purchase from related	BOD approval and justification	All purchase from related party.	Analyse ERP data to check rates of other vendor with same requirements as of related parties to verify transaction are performed at arm length basis or not

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			parties.		party, compliance with relevant provisions of Section 188 of Companies Act, 2013. 5. The procurement price is reasonable according to Section 40 A(2) of Income Tax Act, 1961, if purchase is made from sister concern.			
		System control may not be implemented for modification at RFQ level, Quotation level, approval level may lead to unauthorised purchase.	1. System are not allowed to raise RFP without approved requisition in place. 2. All vendor quotations and bid are locked in modification and are opened in presence of designated authorities. 3. Selected party is	As per company policy	1. System walkthrough for RFQ without approved requisition. 2. System walkthrough for modification in quotation and locked parties, so identified, check the audit trail for it. 3. Check rates of vendors in final comparison	System control for modification at RFQ level, quotation level, Identified vendor and other information.	System walkthrough	Analyse ERP or other software final rates data for all vendors with original rates quoted by individual vendor to identify difference.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			identified and locked in system after all approval. 4. System are not allowed to backdate / modify any information once process is completed.		sheet matched with rates in individual quotes. 4. Verify all approved vendor with final vendor comparison list. 5. Change log must be available for all modification and reviewed by authorised person.			
		Unauthorised updates / alterations may be made to vendor master.	1. Updates (Additions / Alterations) to the vendor master are made only with the approval of authorised person on the basis of requisition in proper format from users. 2. Also, the access to make additions / alteration to the vendor master is	As per company policy	1. Check the Access Control List (ACL) is as per approved authorities matrix. 2. Check that the person making the addition / alteration is authorised to do so. 3. Verify vendor creation/alteration forms are approved by authorised persons.	1. Approvals for addition / alteration, 2. ACL	40% of addition/alteration or 20 whichever is higher	Analyse transaction carried out in vendor master during the review period to identify the following: 1. Transactions performed by unauthorised users. 2. Conflicting transaction rights granted to same person.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			restricted to personnel authorised as per approved Authorities Matrix. The Authorities Matrix is entered in the Access Control List (ACL) in the systems(Normally additions/ alteration rights provided to IT).					
		Inaccurate updation in the vendor master.	Recorded changes to the supplier master file are compared to authorized source documents by authorized person to ensure that they were input accurately and he should be different from person who entered data in file.	As per company policy	1. Check that information so entered is reviewed and authorised. 2. Check with the supporting documents that the information has been Completely & Accurately entered.	1. Supporting documents 2. Approvals	40% of alteration or 20 whichever is higher	Analyse vendor master data to validate following: 1. Matching of PAN with GST 2. GST no. with state code 3. Length of PAN and GSTIN 4. Length of mobile number 3. Check bank account no. provided or not.

240

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
								Analyse Vendor Database is comprehensive, and all vendor details are complete and accurate – viz., Name, PAN, Address, Contact Details, GST registration details, place of business, etc.
		Audit logs for changes made in vendor master may not be available and reviewed that may lead to unauthorized changes.	Request to change supplier master file is logged; the log is reviewed to ensure that all requested change is processed timely. Steps taken when there are unauthorized changes.	As per company policy	1. Check the request log to ensure that there are no long pending requests for change.	1. Outstanding list in Request log	1. Request log	NA
		Critical vendor data is incomplete and is not up to date.	1. Vendors are classified correctly as MSME data in master	As per company policy	1. Verify mail sent to vendor for declaration as MSME	1. MEME and E-invoicing Vendor listing.	20% of service /material vendor	NA

241

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			and updation are done on yearly basis. MSME certificates are obtained yearly. 2. List of vendors who have to do E-Invoicing are prepared and bills are processed accordingly.		and for turnover. In case, there is portal for vendor, check vendor have submitted their credential. 2. Verify vendors' declaration received and vendors' record updation is done on the basis of declaration. 3. Verify E-invoicing by specified vendors.			
			Request to make change in supplier master file is submitted account and ensure that all requested changes are processed timely.	As per company policy	1. Check the request log to ensure that there is no missing request. Alternatively, there should be request cancellation note in the log.	1. Sequence of the request forms used.	1. Request log	NA
			Supplier master is periodically reviewed by management for accuracy	As per company policy	1. Check the evidence of the management review.	1. Management review of supplier master	Management signoff or approved file.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			and ongoing pertinence.					
		Risk of conflict of Interest of vendor	1. As per Company's Code of Conduct, the employees are mandated to inform the concerned HOD / Superior where conflict of interest exists. 2. Employees are required to comply with the policy. 3. Also, the vendors are required to inform as per the standard terms and conditions printed on the PO, if they have any relations with employee in organization.	As per company policy	1. Check the employee's declarations for compliance with the ethical standards. 2. Check the vendor's acknowledgements in the PO, if they have relation with employee.	1. Declarations by vendors and by the employees.	1. Certifications from 30% employees 2.Acknowledgement from 20% vendors or having 60% business with company.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		One-time vendors are not subjected to same controls as all other vendors.	1. There is an option of ticking "One time flag" which needs to be updated at the time of vendor creation. As a result, the vendor gets deactivated after placing one PO. 2. Specific vendor code is used for creating one-time vendors (e.g. 1000 for domestic and 1100 for import).	As per company policy	1. Check by creating a dummy PO, if the vendor flagged off as One time user. 2. Obtain a list of One-time vendors and compare it with the PO Records to check whether one-time vendors have not been used more than once order.	1. Field validation to use code one-time only.	1. List of one-time vendors. 2. PO Records 3. System walkthrough	Analyse ERP records for POs with pre-define one-time vendor code and identify more than one PO are raised with one-time code from same vendors.
		Contractor performance not reviewed periodically	1. Performance Appraisal of vendor is done once in a year for long term PO / Contract and quarterly for short term PO / Contract. 2. Based on the evaluation, Approved contractor	As per company policy	1. Verify whether the contractor appraisals have been done annually & quarterly as the case may be and it documented. . Verify department wise list of vendors and total appraisal done during	1. contractor Performance evaluation and appraisal	1. For annual appraisal - check appraisal of 30% contractor or 15 whichever is higher. 2. same for quarterly appraisal.	Analyse PO record with GRN records to identify vendor wise: - Cases of quality rejection - Case of late delivery against PO terms - Cases of low quantity delivery against PO quantity

244

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			list is updated. respective departments are responsible for doing the contractor appraisals. 3. Based on the same and subsequent discussions with the user department, the Purchases department revises the approved contractor list.		audit period by each department. 2. Verify updation of the approved contractor list on basis of appraisal, Check list is updated on the basis of appraisal only. 3. Mails sent to contractor by management to take action otherwise remove from approved vendor list.			to ascertain 1. Vendor with low performance evaluation have high share of business 2. Action taken against regular default vendor.
		Dummy/ inactive/ unsatisfactory performance by contractor	1. Contractor that have not been selected from a significant period of time are reviewed by purchase team and marked for deletion. 2. Ensure contractor are timely blacklisted	As per company policy	1. Compare the active vendor listing (VLOOKUP) with the PO listing for the year. 2. Scrutinize the vendor Records for vendors with common/ dummy names or details. 3. Unsatisfactory vendors	1. dummy / Inactivity in vendors accounts	1. Active vendor listing 2. PO Records 3. Performance evaluation report	Analyse Vendor master file for Service /Material PO list of 2 to 3 years to ascertain following: 1. Blocking of vendors with whom organization had no transaction 2. Restrict to use vendor

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			wherever required for unsatisfactory performance as per the defined policy. 3. Vendors are restricted for award of contract, who are not engaged with organization from long period and are allowed after updated KYC document only.		removed after performance evaluation. 4. User department approval for removal of service / material vendor. 5. Check vendor are in master but work or transaction could not performed with them due to restriction or blockage. 6. Check process to obtain updated KYC document if vendors are used after define period.			code for non-submission of updated KYC document.
	Placing Order	Inadequate number of vendors are identified for RFQ	Sufficiency of quotations, is checked before approving the PO. Justification for deviation from purchase	As per company policy	1. Check for compliance with the purchase policy for identification of vendors for RFQ. 2. Check whether in case, the requisite	Number of contractor vis-à-vis the requirement of purchase policy	Select vendors and corresponding PO's to cover major item and service category (Cover at least 60-120 PO's or more depend on	1. Analyse vendor list are updated by company on frequent basis and should have sufficient vendor who actively participate in bidding.

246

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			policy is mentioned as remarks, which is also reviewed by the approver before PO is approved.		number of vendors were not available, the due escalation procedure was followed 3. Ask reason for significant change in rates of products. Check reason and approval of higher price. 4. Approval, in case change is approved vendor.		quantum of business)	2. Check company should not be dependent on some vendors only for quotation purpose.
			All POs are required to be approved by approved authority matrix. The Authority Matrix specifies the expenditure limits of the relevant personnel and has been entered into relevant software.	As per company policy	1. Check the approvals for the PO with the Authority Matrix. 2. In case, the approvals are not as per the authority matrix, ratification / justification for the same needs to be checked.	Prepare, Review and Approval of purchase order	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	Analyse transaction carried out in vendor master during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
								person. Also analyse purchase on same or nearby dates to identify cases of splitting of PO to override authority matrix.
		PO's raised with wrong quantity / rates / payment terms, etc.	1. PO is prepared by the designated person which is reviewed and approved by the person so authorized as per Authority Matrix. 2. The reviewer verifies the details in the PO with the supporting. 3. Access to create and approve PO are with different users in system.	As per company policy	1. Check that the PO is supported with a duly approved indent. 2. Check that the PO is approved as per Authority Matrix 3. Check creating and approving right should be with different person.	1. Quantity as per indent vis-à-vis PO 2. Approval for the PO	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		Indent raised / approved for purchase when there is no requirement for goods / services or goods are already in stock	The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to procure material. The Authority Matrix is configured in the ERP system in Access Control List (ACL)	As per company policy	1. Check that indents are approved in accordance with the Authority Matrix. 2. Check whether Authority Matrix is configured in the system in Access Control List for system control point of view.	1. Approvals for indent 2. Access control list	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	Analyse transaction carried out during the review period to identify the following: 1. Unauthoirsed users performing transactions 2. Conflicting transaction rights grated to same person.
		Unauthorised indents may be raised for purchases.	1. The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to procure material. The Authority Matrix is entered in the ERP	As per company policy	1. Check that the indents are approved in accordance with the Authority Matrix 2. Check service budget availability while approving of indents. 3. Check excess budget are approved from	1. Approvals for indent 2. Budget availability at the time of indent approval.	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	Analyse the total Service budget approved by department before start of year and total value of indent approved during budget period to verify. -Indent approved more than original budgeted

249

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			system in Access Control List (ACL) 2. Budget availability with department is considered before approval of Service indent otherwise indent could not be approved. 3. Service budget are approved from appropriate authority to release indent.		authority in case of total budget exhausted by department before release of service indent.			without obtaining approval for excess budget which is against the policy of organization.
			The system, does not allow changes to be made to the approved indents. They can either cancelled or processed for PO. The amendment rights are available only with Head of Department	As per company policy	1. Check the access control list to verify that no one other than HOD has modification access for indent and access to cancel indent.	1. Approval for indent 2. Access control list	System walkthrough and check system allowed to make changes in approved indent.	Analyse records of purchase despite same item in hand and lying un-utilised. Analyse quantity, specification as per indent and PO records punched in ERP system for any

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			(HOD).					deviation. If excess quantity purchased, verify excess quantity consumed or not to, verify wrong decision of high purchase against indent.
		Indent does not prescribe the correct technical specifications of goods/services required resulting in procurement of incorrect goods/ services.	Specifications are mandatory field in the indent and cannot be bypassed (in ERP). Maker checker controls is established to verify completeness and correctness of all details.	As per company policy	1. Check the exception report generated from ERP for indents raised without any specification. 2. Check the rejection report for the material rejected due to incorrect specification.	1. Rejections due to incorrect / missing specifications.	Exception report and Rejection report for the period of audit.	Analyse ERP data to compare specification as per indent and corresponding specification in PO to identify deviation. Further, verify deviation with rejected GRN at quality stage to establish rejection due to wrong purchase against indent.
		Indent sent to purchase	1. Material and service	As per compan	1. Check indent	1. Timely conversion	Indent report compare with	Analyse ERP data of

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		department with delay may hamper production activity.	requisition are sent to purchase department within defined timelines. 2. Timeline are defined for approval of indent and issued further to procurement team for processing.	y policy	reports to verify timely sharing and conversion of approved indent into PO. 2. Check list of indents raised by user department but not approved yet. 3. Check list of approved indents sent but no action initiated by purchase team on same.	of indents into PO's	PO reports	indent and PO to identify following: 1. Time gap between indent raised and approval/ release of indent. 2. Time gap between indent release to PO approval date. 3. Expected date of material as per indent along with deadline to vendor in PO for supply. to calculate probable losses due to delay in approval at different stage from indent to PO.
		Indent does not prescribe the correct technical specifications of goods/	The indent is reviewed and approved by the authorized personnel	As per compan y policy	1. Check that the indents are approved in accordance with the	1. Approvals for indent 2. Access control list	1. System walkthrough for approval procedure and specification.	Analyse Purchase requisition transaction to identify the

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		services required resulting in procurement of incorrect goods/services .	(as per the limits set out in approved Authority Matrix), signifying the need to procure material. The Authority Matrix is entered in the ERP system in Access Control List (ACL) Indents without the specifications are treated as incomplete since the quotations cannot be obtained for the same.		Authority Matrix. 2. System walkthrough to check indent without specification.			following: 1. Incomplete or incorrect details in PR 2. PRs backdate or raised after ordering 3. PRs are created for quantity/service in excess of the budgeted amount 4. Requisition is in excess of average consumption or in spite of high inventory levels. 5. Open PRs not reviewed and closed
			In case the goods/ services are rejected by Quality Control department or by user department, reasons for the same are reviewed to ensure that the same were not due	As per company policy	Check the Material Rejection list and if it is due to incorrect specifications.	Service and goods specifications mentioned properly with complete description.	Rejection report along with reasons.	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			to incorrect specifications mentioned on indent.					
		Indents / PRs are not used when purchasing goods or services.	All supporting documents (Indents/vendor quote analysis sheet/vendor quotes, etc.) are reviewed at the time of PO approval by authorized personnel (as per the approved Authority Matrix).	As per company policy	1. Check the PO review and approval process. Check that the PO is supported with a duly approved indent.	Supporting documents (including indents)	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	Analyse PO Records with Indent Records to verify each is supported by indent.
		POs do not contain accurate information.	All supporting documents (Indents/vendor quote, analysis sheet, etc.) are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).	As per company policy	1. Check the PO review and approval process. 2.Check that the PO is supported with a duly approved indent. 3. To check accuracy of PO verify it with customer source document, management approval process of	Supporting documents (including indents)	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					project.			
			All POs are required to be approved by the authorized personnel (as per the limits set out in approved Authority Matrix), verifying correctness and accuracy thereof. The Authority Matrix is entered in the ERP system in Access Control List (ACL)	As per company policy	1. Check that the PO are approved as per Authority Matrix. 2. Check that the PO cannot be created in absence of approval.	1. Approvals 2. ACL	Cover all service /Material and approval matrix which combinedly cover more than 30% of purchase value.	Analyse purchase in record to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
		Service / Material prices are not competitive	ERP system requires the PO approving authority to review vendor quotes at the time of approval of the PO	As per company policy	1. Check the PO review and approval process. 2.Check that the PO is supported with a duly approved indent. 3. To check accuracy of PO to verify it with customer source document, management	1. Supporting documents 2. Price fluctuations	1. PO records 2. All cases of deviation in rates within audit period	Analyse ERP data for review of vendor quote by appropriate authority before approval of PO.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					approval process of project.			
			The purchase policy of the company requires obtaining certain minimum number of quotations before placing the order. In case, the specified number of quotes are not available, then as procedure specified in the purchase policy needs to be followed.	As per company policy	1. Check that specific number of quotes required as per purchase policy are obtained. 2. Check that in case of exceptions, procedure as per the policy is followed.	Sufficient quotes obtained or not	Select vendors and corresponding POs to cover major items and services (Cover at least 60-120 PO's or more depend on quantum of business)	Analyse ERP data for number of quotation and compare with purchase policy to identify exception. Verify exception approval for insufficient no. of quotes.
		Change in order are not authorised.	1. If the terms of an approved PO are altered for price and scope, it automatically sends PO in pre-approval stage. 2. Original Pos' terms are reviewed	As per company policy	1. Check by raising a dummy PO, getting it approved and then altering it. 2. Check by review of the audit trail report in ERP, if any PO has been modified	Price and scope alteration in original order.	Audit trail report and select 20 sample for change order	Analyse change order record to identify the following: 1. Unauthorised users performing transactions. 2. Conflicting transaction

256

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			regarding provision for change due to change in price and scope.		after approval. 2. Changes could be done only if original PO permits for changes.			rights granted to same person.
			1. The purchase policy of the company requires that in case of Change in Order, it needs to be re-approved / re-processed as if it is a new PO. 2. Amendment number must be provided in change in order for trail log of old PO.	As per company policy	1. Check whether the PO wherein price has been altered has been re-approved as per the Authority Matrix. 2. Check amendment no. shown in PO after price change.	Price and scope alteration original order	15 PO or 50% of change order whichever is lower.	Analyse ERP original POs with change orders due to price revision and check significant impact on budget.
			1. Change orders are approved by next higher authority (DOA) or from highest authority, if changes are above defined	As per company policy	1. Check whether authority matrix defined for change order. 2. Whether reason for changes is documented	1. Authority matrix for change order 2. Justification remark with approval	15 PO or 50% of change order whichever is lower.	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			limits. 2. Reason for change order with proper justification must be documented which also show impact on budget and should also be approved.		and approved with impact on budget.			
		Unauthorized Pos/Contracts	All Pos are approved as per the approved Authority Matrix. Also the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 Pos	Analyse transaction carried in purchase record to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
			All supporting documents (Indents/ vendor quote analysis sheet/vendor quotes, etc.)	As per company policy	1. Check the PO review and approval process. Check that the PO is supported with a duly	Supporting documents (including indents)	30 POs	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).		approved indent.			
		Unfavorable terms and conditions of the purchase order.	1. General terms and conditions, approved by legal team and part of Agreement/ Purchase order/ Work order are pre-printed on reverse of PO. 2. Standard terms and condition, approved by legal team and part of Agreement/ Purchase order/ Work order.	As per company policy	1. Check whether the general and standard terms and conditions are approved by Legal and part of agreement/p urchase order/work order.	General and Standard PO Terms and Conditions; Approval	30 PO / Contracts	NA
			In case of unusual or non-regular contracts, the personnel authorised as per	As per company policy	1. Check whether the terms and Conditions of unusual or non-regular contracts are approved by	Approval of terms for customised contracts	30 PO/ Contracts (Unusual and non-regular)	NA

259

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Authority Matrix to approve the contract are required to obtain the approval of person authorised to do so in Legal department.		authorised personnel in legal department.			
		Contracts are not stored/ kept in a central/ safe repository to safeguard company's interests and to prevent the use of the contract which might be detrimental to company's interests.	1. All PO/ contract copies (active/expired) are maintained with department. 2. Contracts on stamp paper are being stored centrally with designated authorities.	As per company policy	1. Check the existence of contracts with designated authority only and no other person have access for same. 2. Stamp paper stored centrally with designated authority only.	Existence and storage of contracts	1. Check process of maintaining documents by buyer/ legal department. 2. Check 15 PO on sample basis.	NA
		Contractor, order details are not accurately input in the system.	At the time of PO approval, PO is printed and the details of the order, contractor and terms of the order are checked for accuracy by the personnel	As per company policy	1. Compare the approved PO with the supporting documents to ensure accuracy of data input.	Accuracy of data updation	30 POs	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			authorised to approve the PO as per the Authorities Matrix.					
		PO issued after the goods have been received or goods / services may have been procured without raising a PO	Receipts for the goods cannot be affected in the ERP system unless the POs exist in the system. i.e. GRN/SRN cannot be prepared in the absence of PO Reference in the ERP system.	As per company policy	1. Check by raising a dummy receipt where PO does not exist. 2. Compare the GRN/SRN record with the PO to ensure that PO exists for all the goods receipt and the POs are dated prior to GRN/SRN.	Existence of PO for goods/service received	GRN/SRN and PO records	Analyse GRN/SRN record or Gate entry record having transactions of goods and service to identify: - GRN/ SRN or gate entry without PO reference. - PO created after gate entry or invoice date. Calculate value of such purchases during audit period to show impact.Also to check GRN prepared but risk of inventory not being received.
			Vendor	As per	1. Compare	Existence of	Vendor-wise	Analyse

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			invoices cannot be processed in ERP system in absence of a PO in system.	company policy	the invoices recorded in vendors' accounts with the PO listing to ensure that PO is available for invoices booked.	PO for invoices booked	Invoice listing	ERP data of various expense GL with Goods receipt / Service clearing account to check expenses rooted through 3-way control system i.e. PO, GRN/SRN and invoice instead of direct booking.
		Orders not clubbed to save logistics cost	1. Purchase Report is generated on monthly basis and is reviewed by designated authority. 2. Procurement requirements are evaluated for scheduling deliveries so as to reduce logistics / freight and related costs.	As per company policy	1. Check the receipt of material vis-à-vis locations - date wise and quantity-wise. 2. Check the monthly purchases report to check that it is reviewed by designated authority.	Planning for possible saving in logistic cost	GRN records and PO records	Analyse purchase on same or closed date from same location/city and from same or different suppliers to calculate total logistic saving possible during audit period if transported through same vehicle.
		Business share	All POs are	As per	1. Check that	Unauthorise	1. ACL	Analyse PO

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		allocation among different vendors result in higher procurement prices.	reviewed and approved as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	company policy	the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	d approval rights	2. Authority Matrix 3. 30 POs	records with GRN/SRN records to identify vendor wise. - Cases of quality rejection - Case of late delivery against PO terms, - Cases of less quantity delivery against PO quantity. and ascertains:- 1. Vendor with low performance evaluation have high share of business 2. Action taken against regular default vendors.
			1. Purchases MIS is reviewed on a monthly basis by cross functional team of Heads of Purchases,	As per company policy	1. Check the monthly purchases MIS review as evidence for HODs review 2. See the minutes of	Monthly MIS review	MIS for 3 months	Analyse ERP procurement as per approved allocation of business among vendors or not.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Finance and Production and reasons / costs for or due to allocation of procurement among different vendors are analysed. 2. Exceptions, if any are taken into account at the time of placement of subsequent orders.		discussion and check whether the action points have been implemented. 3.Check approval of allocation of business among different vendors and check same allocation provided in system for procurement purpose.			Analyse latest quality, delivery reports to recommend change in share of business among vendor. Also analyse charges for same services by different vendors. Calculate losses due to high allocation of business to high-rate vendor even provides low quality goods/service or late delivery.
		Inadequate segregation of duties -- Vendor identified by the user and goods/services ordered directly by the user from the vendor (including	Adequate segregation of duties (SOD) exists for all purchases that are routed through the buying department which is	As per company policy	1. Check that the user department does not have access to raise PO by creating a dummy PO with id of a purchase department. 2. Check the	Review SOD conflicts	ACL	Analyse ERP data to verify ID of user (Indent) department and purchase department must be different.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		determination of purchase price and other terms and conditions)	different from the user department. The same is ensured in ERP system through updation of Access Control List (ACL).		ACL for existence of SOD.			
		Service and material procurement contract not approved after expiry and procurement done against Invalid/expired contracts.	Majority of service contracts are generated for a calendar year thereby facilitating timely renewal. Details of each of these time-bound contracts are maintained in a Tracker. As and when contracts are shown due for renewal in tracker, they are reviewed to assess whether fresh terms and conditions/contracts need to be drawn up.	As per company policy	1. Check the validity of the contracts. 2. Check the time gap between date of expiry of contract and date of actual renewal to identify value of service procurement against invalid contracts. 3. Analyse losses due to procurement at old rates if subsequent reduction in price.	Timely renewal of Contracts	Contracts records	Analyse contract tracker with dates of original renewal and actually renewed.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		Continued procurement at higher price as reduction in market prices and not renegotiated with suppliers.	Negotiations are conducted with approved vendors on an annual and routine basis so as to reduce cost of purchase. Also, the Quotes are compared for negotiations during the appraisal time of the vendors. This is done by the personnel approved as the Authority Matrix.	As per company policy	1. compare the approved PO with the subsequent reductions in the prices. 2. Check the market rates for the bulk items / critical items and their movements during the period of audit.	Price fluctuations and periodic review	PO records	NA
			MIS is reviewed by cross functional team of HODs for critical items and costs. Actionable, if any, are flagged off for implementation	As per company policy	1. Check the MIS for HODs review 2. See the minutes of discussion and check whether the action points have been actioned upon.	Monthly MIS and review Minutes and timely action	MIS for 3 months	NA
		Duplicate Orders	MIS is reviewed by	As per compan	1. Check the MIS for	Monthly MIS review	MIS for 3 months	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			cross functional team of HODs for critical items and costs. Actionable, if any, are flagged off for implementation	y policy	HODs review. 2. See the minutes of discussion and check whether the action points have been actioned upon.	Status of previous issue flagged.		
			Exception report is generated at the time of processing of invoices for POs / Invoices with certain same attributes such as supplier, quantity, PR reference and is reviewed by designated authority.	As per compan y policy	1. Check the linking of the attributes and the exception report generated for any duplicate order. 2. Sort the Invoice batch / PO Records on the attributes and check for the common information.	Quantities, PO numbers, PR reference, supplier name	Invoice / PO Records and link with PR Records	Analyse gate entry, GRN, PO Records, PR Records for any common information which show duplicate PO raised for same items.
			All POs are reviewed for accuracy and correctness and approved as per the approved Authority Matrix. Also, the same has been	As per compan y policy	1. Check that the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorise d approval rights	1. ACL 2. Authority Matrix 3. 30 POs	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			entered into ERP software in Access Control List (ACL).					
		All POs are not recorded	PO are sequentially pre-numbered. The sequence of PO processed is accounted for.	As per company policy	1. Review of PO records if there are any missing serial numbers of the Pos.	Serial no. control of purchase order	PO records	Analyse ERP PO records to verify PO sequence number.
			In case of emergency purchases, the purchases made without indent / PO need to be specifically approved as per the Authorities Matrix.	As per company policy	1. Check that there exists specific approval for purchases without indent or PO as per the Authorities Matrix.	Approval of emergency purchase	Invoice records	Analyse GRN record or Gate entry record having transactions of Service/material to identify: - GRN/SRN or gate entry without PO reference. - PO created after gate entry or invoice date. Calculate value of such purchases during audit period to

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
								show impact.
		Validity of the open POs / Contracts	1. The list of open POs / contracts is reviewed on a monthly basis by purchase team. The redundant / expired PO are purged from the list. 2. Timelines of the procurement activities are monitored on monthly basis. Reason of analysis is performed and documented for all delayed beyond the defined timelines.	As per company policy	1. Check the validity of open PO / Contracts. 2. Check the documented reason for delayed Pos.	Open PO dates	Open PO listing	Analyse list of Purchase Orders for following: - Instances of open purchase orders not closed for long times. - may be used for unauthorised transactions. Calculate financial loss to the company due to delay in delivery, If possible.
		Audit logs for changes in PO may not be available and reviewed leads to unauthorized changes.	1. Audit logs are generated for all POs / WOs raised / modified in the system. 2. Process is in place to monitor audit	As per company policy	1. Check logs are available for POs/ Wos and modification. 2. Mechanism in place to review audit	Audit Logs of changes in PO	1. Audit logs 2. monthly review on logs- 3 Month.	Analyse Audit log of modification carried in purchase record to identify the following: 1. Unauthorise

269

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			logs to identify any inappropriate / suspicious activity.		logs.			d users performing transactions 2. Conflicting transaction rights granted to same person.
	quality assessment	Stock outs due to delays in delivery of stocks ordered through open Pos.	Open PO/contract list is prepared on a weekly basis by designated department. This is used as basis for tracking timely deliveries by the user department.	As per company policy	1. Check the instances of stock outs and review the justification / root cause for the same 2. Check whether the purchase department track deliveries against the Open PO list	1. Open PO dates 2. stock outs	1. 10 weeks open PO list 2. Stock out event list	Analyse ERP Open PO records with daily stock details to identify instances where PO is undelivered, and material is out of stock.
		Goods/ service received may not be recorded.	Statements received from vendors are reconciled with the vendor accounts in the accounts payable sub ledger quarterly and differences are investigated. This is	As per company policy	1. Check that the vendor accounts reconciliation is done on a periodic basis. 2. Check the differences, if any are reconciled and are not carried forward.	Unrecorded services/goods	Top 30 vendor service/material Vendors Reconciliation statements or cover 40% purchase value.	NA

270

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			reviewed by Accounts teams.					
			The stock at the business locations of the company is physically verified at least once a year by Accounts department / independent auditors. Variances, if any, are reconciled with the books of accounts to ensure accuracy of the books of accounts.	As per company policy	1. Check the working papers of physical verification and see that the differences, if any, were reconciled and accounted for.	Periodicity and Variances noted in physical verification	Physical verification statements and reconciliation	NA
		Goods and services accepted without proper inspection and verification	1. The receiving personnel are required to match the goods received with the open purchase orders. In case the goods received do not match with the quantities or specification	As per company policy	1. Check whether GRN / SRN can be raised for items without a PO or that do not meet the PO specifications 2. Verify user department head approval on service invoices	GRN and service against Authorised PO only	PO records and GRN records 30 GRNs for physical verification	NA

271

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			s or exceed the purchase order quantity, the same are rejected. 2. The user department verifies service invoices of vendor with internal service records and obtained approval of department head. Only after service booked in system. 3. Invoice quantity and physical quantity are matched for which store person count inventory before GRN and sign off on invoice.		before booking the same in books. 2. Whether store person sign off on invoice after physical count of goods.			
			All receipts are reviewed and approved by the personnel as per the approved Authority Matrix. Also,	As per company policy	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse records of GRN/SRN with records of PO quantity and rates to identify Instances of deviation.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			the same has been enteredinto ERP software in Access Control List (ACL).		per Authority Matrix.			
		Quantity/service received in excess of ordered quantity	1. The receiving personnel is required to match the goods/ service. So, received with the open purchase orders. In case, the goods/ service received do not match with the quantities or specifications or exceed the purchase order quantity, the same are rejected.

2. ERP also has control over quantity booking, system does not allowed booking of quantity | As per company policy | 1. Check possibility of GRN/ SRN more than PO quantity by system walkthrough. 2. Check approved tolerance limit against PO quantity from management side. Verify cases where goods/service allowed more than tolerated limit. | Order Vs Receipt qty Material not received as per specifications | PO Records VS GRN Records and amended PO for change in order qty. | Analyse list of GRN/SRN for following: 1 Instance of delays in receipt of materials/service. 2. Instances of GRN / SRN without PO or before PO 3. Instances of GRN without gate entry 4. Instances of GRN before gate entry 5. Instances of GRN/SRN more than PO quantity 6. Instances of GRN / SRN value more than PO / SO value |

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			more than PO quantity.					
			All receipts are reviewed and approved by the personnel as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse ERP receipt record during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
		Quantity received has not been ordered.	The receiving personnel is required to match the goods received with the open purchase orders. In case, the goods received do not match with the quantities or specifications or exceed the purchase order	As per company policy	1. Check whether GRN/SRN can be raised for items without a PO or that do not meet the PO specifications	Material not received as per specifications	PO records VS GRN records and amended PO for reason of Qty and specification.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			quantity, the same are rejected.					
			All receipts are reviewed and approved by the personnel as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the GRN/SRN is approved as per Authority Matrix 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorise d approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse ERP receipt record to identify the following: 1. Unauthorise d users performing transactions 2. Conflicting transaction rights granted to same person.
		Unauthorized person can create receiving documents	All receipts are reviewed and approved by the personnel as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the GRN is approved as per Authority Matrix 2. Check the ACL and confirm that the same is updated as per Authority Matrix	Unauthorise d approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse ERP receipt record during the review period to identify the following: 1. Unauthoirse d users performing transactions 2. Conflicting transaction rights granted to same person.
		Terms and	The	As per	1. Check that	Appropriate	30 GRNs	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		conditions of acceptance of goods at the factory gate (before the goods have been approved by quality/ indenter may be detrimental to the interests of company.	receiving stamp that is used to acknowledge receipt of goods at the gate on GRN, bears the inscription *'goods are being received subject to count and quality procedures'*. Accordingly, liability would not accrue to the Company until these procedures are complied with.	company policy	the GRNs are being marked with the stamp 'goods are being received subject to count and quality procedures'.	stamp on the GRNs		
		Inappropriate quality of service / material accepted	1. Before the GRN is sent to Accounts for booking the liability or the goods are sent to store, quality department is required to certify the quality of material received in accordance with the set guidelines.	As per company policy	1. Check whether the GRNs have been marked as approved by Quality head. 2. Review exception report for the goods rejected due to quality constraints at the shop floor. Check all these goods are	Post QC - rejections	1. 30 GRNs 2. Exception report raised for post QC - rejections	Analyse Quality and Return to Vendor for following: - Delays in sending back rejected material to vendor. - Instances of GRN and issue of material despite quality rejection.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			2. The user department verify service invoices of vendor with internal service records and obtained with approval of department head. Only after service booked in system. 3. The store clerk will not accept the goods unless the "QC checked" is stamped on GRN. 4. Also, Accounts will not book the liability and process the payment unless the QC checked and stamped on GRN is received by them. 5. Quality check is not required for any item, the same should be a part of QC		returned to vendors as per agreement. 3. If rejected goods are not returned, it should be recorded as scrap. 4. Monthly quality exception list reviewed by authorised person. 5. Verify user department head approval on service invoices before booking the same in books.			- Quality note are created by unauthorized person/ Absence of SOD.

277

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			exceptions list which is reviewed on a monthly basis.					
			Access to certify the quality of material is restricted to persons per approved Authority Matrix in ERP.	As per company policy	1. Review Access Control List for access to personnel other than those authorised for certifying quality of the goods.	Access rights for certifying quality	Access Control List	Analyse GRN and Quality record to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
		Policy may not be in place for sampling, methodology, checklist leads to credit to vendor for poor quality service / material.	1. Policy in place for quality testing of required material including sampling, methodology and documentation of quality testing. 2. Quality inspection standards are defined for all	As per company policy	1. Check policy of sampling and methodology of quality testing is documented. 2. Check quality inspection policy is defined for all material. 3. Inspection carried out as per policy or ISO certification process.	Checklist, sampling and quality methodology	Select 30 GRN/SRN	Analyse ERP Quality Records and check quantity transferred to unrestricted category or not (for issue purpose). Check quantity in restricted category and reason for same.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			materials. 3. Ensure all steps are carried out as per company policy or ISO certification process for quality assessment and documentation. 4. All service are approved basis of complete checklist.		4. Check services should be approved basis of complete checklist and reviewer approval. Verify checklist for different type of services.			Analyse ERP quality record of actual sample with define sampling method.
		Rejected material may be placed separately (Quarantine) and return to vendor on timely basis leads to risk issue to floor and ownership.	1. Any rejection is segregated and stored separately. 2. All rejections are supplied back to vendor on timely basis. 3. Department ensure timely return and recording of return. 4. Material is consumed only after Quality checks.	As per company policy	1. Physically verify rejected items and storage control to avoid issue for operation. 2. Check rejected item are returned and replaced by vendors on timely basis or not. 3. Verify return recorded on timely basis in books or not. 4. Ensure	Storing of rejected and return to vendor	4 Month Mis of rejected items 20 Debit notes for rejected material	Analyse ERP quality, GRN records and Vendor's ledger to establish following: - Debit note raised to vendor or not for quality rejection. - GRN reversal in case of rejected material - GRN records for replacement

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			5. Perform assessment in case of high rejection in the material supplied by the vendor 6. Debit notes should be raised immediately for all rejections and return to vendors. 7. Credit to service vendors provided only for satisfactory services only.		material consumed after quality check only. 5. Monthly assessment of vendor wise rejection to take appropriate action against regular default vendors. 6. Debit note raised for rejected material and approved by appropriate authority. 7. Verify rejected material with advance paid vendors. 8. Check whether services are not performed as per agreement, credit not passed on to vendors for same.			by vendor against same PO. - Material are issued after quality approval only.
		Delay in clearing and forwarding of imported	The report on demurrage charges	As per company policy	Check the Demurrage charges paid and	Demurrage charges due to delay in clearing	Demurrage charges ledger	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		goods.	incurred due to delay in carrying and forwarding of imported items is reviewed by the designated person on a monthly basis. Also, these charges are separately disclosed in the MIS for Sr. Management review.		justification for the same.		30 imported invoices	
		Unauthorised or Inaccurate release of payments for transporter dues.	All transporter claims are authorised by the Sr. Manager - Stores prior to payment by Accounts. This is based on the agreements with the vendors / transporters.	As per company policy	1. Check the supporting for the claims viz. agreements, if any. Rate contract should also be reviewed for any changes in petrol/ diesel prices. 2. Check reconciliation of purchase register with transporter invoice to avoid duplicate booking.	Transporter charges authorizatio n	50 transporter invoices or as per quantum of business of company.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					3. Check lorry documents for freight payment.			
		GST Input Credit not availed / Short / Excess availed	Monthly reconciliation of GST Input Credit account and register is done both by Stores and Accounts.	As per company policy	1. Check the GST Input Credit reconciliation for long outstanding items and justifications and action taken for the same.	Periodicity of reconciliation and reasons for outstanding items	3 months reconciliation	Analysis GSTR-2A report with purchase register to indemnify cases where GST credit available as per portal but invoice are not booked or vice versa.
	Invoice Processing	Invoices may be booked incorrectly	Before any invoice is approved for booking, AM - Accounts performs a three-way match of the PO, GRN and Invoice	As per company policy	1. Check that the invoice is supported by duly authorised PO and GRN.	Three-way control PO, GRN and Invoice	50 invoices or as per quantum of transaction	Analyse and compare PO Records with GRN records to verify accuracy in booking value. Verify transporter charges GL or clearing & forwarding or suspense GL where excess invoiced value (More than PO value) may be provided

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
								to verify approval process. Analyse ERP data of various expense GL with Goods receipt / Service clearing account to check expenses rooted through three-way control system i.e. PO, GRN/SRN and invoice instead of direct booking.
			In case of emergency purchases, the invoice is verified with the GRN /SRN and the subsequent approval obtained for the purchase from personnel authorised as per Authority	As per compan y policy	1. Check that the invoice is supported by GRN and post-purchase approval of the personnel authorised as per Authority Matrix.	Emergency purchase approval	50 invoices or as per quantum of transaction	Compare Invoice date and PO date to identify emergency purchase. (Invoice date should be after PO date). Verify ERP records where invoices booked without

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Matrix.					three-way control i.e. PO, GRN and invoice to check approval procedure.
		Duplicate booking of the invoice.	At the time of booking of invoice, invoice is defaced with the Stamp "Processed" by executive.	As per company policy	Check that the invoices are defaced at the time of booking.	Defacing of invoice to avoid duplicate booking.	50 invoices or as per quantum of transaction	Analyse Vendor Invoices for following: 1. Incorrect/ duplicate Invoices processed 2. Check for same invoice amount in the same period for same vendor.
			Once a invoice is booked, the supporting documents viz. GRN, PO, Indent are attached with it. Invoices without supporting, cannot be processed.	As per company policy	1. Check that the invoice is supported by duly authorised PO and GRN.	Supporting documents	50 invoices or as per quantum of transaction	Analyse POs value from ERP records and compare it with GRN value for accuracy in between.
		Unapproved invoices are processed.	The invoices before being processed are reviewed by	As per company policy	Check the approval of AM - Accounts on the invoice.	Invoice approval from designated authority	50 invoices or as per quantum of transaction	Analyse GRN and invoice record to identify the

284

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			designated authority.					following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
			Access rights to process the invoices are restricted to the personnel authorised as per the Authorities Matrix and are entered in Access Control List (ACL) in ERP system	As per company policy	Check the Access Control List for the access rights given to the authorised personnel.	Transaction performed as per access rights.	ACL	
		Delay in accounting of invoices	Statements received from vendors are reconciled with the vendor accounts in the accounts payable subledger quarterly and differences are investigated. This is reviewed by designated authority.	As per company policy	1. Check the periodicity of vendor reconciliation for appropriateness thereof. 2. Sample check the pending items in the reconciliations for invoices pending booking and confirm the reasons for same.	Timely booking of invoices	Reconciliation for 30 vendors	Analyse ERP data to compare invoice date, GRN date, Quality date, invoice booking date to verify timely processing of invoice.
			The list of Goods Received Not Invoiced (GRNI)/Service Receipt	As per company policy	1. Check aging of the Temp GRN raised for the material with Quality	Aging of GRN and material being held by QC	records of GRN with QC Liability provides for non-booked	Analyse ERP data to compare invoice date, GRN date, Quality date,

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Note and the items with Quality Control are reviewed on a monthly basis to ensure that there are no delays in booking the liability.		Control department and the GRNIs. 2. Ensure that the same are accounted in the books as liability in the suspense accounts.		GRNs	invoice booking date - to verify timely processing of activities - to check vendor liability booked on timely basis so that reconciliation gaps should be zero or minimum.
		Booking of related expenditure and cenvat along with invoice may not be booked.	1. GST Input credit are obtained for all eligible credits, and it is duly verified at the time of recording of invoices. 2. All the related expenditure, such as toll tax, cess, freight, etc., are recorded as cost of material or service. 3. Appropriate deduction and	As per company policy	1. Check cenvatable credit provided along with invoice booking 2. All related expenditure like toll tax and freight booked along with goods/services 3. TDS and other deduction as per law are done and recorded	Credit booking and deduction	50 invoice and as decided with management	NA

286

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			recording of TDS are done wherever applicable.					
		Delay in raising debit/ credit notes	Statements received from vendors are reconciled to the vendor accounts in the accounts payable subledger quarterly and differences are investigated. This is reviewed by AM - Accounts	As per company policy	1. Check the vendor reconciliation for the periodicity of reconciliation. 2. Sample check the pending items in the reconciliations for debit / credit notes yet to be raised. Confirm reasons for the same.	Timely issue of Debit / Credit Notes	Reconciliation for 30 vendors	Analyse time taken to issuing debit / credit notes from the date of booking of invoices or date of receipt/return of material
		Unauthorized debit/ credit notes may be raised	The debit / credit notes are approved by the personnel approved in the Authority Matrix. The same entered in the Access Control List existing in the ERP system	As per company policy	1. Check that the access control list defined in ERP system is as per the approved Authority Matrix. 2. Check that adequate back up / supporting documents exist for issuing debit / credit notes.	1. Approvals for debit/credit noted 2. Reasons for issuance	30 debit / credit notes	Analyse number of debit / credit notes issued vis-à-vis number of purchases made. Analyse value of debit / credit notes issued vis-à-vis value of purchases made. To check

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
								efficiency of purchase
	Accounting and payable	Unauthorised payments	The payment voucher with required supporting's is reviewed and authorised by the personnel authorised as per approved Authority Matrix. The authority matrix is entered in the Access Control List (ACL) in ERP system. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved. In case cheque payment, when cheque is handed over to vendor representativ	As per company policy	1. Check that the Access Control list in ERP is as per the approved Authority Matrix. any changes to the authorised signatory to the bank transactions should be authorised by Board and intimated to the Bank immediately. 2. Check that requisite supporting is attached with the payment voucher. 3. Check that the supporting is defaced for the approved vouchers. 4. Sign of vendor's representative.	1. Access Control List 2. Approved supporting documents.	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	Analyse Vendor payment record during the review period to identify the following: 1. Unauthorised users performing transactions. 2. Conflicting transaction rights granted to same person.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			e and acknowledgement obtained.					
			At the time of processing a vendor invoice for payment, designated authority is required to identify and set off all the advances pending adjustment for such vendor.	As per company policy	1. Check that there are no amounts pending adjustment for vendors where all the invoices have been paid. See justification for exceptions. 2. Scrutinise the vendor accounts / party accounts to check the cases of segregation of amounts to avoid authority matrix. 3. Vendor advance should be adjusted as er contract terms. 4. Check cases of advance paid contractor but work performed with slow pace, leads	1. Advance amounts in vendor accounts pending for adjustments, 2. Multiple payments on same or nearby date	30 vendor accounts and per business need	Analyse vendor payment for following 1. Same vendor with same date-and more than one payment 2. Check advance is adjusted as per contract terms. 3. Check advance paid but without bank guarantee against the policy of the company.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					to financial loss to the company.			
			The listing of vendor payments is reviewed prior to release of payment by the personnel authorised as per approved Authorities Matrix	As per company policy	1. Check that the evidence of review on the vendor payment list	Review of payment	30 vendor payment lists	Analyse vendor payment record during the review period to identify the following: 1. Unauthorized users performing transactions 2. Conflicting transaction rights granted to same person.
			The personnel making the payment (either through cheque / DD / wire transfer) are authorised to do so as per the approved Authority Matrix.	As per company policy	1. Check the approval for authority to make the payment. 2. Check whether the same has been communicated to the bank.	Approval of payment to vendors	Authority Matrix	
			Management periodically reviews the returned paid cheques for unauthorised signatures, alterations and / or alterations	As per company policy	1. Check the evidence of the management review.	Review of returned cheque	Returned cheques	Analyse total cheque issue during the period and returned to verify following: 1. Control at the time of issue of

290

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
								cheques 2. Period for which cheques returned due to alteration/mismatch, etc.
		Payments are made to incorrect vendors	1. The payment voucher with required supporting is reviewed and authorised by the personnel authorised as per approved Authorities Matrix. The authority matrix is entered in the Access Control List (ACL) in ERP system 2. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved.	As per company policy	1. Check that the ACL in ERP is as per the approved Authority Matrix. 2. Check that requisite supporting are attached with the payment voucher. 3. Check that the supporting are defaced for the approved vouchers.	1. Access Control List 2. Approved supporting document.	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	NA
			1. The listing	As per	1. Check that	Managemen	30 vendor	1. Data

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			of vendor payments is reviewed prior to release of payment by the personnel authorised as per approved Authorities Matrix 2. Cheques / DD are restrict endorsed by the preparer to ensure that they are paid to specific payee	compan y policy	the evidence of review on the vendor payment list	t review before release of payment	payment lists	analysis of the Open/Long pending advances which are not adjusted 2. Analyse data for Instances of delay in payment made to MSME vendors over 45 days 3. Whether liability write off approval are obtained from management as per policy.
			Management periodically reviews the returned paid cheques for unauthorised signatures, alterations and / or alterations.	As per compan y policy	1. Check the evidence of the management review.	Managemen t review for returned cheque and reissue	Returned cheques	Analyse total cheque issue during the period and returned to verify following: 1. Control at the time of issue of cheque. 2. Period for which cheques returned due to alteration/mi smatch, etc.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
		Credit terms may not be utilized effectively.	1. Payment are processed for approved invoices as per agreed payment terms to optimize on using credit period and efficient utilization of working capital. 2. Vendor ageing is prepared and reviewed by the Finance head on weekly basis to ensure all overdue payments are processed.	As per company policy	1. Check payment and credit terms with vendors 2. Review document of vendor ageing on weekly basis	Credit terms and weekly review of overdue	check ledger of 10 major vendor 10 weekly review of overdue payment	Analyse ERP vendor ageing of different month to verify payment made after utilizing credit terms to maintain working capital balance.
		MSME Vendor not paid on timely basis	Payment to MSME vendors is reviewed and made within defined timelines as per terms of agreement or timelines defined under Micro, Small and Medium Enterprises	As per company policy	1. Check ageing of MSME vendors on different date/months	Timely payment to MSME vendors	Check Ledger of 20 MSME vendors	1. Data analysis of the Open/Long pending advances which are not adjusted 2. Analyse data for Instances of delay in payment made to MSME

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			Development Act, 2006 or amendments thereafter (45 days), whichever is earlier.					vendors over 45 days
		GST credit reconciliation and payable more than 180 days	Reconciliation of eligible GST credits on GST portals with GST Input credit available and deposited are performed periodically.	As per company policy	1. Check monthly reconciliation sheet of GST credit as per books with Portal and deposited.	GST reconciliation	3 Month reconciliation	Analyse vendor wise credit available at portal and credit availed/booked by the company and reason for non-utilization/booking and vis a vis cases.
			If payment to vendors is not made within 180 days then GST credit related to particular amount needs to be reversed.	As per company policy	1. Verify vendors ageing and identified cases where payments are outstanding by more than 180 days. 2. Check GST return and verify credit related to this vendor is reversed in particular month or not.	GST credit reversal in case of non-payment within 180 days.	1. Vendor ageing 2. GST returns for reversal purpose	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					3. Tracker should be maintained by the company for credit reversal and subsequent utilization after payment.			
		Duplicate payments	1. The payment voucher with required supporting is reviewed and authorised by the personnel authorised as per approved Authority Matrix. The authority matrix is entered in the Access Control List (ACL) in ERP system. 2. The supporting documentation is cancelled or defaced, once it is reviewed and payment	As per company policy	1. Check that the Access Control list in ERP is as per the approved Authority Matrix. 2. Check that requisite supporting are attached with the payment voucher. 3. Check that the supporting are defaced for the approved vouchers.	1. Access Control List 2. Approved supporting document.	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
			voucher is approved.					
		Non-receipt of material against advances	The listing of Open POs is reviewed on a monthly basis to check the cases of delayed supplies/contractor wherein advances have been released to them. This is reviewed by the personnel authorised as per the approved Authority Matrix.	As per company policy	1. Check the due dates in the open PO / Contracts. 2. Check the reasons for delays in supplies. 3. Verify advance GL for long pending unadjusted advance.	1. Open PO with corresponding advances 2. justification for delays	1. Open PO listing 2. Unadjusted advances GL	Analyse PO list (where timeline of supply/service has been expired) and compare with advance GL to identify cases where advance unadjusted and vendor POs are also outstanding.
			Ageing of the party balances is reviewed on a monthly basis and account reconciliation is done on a quarterly basis	As per company policy	1. Check the debit balances appearing in the supplier's account and ageing thereof 2. Check whether any unauthorized advance has been given to the supplier (this needs to be checked with	1. Approvals, 2. Amount, 3. Receipt of material 4. Due date	Vendors Account and the Advances Aging statement	Analyse various figures reported in MIS vis a vis the details appearing in ERP system to identify instances of incorrect reporting.

296

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size (* may vary upon organization size, policy, decision)	Data analytics performed
					the justification provided and the Authority Matrix) 3. Check whether the advances have not been adjusted correctly while accounting for receipt of goods.			
		Wrong Foreign exchange rates used for conversion of foreign currency invoices.	Weekly foreign currency rates are updated in the ERP system by the personnel authorised as per the Authority Matrix. The rights to update the masters are restricted as per Authority Matrix the source of foreign exchange rates should also be approved by Management.	As per company policy	1. Compare the rates applied for invoice processing with the RBI rate.	Exchange rate applied as per RBI rate	Forex rates in 10 weeks	NA

Purchase to Pay – Capital Items

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
Procurement of Capital Items	General and entity level control	Procurement policy and Authority matrix may not be prepared or approved by Board of Director (BOD).	The organisation has clear and comprehensive (up to date) capital procurement policy approved by Board of Directors (BOD) or designated authority. Due consideration given to: - Time (speed vs certainty of completion date) - Cost (price level vs cost certainty) - Quality (functionality and performance)	As per company policy	1. Check updated and comprehensive capital procurement policy approved by BOD or designated authority. 2. Check it addresses all attributes related capital items to procurement.	1. Approved Capital procurement policy 2. Completeness	Capital item procurement policy approved by BOD	NA
			1. The organisation has clear and comprehensive (up to date) Delegation	As per company policy	1. Check capital item procurement DOA/DOP is available and approved	Approved DOA/DOP for capital purchase	Approved DOA/DOP from BOD	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			of Authority (DOA)/ Delegation of Power (DOP) and Authority Matrix. 2. Authority matrix is approved by Board of Directors, defining the authorities for approving capital purchase transactions or performing various transactions during the purchase process.		by BOD.			
		Inadequate Segregation of Duties and access rights which may result in fraudulent / unauthorised transaction.	1. Document defining appropriate Segregation of Duties (SOD) is in place. 2. Access rights (Write / Read / Delete / Modify) to various people in the origination	As per company policy	1. Check documented SOD and Access right list. 2. Verify same SOD and Access right also entered in system for approval of transactions. 3. Verify evidence of periodic review of	1. Documented SOD, Access right 2. Periodic review	1. SOD 2. Access right List 3. Half yearly review document	Analyse transaction carried out during the review period to identify the following: 1. Unauthorised users performing transaction. 2. Conflicting transaction rights granted to

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			of reviewed periodically to ensure appropriate SOD and avoid any unauthorized transactions. 3. Periodic Review of Segregation od Duties and Access rights is conducted.		SOD and Access rights in ERP system.			same person. 3. Internal Auditor to review the circumstances of conflict of interest.
		SOP may not be defined to ensure consistency and standardisation of operations.	1. The organization has clearly defined Standard Operating Procedures and are in place. 2. Should define sequence of activities, Roles and Responsibilities, Key Performance Indicators (KPIs), Timelines and Frequency of activities along with various	As per company policy	1. Check SOP available and complete in all aspect of roles, KPIs, Timelines and frequency of activities, etc. 2. Check when SOP updated last and enquire the reason for not updating the SOPs, in case, not updated for long time.	Approved SOP and completeness	Updated SOP	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			documents to be maintained by the organization for performance of capital transactions.					
		Review system to mitigate risk of inappropriate transaction and project progress may not be in place.	1. The organization has set up an appropriate Management Information System (MIS) for regular monitoring of operations and financial activities by senior/ top management. 2. Appropriate Risk Management System (RMS) is in place to identify and mitigate various risk. 3. Fraud Risk	As per company policy	1. Check MIS for monitoring of capital procurement/ project operation. 2. Check RMS in place to identify and mitigate risk and its functioning related to project. 3. Fraud risk assessment activity conducted, and control deployed. 4. Check project milestone is achieving on timely basis.	1. MIS 2. RSM 3. Fraud assessment activity	MIS for 3 months Action and step taken to identify and control fraudulent activity.	Analyse various figures reported in MIS vis a vis the details appearing in ERP system to identify instances of incorrect reporting.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			Assessment activity is conducted, and fraud risk are identified along with relevant controls to avoid any fraudulent transactions.					
	Annual Capital procurement budget	Procurement budget may not be prepared and monitored on regular basis to avoid deviation in future.	1. Base for preparing budget and Capital budget is approved by BOD before start of financial year. 2. Monitoring of Budget Vs Actual is done on monthly basis and review of action plan wherever required.	As per company policy	1. Check Annual Capital Procurement Budget is approved by the designated authority and agreed with / communicated to the delegated authority well in advance. 2. Review of periodic monitoring of deviations from the approved budget conducted along with reasons for deviations, if any. 3. Action	Approved budget and subsequent monitoring	Approved Budget for the year Budget Vs actual MIS for 3 months and upto date	Verify the accuracy of the Budget vs Actual MIS from the independent data source e,g, transactions recorded in ERP to identify instances of incorrect monitoring or Budget overrides. Understand the reasons for variance and not limited to (a) Incorrect preparation of budget. (b) Accounting and classification of errors.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
					plan is documented and adhered for avoiding such identified variance in future.			(c) Use of budgetary provision for other purpose, etc.
		Absence of formal planning policy may lead to increased capital cost or increased inventory levels.	An annual plan is developed for defining the capital requirement for each of the departments. The plan is duly approved by the different HODs and CEO. The plan includes the following factors (regarding procurement): 1. Capital items required 2. Capital requirement (Owned or financed) 3. Authorisation Based on the Annual	As per company policy	1. Check approved capital procurement plan exist and prepared after considering production plan and business plans. 2. Check whether project/procurement activity are as per plan and check process is in place to identify and report/MIS in case of deviations.	1. Timeliness followed in updating the plan. Completeness of defining material requirement, Vendor identification, Vendor communication and Authorizations	1. Annual Plan 2. MIS for 3 months	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			plan, purchases department identifies the suppliers for the capital items, Pre-qualification and do agreements with the suppliers, communication of the plan to the suppliers, lead time for delivery, periodicity of supply, etc.					
	Indenting and approval	Indent raised / approved for purchase when there is no requirement for capital items.	The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to procure capital items. The Authority Matrix is configured in the ERP system in	As per company policy	1. Check that indents are approved in accordance with the Authority Matrix. 2. Check whether Authority Matrix is configured in the system in Access Control List for system control point of view.	1. Approvals for indent 2. Access control list	Cover capital category and approval matrix which combinedly cover more than 40% of capital purchase.	Analyse transaction carried out during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			Access Control List (ACL).					
			A Monthly Budget Vs Actual review is conducted considering department budgets and major capital expenditures incurred are identified. Any unauthorized expenditure or double processing of significant expenditure would be identified in the review meeting.	As per company policy	1. Check that all the indents which get converted into PO are reported as part of MIS for variance analysis (viz. budget vs. actual).	Quantity reported in MIS	1. MIS - 3 months	Verify the accuracy of the Budget vs Actual MIS from the independent data source, e.g., transaction recorded in ERP to identify instances of incorrect monitoring or Budget overrides.
			1. Budget for particular capital expenditure are made at the time of indent approval and amount are deducted from total capital expenditure budget.	As per company policy	1. Check all budget for particular capital expenditures are blocked at indent approval stage only and could not be increased. 2. Check any increase in	1. Budget freezing at indent stage 2. Approved of deviation at later stage	1. Activity/project wise capital expenditure budget tracker. 2. 10 cases of deviation from approved budget.	Analyse budget for 2 to 3 year period and identify following: 1. Number of projects where budget increase vs total no. of project executed/ awarded. 2. Total value of

305

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			2. If value of capital expenditure is higher from budget at later stage, approval of appropriate authority are required depending on increased in amount or define limit as decided by Board. 3. Reason for higher value should be supported by evidence and documented.		particular capital expenditure against freeze budget should be approved from designated authority with proper documented justification. 3. Check whether working done by management for total cost to be incurred to complete project.			budget increased to analyse effectiveness of planning in contract awarding process.
		Unauthorised indents may be raised for purchases.	1. The indent is reviewed and approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying the need to	As per company policy	1. Check that the indents are approved in accordance with the Authority Matrix. 2. Check budget availability while approving of indents. 3. Check	1. Approvals for indent 2. Budget availability at the time of indent approval.	1. Cover different items for different user departments to cover major & medium value. 2. ACL	Analyse the total budget approved for the department before start of year and total value of indent approved during budget period to verify.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			procure of capital items. The Authority Matrix is entered in the ERP system in Access Control List (ACL) 2. Budget availability with department is considered before approval of indent otherwise indent could not be approved. 3. Budget are approved by appropriate authority to release indent.		excess budget are approved from authority in case of total budget exhausted by department before release of indent.			-Indent approved more than original budgeted without obtaining approval of excess budget which is against the policy of organization.
			The system, does not allow changes to be made to the approved indents. They can either be cancelled	As per company policy	1. Check the access control list to check that no one other than HOD has modification access for indent and access to cancel	1. Approvals for indent 2. Access control list	System walkthrough and check system allowed to make changes in approved indent.	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			or processed for PO. The amendment rights are available only with the Head of the Department (HOD).		indent is with Managers in respective user departments / Cost centers.			
		Indent does not prescribe the correct technical specifications of project/capital items required resulting placing in incorrect order.	1. Specifications are mandatory field in the indent and cannot be passed (in ERP). 2. Maker-checker controls is established to verify completeness and correctness of all details.	As per company policy	1. Check the exception report generated from ERP for indents raised without any specification. 2. Check the rejection report for the items rejected due to incorrect specification.	1. Rejections due to incorrect / missing specifications	Exception report and Rejection report for the period of audit	Analyse ERP data to compare specification as per indent and corresponding specification in PO to identify deviation. Further verify above deviation with rejected GRN at quality stage to establish rejection due to wrong purchase against indent.
		Indent sent to purchase department with delay may	1. Purchase requisition is sent to purchase department	As per company policy	1. Check indent reports to verify timely sharing	1. Timely conversion of indents into POs	Indent report compare with PO reports	Analyse ERP data of indent and PO to identify following:

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		hamper procurement activity.	within defined timelines. 2. Timeline are defined for approval of indent and issued further to procurement team for processing.		and conversion of approved indent into PO. 2. Check list of indent raised by users department but not approved yet. 3. Check list of approved indent sent but no action initiated by purchase team on same.			1. Time gap between indent raised and approval/ release of indent 2. Time gap between indent release and PO approval date. 3. Expected date of material as per indent along with deadline to vendor in PO for supply. To calculate probable losses due to delay in approval at different stages from indent to PO.
		Indent does not prescribe the correct technical specifications of project/capital items	1. The indent is reviewed and approved by the authorized personnel (as per the	As per company policy	1. Check that the indents are approved in accordance with the Authority Matrix.	1. Approvals for indent 2. Access control list	1. System walkthrough for approval procedure and specification.	Analyse Purchase requisition transaction to identify the following: 1. Incomplete

309

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		required resulting in incorrect ordering.	limits set out in the approved Authority Matrix), signifying the need to procure material. The Authority Matrix is entered in the ERP system in Access Control List (ACL) 2. Indents without the specifications are treated as incomplete since the quotations cannot be obtained for the same.		2. System walkthrough to check indent without specification.			or incorrect details in PR. 2. PRs backdate or raised after ordering. 3. PRs are created for quantity in excess of the budgeted amount. 4. Requisition quantity in excess of average consumption or in spite of high inventory levels. 5. Open PRs not reviewed and closed.
			In case, the capital items are rejected by Quality Control department or shop floor, reasons for the same are reviewed to ensure that the same were not due to	As per company policy	1. Check the Material Rejection list and if they are due to incorrect specifications. 2. Check specification of item in indent and PO compare	Capital item specifications mentioned properly with complete description	1. Rejection report along with reasons.	

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			incorrect specifications mentioned on indent. Project activity are rejected by quality department if wrong item is utilized against specified BOM item.		them with BOM specifications.			
		Indents / PRs are not used when purchasing capital items.	All supporting documents (Indents/vendor quote analysis sheet/vendor quotes, etc.) are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).	As per company policy	1. Check the PO review and approval process. Check that the PO is supported with a duly approved indent.	Supporting documents (including indents)	30 PO or as per business need	Analyse capital PO Records with Indent Records to verify each order is supported by indent.
	Vendor Selection and Master Management	Contractor chosen is not competent resulting in inferior quality in execution of projects.	Defined process for vendor evaluation and approval exists and includes the following:	As per company policy	1. Check the approval for technical evaluation and supporting documents thereof	1. Approvals of plan evaluations 2. Supporting for evaluations	30% of new vendors or 10 whichever is higher	1. Analyse vender list of current year vis-à-vis previous year to identify addition of new

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			- technical and commercial evaluation by cross functional teams, - approval authority - single vendor justification like for imports or critical items, OEM item		2. Check approval for commercial evaluation and supporting documents thereof 3. Check justification for exceptions, if any 4. See the overall approval including the party in approved vendor list			vendors to increase competition. 2. Analyse sufficient no. of vendor were not identified for each type of capital work get best competitive rates. 3. Check quotation were asked form incompetent vendors on regular basis to give contract to desired parties.
		Incomplete / Inaccurate vendor records	1. Vendor account creation form contains key details of vendor, i.e., Name, PAN, Address, Contact Details, GST registration details, Bank Account, place of	As per company policy	1. Check approved format for vendor account creation and all requests should be received in that format only. 2. Complete details of vendors as filled in that format	1. Approved format for creation/alteration 2. Completeness and accuracy	30% of new vendors or 10 whichever is higher.	Analyse Vendor Database for any duplicate vendor records and corresponding purchase/ payment transactions with such codes.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			business, MSME certificate, Turnover details for e-Invoicing, etc. 2. Mandatory field are defined in the system without which vendor code is not allowed to be created in the system.		along with field that is not applicable in any case. 3, Check system controls to avoid duplicacy at code level, PAN and GST level, address and contact level.			
		Selection of inappropriate vendor	1. Market research are carried out from time to time to identify prospective contractor for the required capital item. 2. Appropriate due-diligence and financial background check are performed as per approved	As per company policy	1. Check the list of pre - qualified contractors for different type of capital requirements of organization. 2. Due diligence process is followed financial background is checked as per checklist. 3. Frequency	Management review and approval mechanism to identify prospective contractor.	Select 2 contractor from each major category of projects and capital items. Or as per business need	1. Analyse that vendor list as are updated by company on frequent basis and should have sufficient vendors who actively participate in bidding. 2. Check company should not be dependent on some vendors for quotations.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			checklist and the contractor is added in the approved list after due approval. 3. Contractor who do not participate in bidding process, are reviewed and removed after obtaining NOC. 4. Contractor is selected on basis of Pre - qualification and merit basis. After selection of vendor, list is approved by designated authority before quotation.		of updating list and identification of non-responsive bidders. 4. Check approval of designated authority for selected vendor for quotation.			
			1. Open tender system is followed for high value	As per company policy	1. Check open tendering used by the company	Tendering as per policy of the company.	PO Records	Analyse ERP Open tender, Limited tender data and verify

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			transaction or critical items as per the organization policy for inviting all possible vendors for indented procurement. 2. Limited tender requests for quotation are given to the pre-approved vendors for selected category of capital items or value below the define limit as per the organization policy.		for high value transactions or critical items. 2. For other items, limited tender requests are sent to all approved vendors. 3. Check method used for open tendering, i.e., no. of advertisement in different newspapers, coverage area and in different languages to create competition among vendors. 4. Check NOC are obtained from vendors who did not sent quote to check they obtain quote			tendering done as per policy of the company.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
					request but would not participate by their will.			
			Standard Request for Quotation/ tender are prepared and circulated to all parties for inviting quotations as per the organization policy.	As per company policy	1. Check standard format of request is approved and used by department. 2. Check changes should not be done by anyone other than addendum after approval. 3. If quotation provided in other than standard format should be rejected.	Standard format used for Tender /quotation	For 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher	NA
			1. Technical criteria are defined in the bids as per the requirement of user department and approved by HOD purchase. 2. Marks should be	As per company policy	1. Check technical criteria of selection of vendors are define in bids and matched with requirement as specified by user department and approved	1. Defining of technical criteria 2. Deviation approval	for 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher.	Analyse tracker to verify technical qualification, financial qualification and other details are obtained and are considered for all bidders. Report exception

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		allotted to bidders on the basis of technical qualifications and no deviation allowed.			by HOD. 2. Check technical qualification document provided and accordingly marks allocated to bidders. 3. Check for any deviation from technical qualification, verify approval obtained from designated authority or not.			and check deviation approval is obtained.
		Possibility of vendor favoritism	Same timelines and processes are followed for all parties and deviation are approved by designated authority except procurement of low value / select category	As per company policy	1. Check bidding document and process to verify timeline and process are common in case of all tendering parties. 2. In case of deviation, approval obtained from	1. Same and timely process for all parties 2. Deviation approval	for 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher.	Analyse time tracker of: - Submission of technical and financial qualification document and approval thereof - Submission of financial

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			as per the procurement policy.		designated authority.			bidding and approval. - to verify all process are time bound for all vendors. Report exceptions and check deviation for same.
		Selection of inappropriate contractor or high-cost procurement of capital goods.	1. Comparative quotation analysis sheet drawn before purchases are authorized. 2. If lowest quotation is not accepted, appropriate justification may be documented and approved by designated authority. 3. Quotations are opened and registered, and a comparativ	As per company policy	1. Check whether comparative sheet is prepared or not. 2. Check Justification and approval in case of selection of other than lowest bidders. 3. Check whether quotation opened, registered and comparative approved by authorised persons. 4. Check quotation opened in presence of tendering	1. Approval of comparative sheet 2. Deviation approval 3. Signing by tender committee.	For 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher.	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			e chart is prepared and authorised. 4. Quotations are opened in presence of tendering committee only for the technically qualified bidders.		committee for technical qualified bidders and sign off by them. 5. Check even order given to lowest bidder but whether earlier project is performed within time and approved cost (Check previous history of vendor).			
			Approval note with all relevant justifications is documented for selected vendor and same is approved by all designated authorities as per the Delegation of Authority. Adequate approval from Board	As per company policy	1. Check justification must be prepared and approved by designated authority. 2. Check justification must be supported by evidence, i.e,. project delivered in past. 3. Check justification	Approval note with Justification to select vendor	for 5 major tenders and 5 major RFQ process or cover 50% tender whichever is higher.	Analyse justification given in approval note with actual work performed by vendor or with previous work performed from ERP records. 1. Quality rejection 2. Timely delivery 3. Qualitative delivery

319

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			of Directors is in place for purchasing from related parties.		given in approval note. Verify justification with actual work performed by vendor during audit period or record of previous work performed by same vendor.			
		Non-compliance with requirement of Companies Act and other regulations.	1. Adequate approval from Board of Directors is in place for purchasing from related parties. 2. Disclosure of related parties and purchased from related parties is ensured. 3. Adequate documentation is in place to justify appropriate pricing of	As per company policy	1. Check BOD approval obtained in case of related party's purchase 2. Check disclosure note given in financial statement. 3. Justification documented for purchase from related parties.	BOD approval and justification	All related party purchase	Analyse ERP data to check rates of other vendor with same scope as of related parties to verify transaction are performed at arm's length basis or not.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			purchases from related parties.					
		System control may not be implemented for modification at RFQ level, Quotation level, approval level may lead to unauthorised purchase.	1. System are not allowing to raise RFP without approved requisition in place. 2. All vendor quotations and bid are locked for modification and opened in presence of designated authorities. 3. Selected party is identified and locked in system after all approval as per the requirement of Delegation of Authority. 4. System is not allowing backdating / modifying any information	As per company policy	1. Do system walkthrough for RFQ without approved requisition. 2. System walkthrough for modification in quotation and locked identified parties. 3. Check rates of vendors in final comparison sheet matched with rates in individual quotes. 4. Verify all approved vendor with final vendor comparison list. 5. Change log must be available for all modifications and reviewed by	System control for modification at RFQ level, quotation level, Identified vendor and other information.	System walkthrough Verify final comparison sheet with individual quotes.	Analyse ERP or other software's final rates for all vendors with original rates quoted by individual vendor to identify difference.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			once process is completed		authorised person.			
		Unauthorised updates / alterations may be made to vendor master.	1. Updates (Additions / Alterations) to the vendor master data done only with the approval of authorised persons on the basis of requisition in proper format from users. 2. Also, the access to make additions / alteration to the vendor master is restricted to personnel authorised as per approved Authority Matrix. The Authority Matrix is entered in the Access Control List (ACL) in the systems. (Normally	As per company policy	1. Check the ACL is as per approved authority matrix. 2. Check that the person making the addition/ alteration is authorised to do so. 3. Verify vendor creation/alteration forms are approved by authorised persons.	1. Approvals for addition / alteration, 2. ACL	40% of addition/ alteration or 20 whichever is higher.	Analyse transaction carried out in vendor master data during the review period to identify the following: 1. Unauthorised users performing transactions. 2. Conflicting transaction rights granted to same person.

322

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			additions/ alteration rights provided to IT).					
		Inaccurate updation of the vendor master data.	Recorded changes in the supplier master file are compared to authorized source documents by authorize person to ensure that they were entered accurately.	As per company policy	1. Check that information so entered is reviewed and authorised. 2. Check with supporting document that the information has been Completely & Accurately entered.	1. Supporting documents 2. Approvals	40% of alteration or 20 whichever is higher.	Analyse vendor master data to validate following: 1. Matching of PAN with GST 2. GST no. with state code 3. Length of PAN and GSTIN 4. Length of mobile number 3. Check bank account no. provided or not. Analyse Vendor Database is comprehensive, and all vendor details are complete and accurate – *viz,* Name, PAN, Address, Contact

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
								Details, GST registration details, place of business, etc.
		Audit logs for changes in vendor master may not be available and reviewed leads to unauthorized changes.	Request to change in supplier master file data are logged; the log is reviewed to ensure that all requested change is processed timely.	As per company policy	1. Check the requests log to ensure that there are no long pending change requests.	1. Outstanding list in Request log.	1. Request log	NA
		Critical vendor data is not complete and upto date	1. Vendors are classified correctly as MSME or not in master data and updations are done on yearly basis. MSME certificates are obtained on yearly basis. 2. List of vendors who have to do E-Invoicing are prepared and bills	As per company policy	1. Mails sent to vendor for MSME and turnover declaration. 2. Vendors declaration received and vendors updation done basis of declaration. 3. E-invoicing by specified vendors done or not	1. MEME and E-invoicing Vendor listing.	20% of capital vendors	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			are processed accordingly.					
			Requests to change supplier master file data are submitted on pre-numbered forms; the numerical sequence of such forms is accounted for to ensure that all requested changes are processed timely.	As per company policy	1. Check the requests log to ensure that there are no missing request numbers. Alternatively, there should be number cancellation note on the log.	1. Sequence of the request forms used.	1. Request log	NA
			Supplier master file data is periodically reviewed by management for accuracy and ongoing pertinence.	As per company policy	1. Check the evidence of the management review.	1. Management review of supplier master	Management sign-off or approved file.	NA
		Risk of conflict of Interest of vendor.	1. As per Company's Code of Conduct, the employees are mandated	As per company policy	1. Check the employee declarations for compliance with ethical standards.	1. Declarations by vendors and by the employees.	1. Certifications from 30% employees. 2.Acknowledgement from 20%	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			to inform the concerned HOD / Superior where conflict of interest exists. 2. Employees are required as per Code of Conduct to certify compliance with the policy on an annual basis. 3. Also, the vendors are required to inform as per the standard terms and conditions printed on the PO, if they have any relations with employee in the organisation.		2. Check the vendor acknowledgements in the PO.		vendors or having 60% business with company.	
		One-time vendors are not subjected to same	1. There is an option of ticking "One time flag" which	As per company policy	1. Check by creating a dummy PO, if the vendor	1. Field validation to use code one time only.	1. List of one-time vendors 2. PO Records	Analyse ERP records for POs with pre-define

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		controls as for other vendors.	needs to be updated at the time of vendor creation. As a result, the vendor gets deactivated after placing one PO. 2. Specific vendor code is used for creating one-time vendors (e.g. 1000 for domestic and 1100 for import.)		flagged off as One-time vendor can be reused. 2. Obtain a list of One-time vendors and compare it with the PO Records to check whether one-time vendors have been used more than once.		3. System walkthrough	one-time vendor code and identify more than one PO are raised with one-time code from same vendors.
		Contractor performance not reviewed periodically.	1. Performance Appraisal of vendor is done once in a year for long term PO / Contract and quarterly for short term PO / Contract. 2. Based on the evaluation, Approved contractor	As per company policy	1. Verify whether the contractor appraisals have been done annually & quarterly as the case may be. Verify department wise list of vendor and total appraisal done during audit period by each	1. contractor Performance evaluation and appraisal.	1. for annual appraisal – check appraisal of 30% contractor or 15 whichever is higher. 2. Same for quarterly appraisal.	Analyse PO record with GRN records to identify vendor wise: - Cases of quality rejection - Case of late delivery against PO terms, - Cases of less quantity delivery against PO quantity

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			list is updated. Respective departments are responsible for doing the contractor appraisals. 3. Based on the same and subsequent discussions with the respective department, accordingly, purchases department revises the approved contractor list.		department. 2. Verify updation of the approved contractor's list on the basis of appraisal, Check list is updated on the basis of appraisal only. 3. Mails sent to contractor management on basis of performance analysis to take action otherwise remove it from approved vendor list.			to scertain 1. Vendor with low performance evaluation have high share of business 2. Action taken against regular default vendors.
		Dummy / inactive/un satisfactory performance contractor exists.	1. Contractor that have not been used for a significant period of time are reviewed by purchase team and marked for deletion by	As per company policy	1. Compare the active vendor listing (VLOOKUP) with the PO listing for the year. 2. Scrutinise the vendor Records	1. Dummy / Inactive vendors accounts	1. Active vendor listing 2. PO Records 3. Performance evaluation report	Analyse Vendor master data vs capital PO list of 4-5 years to ascertain following: 1. Blocking of vendors or not with whom

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			the application, if appropriate. 2. Ensure contractor are timely blacklisted wherever required for unsatisfactory performance as per the defined policy. 3. Capital vendors are required even after 4, 5 or 10 years for spare parts and OEM items. So, approval is obtained from user department before removal. 4. Vendors are restricted for award of contract, who are not engaged with organizatio		for vendors with common / dummy names or details. 3. Unsatisfactory vendors are removed after performance evaluation or not 4. User department approval for removal of capital vendor. 5. Check vendors are in master data, but work or transaction could not perform with them due to restriction or blockage. 6. Check process to obtain updated KYC document if vendors are used after defined			organization had no transaction. 2. Restrict to use vendor code for non-submission of updated KYC documents if not blocked.

329

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			n from long period.		period.			
	Ordering	Department approval may not be obtained before raising indent for capital item.	1. Project is approved by the department side along with complete details of projection, cash inflow, Cash outflow, payback period. 2. Customer approval for go ahead are obtained on project if needed. 3. BOD or designated authority is approved the project and provide go ahead for further feasibility.	As per company policy	1. Check whether approval of marketing team along with customer obtained before raising indent. 2. Whether approval is sought from BOD or designated authority.	1. Marketing analysis along with customer approval. 2. BOD or designated authority approval.	15 projects approval 5 top 5 medium 5 lower	NA
		Project feasibility study may not be done by project team leads to wastage of money if	1. Project team has done project feasibility study and evaluate technical capability,	As per company policy	1. Check whether feasibility study with complete details and approval from project	1. Feasibility study or not 2. Comparison sheet for inhouse developme	15 projects Feasibility study and comparison sheet. 5 top 5 medium 5 lower	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		not able to execute effectively at later stage.	commercial and capacity evaluation. 2. Accordingly, project team has prepared cost sheet of inhouse development of tools or of purchase from third party and obtain approval from management.		side is obtained. 2. Comparative cost sheet of tool development inhouse or third party are approved from management side. 3. Check differential cost of Inhouse development or purchase from third party and calculate impact of it for full year. (Check reason i.e. capacity, technical staff, technology issue).	nt and third-party purchase approval.		
		Inadequate number of contractors are identified for RFQ.	1. Approver checks for sufficiency of quotations, before approving the PO.	As per company policy	1. Check for compliance with the purchase policy for identification of contractor for RFQ.	Number of contractor vis-à-vis the requirement of purchase policy.	Select items, contractor and corresponding PO's to cover each item category and 90%	1. Analyse vendor list are updated by company on frequent basis and should have sufficient

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			2. Justification for deviation from purchase policy is mentioned as remarks, which is also reviewed by the approver before PO is approved.		2. Check whether in case the requisite number of contractors were not available, due escalation procedure was followed. 3. Ask reason for significant change in rates of products. Check reason and approval of higher price.		major item contractor. (Cover at least 60-120 PO's or more depend on quantum of business)	vendor who actively participate in bidding. 2. Check company should not be dependent on some vendors for quotation purpose.
			All POs are required to be approved in accordance with the approved authority matrix. The Authority Matrix specifies the expenditure limits of the relevant personnel and has been entered	As per company policy	1. Check the approvals for the PO as per Authority Matrix. 2. In case, the approvals are not as per the authority matrix, ratification / justification for the same needs to be checked.	Prepare, Review and Approval of purchase order	Cover all item category and approval matrix which combinedly cover more than 30% of capital purchase.	Analyse transaction carried out in vendor master during the review period to identify the following: 1. Unauthorised users performing transactions. 2. Conflicting transaction rights grated to same person.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			into relevant software.					Also analyse purchase on same or nearby dates to identify cases of splitting of PO to override authority matrix.
		PO's raised with wrong quantity / rates / payment terms, etc.	1. PO is prepared by the designated person which is reviewed and approved by the person so authorized as per Authority Matrix. 2. The reviewer verifies the details in the PO with the supporting. 3. Access to create and approve PO by different users in system.	As per company policy	1. Check that the PO is supported with a duly approved indent. 2. Check that the PO is approved as per Authority Matrix. 3. Check creating and approving right should be with different person.	1. Quantity as per indent vis-à-vis PO 2. Approval for the PO	Cover all capital item category and approval matrix which combinedly cover more than 50% of capital purchase.	NA
		POs do not	All	As per	1. Check	Supporting	Cover all	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		contain accurate information.	supporting documents (Indents/vendor quote, analysis sheet, etc.) are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).	company policy	the PO review and approval process. 2.Check that the PO is supported with a duly approved indent. 3. To check accuracy of PO and verify it with customer source document, management approval process of project.	documents (including indents)	capital item category and approval matrix which combinedly cover more than 30% of capital purchase.	
			All POs are required to approved by the authorized personnel (as per the limits set out in approved Authority Matrix), signifying correctness and accuracy thereof. The Authority Matrix is entered in the ERP system in	As per company policy	1. Check that the PO are approved in accordance with the Authority Matrix. 2. Check that the PO cannot be created in absence of approved authorizer.	1. Approvals 2. ACL	Cover all capital item category and approval matrix which combinedly cover more than 30% of capital purchase.	Analyse transaction carried in purchase record during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			Access Control List (ACL)					
		PO prices are not competitive.	ERP system requires the PO approving authority to review vendor quotes at the time of approving the PO.	As per company policy	1. Check the Price fluctuations for same items during audit period. 2. Check that the PO is supported with a duly approved quotes. 3. Check that the PO is approved as per Authority Matrix.	1. Supporting documents 2. Price fluctuations	1. PO Records 2. All cases of deviation in rates within audit period.	Analyse ERP data for review of vendor quote by appropriate authority before approval of PO.
			The purchase policy of the company requires obtaining certain minimum number of quotations before placing the order. In case, the specified number of quotes are not available, then escalation	As per company policy	1. Check that specific number of quotes required as per purchase policy are obtained. 2. Check that in case of exceptions, escalation procedure as per the policy is followed.	Sufficient quotes obtained or not	Cover at least 30-50 PO or more depending on quantum of business.	Analyse ERP data for number of quotations and compare it with purchase policy to identify exceptions. Verify exception approval for insufficient no. of quotes.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			procedure specified in the purchase policy needs to be followed.					
		Change order are not authorised	If the terms of an approved PO are altered for price and scope, it automatically sends PO in pre-approval stage. Original POs terms are reviewed regarding provision for change due to change in price and scope.	As per company policy	1. Check by raising a dummy PO, getting it approved and then altering it. 2. Check by review of the audit trail report in ERP, if any PO has been modified after approval. 2. Changes could be possible only if original PO permits for changes.	Price and scope alteration original order	Audit trail report and select 20 sample for change order	Analyse change order record during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
			1. The purchase policy of the company requires that in case of change in order, it needs to be re-approved / re-	As per company policy	1. Check whether the PO wherein price has been altered has been re-approved as per the Authority Matrix 2. Check amendmen	Price and scope alteration original order	15 PO or 60% of change order whichever is lower.	Analyse ERP original POs with change orders due to price revision and check significant impact on budget.

336

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			processed as if it is a new PO. 2. Amendment number must be provided in change order for trail log of old PO.		t no. shown in PO after price change.			
			1. Change in orders are approved by next higher authority (DOA) or by the highest authority, if changes are more than defined limits. 2. Reason for change order with proper justification must be documented which also show impact on budget and should also be approved.	As per company policy	1. Check whether authority matrix is defined for change in order. 2. Whether reasons for changes are documented and approved along with impact on budget.	1. Approval matrix for change order. 2. Justification remark with approval.	15 PO or 60% of change order whichever is lower.	
		Unauthorized POs/ Contracts	All POs are approved as per	As per company policy	1. Check that the PO is	Unauthorised approval	1. ACL 2. Authority Matrix	Analyse transaction carried in

Final	Sub-process	Risk Description n	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).		approved as per Authority Matrix. 2. Check ACL and confirm that the same is updated as per Authority Matrix.	rights	3. 30 POs	purchase record during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
			All supporting documents (Indents/ vendor quote analysis sheet/ vendor quotes, etc.) are reviewed at the time of PO approval by authorised personnel (as per the approved Authority Matrix).	As per company policy	1. Check the PO review and approval process. Check that the PO is supported with a duly approved indent.	Supporting documents (including indents)	30 POs	NA
		Unfavorabl e terms and conditions of the	1. General terms and conditions, approved by legal	As per company policy	1. Check whether the general and standard	General and Standard PO terms and	30 PO / Contracts	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		purchase order.	team and part of Agreement / Purchase order/ Work order are pre-printed on reverse of PO.		terms and conditions are approved by Legal and part of agreement/ purchase order/work order.	conditions approval.		
			2. Standard terms and condition, approved by legal team and part of Agreement / Purchase order/ Work order.					
			In case of unusual or non-regular contracts, the personnel authorised as per Authority Matrix to approve the contract are required to obtain the approval of personnel authorised to do so in Legal department.	As per company policy	1. Check whether if the terms and Conditions of unusual or non-regular contracts are approved by authorised personnel in legal department.	Approval of terms for customised contracts	30 PO / Contracts (Unusual and non-regular)	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		Contracts are not stored / kept in a central / safe repository to safeguard company's interests and to prevent the use of the contract which might be detrimental to company's interests.	1. All PO / contract copies (active/ expired) are maintained with department. 2. Contracts on stamp paper are being stored centrally with designated authorities.	As per company policy	1. Check the existence of contracts with designated authority only and no other person have access for same. 2. Stamp paper stored centrally with designated authority only.	Existence and storage of contracts	1. Check process of maintaining documents by buyer/legal department. 2. Check 15 PO on sample basis.	NA
		Contractor, order details are not accurately input in the system	At the time of PO approval, PO is printed, and the details of the order, contractor and terms of the order are checked for accuracy by the personnel authorised to approve the PO as per the Authority Matrix.	As per company policy	1. Compare the approved PO with the supporting documents to ensure accuracy of data input.	Accuracy of data updation	30 POs	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		PO issued after the capital item have been received or may have been procured without raising a PO.	Receipts for the capital items cannot be affected in the ERP system unless the POs are existing therefore in the system. i.e., GRN cannot be prepared in absence of PO Reference in the ERP system.	As per company policy	1. Checked by raising a dummy receipt where PO does not exist. 2. Compare the GRNs with the PO to ensure that PO exists for all the goods receipt and the POs are dated prior to GRN.	Existence of PO for goods received	GRN and PO records	Analyse GRN record or Gate entry record having transactions of capital purchase to identify: - GRN or gate entry without PO reference. - PO created after gate entry or invoice date. Calculate value of such purchases during audit period to show impact.
			Vendor invoices cannot be processed in absence of a PO in system.	As per company policy	1. Compare the invoices recorded in vendors' accounts with the PO listing to ensure that PO is available for invoices booked.	Existence of PO for invoices booked	Vendor-wise Invoice listing	Verify ERP data of asset GL with asset clearing account to check assets rooted through 3 - way control system, i.e., PO, GRN and invoice instead of

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
								direct booking.
		In case of projects - Orders not clubbed to save logistics cost.	1. Project Purchases Report is generated monthly and is reviewed by designated authority to ensure that same location. 2. procurement requirements are evaluated for scheduling deliveries to reduce logistics/ freight and related costs.	As per company policy	1. Check the receipt of material of projects vis-à-vis locations - date wise and quantity-wise. 2. Check the monthly purchases report for evidence of review from designated authority.	Planning for possible saving in logistic cost	GRN records and PO records	Analyse purchase on same or closed date from same location/city and from same or different suppliers to calculate total logistic saving possible during audit period if transported through same vehicle.
		In case of projects purchases-business, share allocation amongst different vendors results in higher procurement prices.	All POs are reviewed and approved as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 Pos	Analyse PO record with GRN records to identify vendor wise: - Cases of quality rejection - Case of late delivery against PO terms - Cases of less

342

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
								quantity delivery against PO quantity to ascertain: 1. Vendor with low performance evaluation have high share of business 2. Action taken against regular default vendors.
			1. Purchases MIS is reviewed monthly by cross functional team of Heads of Purchases, Finance and Production and reasons / costs for or due to allocation of procurement among different vendors are analysed.	As per company policy	1. Check the monthly purchases MIS review for evidence of HODs review. 2. See the minutes of discussion and check whether the action points have been actioned upon. 3.Check approval of allocation of business among	Monthly MIS review	MIS for 3 months	Analyse ERP procurement as per approved allocation of business among vendors or not. Analyse latest quality, delivery reports to recommend change share of business among vendor. Calculate losses due to high

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			2. Exceptions , if any, are taken into account at the time of placement of subsequent orders.		different vendors and check that same allocation provided is entered in system for procurement purpose.			allocation of business to high rate vendor even provide low quality or late delivery.
		Inadequate segregation of duties – Vendor identified by the user and capital items/services ordered directly by the user from the vendor (including determination of purchase price and other terms and conditions).	Adequate segregation of duties (SOD) exists for all purchases that are routed through the buying department which is different from the user department. The same is ensured in ERP system through updation of Access Control List (ACL)	As per company policy	1. Check that the user department does not have access to raise PO by creating a dummy PO with id of a purchase department. 2. Check the ACL for existence of SOD.	Review SOD conflicts	ACL	Analyse ERP data to verify ID of user (Indent) department and purchase department must be different.
		In case of large projects having life of 2 to 5 year- Continued procurement at higher price as	Negotiations are conducted with approved vendors on an annual and routine basis so as to reduce cost of	As per company policy	1. Compare the approved PO with the subsequent reductions in the prices.	Price fluctuations and periodic review	PO records	NA

344

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		reduction in market prices and not renegotiated with suppliers.	purchase. Also, the Quotes are compared for negotiations during the appraisal time of the vendors. This is done by the personnel approved as the Authority Matrix.		2. Check the market rates for the bulk items / critical items and their movements during the period of audit.			
			MIS is reviewed by cross functional team of HODs for critical items and costs. Actionable, if any, are flagged off for implementation.	As per company policy	1. Check the MIS for evidence of HOD's review. 2. See the minutes of discussion and check whether the action points have been actioned upon.	Monthly MIS and review Minutes and timely action	MIS for 3 months	NA
		Duplicate Orders	MIS is reviewed by cross functional team of HODs for critical items and costs. Actionable, if any, are flagged off for	As per company policy	1. Check the MIS review for evidence of HOD's review. 2. See the minutes of discussion and check whether the action points have	Monthly MIS review Status of previous issue flagged.	MIS for 3 months	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			implement ation.		been actioned upon.			
			Exception report is generated at the time of processing of invoices for POs / Invoices with certain same attributes such, as, supplier, quantity, PR reference and is reviewed by designated authority.	As per company policy	1. Check the linking of the attributes and the exception report generated for any duplicate orders. 2. Sort the Invoice batch / PO Records on the attributes and check for the common information.	Quantities, PO numbers, PR reference, supplier name	Invoice / PO Records and link with PR Records	Analyse gate entry, GRN, PO Records, PR Records for any common informatio n which show duplicate PO raised for same items.
			All POs are reviewed for accuracy and correctnes s and approved as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the PO is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthoris ed approval rights	1. ACL 2. Authority Matrix 3. 30 POs	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		All POs are not recorded.	PO are sequentially pre-numbered. The sequence of PO processed is accounted for.	As per company policy	1. Check by review of records of PO, if there are any missing serial numbers of the POs.	Serial no. control of purchase order.	Records of PO	Analyse ERP PO records to verify PO sequence number.
			In case of emergency purchases, the purchases made without indent / PO need to be specifically approved as per the Authority Matrix.	As per company policy	1. Check that there exists specific approval for purchases without indent or PO as per the Authority Matrix.	Approval	Records of Invoice Gate entry records	Analyse GRN record or Gate entry record having transactions of capital purchase to identify: - GRN or gate entry without PO reference. - PO created after gate entry or invoice date. Calculate value of such purchases during audit period to show impact.
		Validity of the open POs / Contracts	1. The list of open POs / contracts is reviewed	As per company policy	1. Check the validity of open PO / Contracts.	Open PO dates	Open PO listing	Analyse list of Purchase Orders for following:

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			monthly by purchase team. The redundant / expired PO are purged from the list. 2. Timelines of the procurement activities are monitored monthly Reason analysis is performed and documented for all delayed beyond the defined timelines.		2. Check the documented reason for delayed Pos.			- Instances of open purchase orders not closed for long times. - may be used for parking unauthorised transactions. Calculate financial loss to the company due to delay in delivery, if possible.
		Audit logs for changes in PO may not be available and review lead to unauthorized changes.	1. Audit logs are generated for all Purchase Orders (POs) / Work Orders (WOs) raised / modified in the system. 2. Process is in place to monitor audit logs to identify any inappropria	As per company policy	1. Check logs are available for PO's/ WOs and modification. 2. Mechanism in place to review audit logs.	Audit Logs of changes in PO.	1. Audit logs 2. monthly review on logs- 3 Month.	Analyse Audit log of modification carried in purchase record during the review period to identify the following: 1. Unauthorised users performing transaction. 2. Conflicting transaction

348

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			te / suspicious activity.					rights granted to same person.
	Receiving project material and quality assessment	Project delayed due to delays by contractor to complete various activities.	1. Open PO/contract list is prepared on a weekly basis by designated department. This is used as basis for tracking timely deliveries by the user department. 2. Action needed by project committee are recorded for future action. 3. Drawings are timely provided by architect well in advance before 15 days of start of work.	As per company policy	1. Check the instances of stock outs and review the justification / root cause for the same. 2. Check whether the department track deliveries against the Open PO list. 3. Check action taken by monthly project committee and action recorded and taken by contractor for timely completion. 4. Check timely drawings provided by the architect or not.	1. Open PO dates 2. stock outs	1. 10 weeks open PO list 2. Stock out event list	Analyse ERP Open PO records with daily stock details to identify instances where PO undelivered and material is out of stock.
		Assets received	Statements received	As per company	1. Check that the	Unrecorded assets	Top 20 vendor	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		may not be recorded.	from vendors are reconciled to the vendor accounts in the accounts payable sub - ledger quarterly and differences are investigated. This is reviewed by Accounts teams.	policy	vendor accounts reconciliation is done on a periodic basis. 2. Check the differences, if any, are reconciled and are not carried forward.		capital Vendor's Reconciliation statements or cover 40% capital purchase	
			The stock at the business locations of the company is physically verified at least once in a year by Accounts department / independent auditors. Variances, if any, are reconciled with the books of accounts to ensure accuracy of the books	As per company policy	1. Check the working papers of physical verification and see that the differences, if any, were reconciled and accounted for.	Periodicity and Variances noted in physical verification.	Physical verification statements and reconciliation.	

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			of accounts.					
		Capital Asset accepted without proper inspection and verification	1. The receiving personnel are required to match the assets received with the open purchase orders. In case, the assets received do not match with the quantities or specifications or exceed the purchase order quantity, the same are rejected. 2. Invoice quantity and physical quantity are matched for which store person count inventory before GRN and sign off on	As per company policy	1. Check whether GRN can be raised for items without a PO or that do not meet the PO specifications. 2. Whether store person sign off on invoice after physical count of items. 3. Verify check exist for physical count with invoice quantity by person other than GRN entry person to avoid SOD conflicts.	Capital items against Authorised PO only	PO Records and GRN Records 30 GRNs for physical verification	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			invoice.					
			All receipts are reviewed and approved by the personnel as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse records of GRN with records of PO quantity and rates to identify Instances deviation.
		Quantity received in excess of ordered quantity. Quantity received has not been ordered.	1. The receiving personnel are required to match the goods received with the open purchase orders. In case, the goods received do not match with the quantities or specifications or exceed the purchase order quantity,	As per company policy	1. Check possibility of GRN more than PO quantity by system walkthrough. 2. Check approved tolerance limit against PO qty from management side. Verify cases where material allowed more than tolerated limit.	Order Vs Receipt qty Material not received as per specifications.	PO Records VS GRN Records and amended PO for change in order quantity.	Analyse list of GRNs for following: 1 Instance of delays in receipt of materials. 2. Instances of GRN / SES without PO or before PO. 3. Instances of GRN without gate entry. 4. Instances of GRN before gate entry. 5.

352

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			the same are rejected. 2. ERP also has control over quantity booking, system does not allowed booking of quantity more than PO quantity.					Instances of GRN more than PO quantity. 6. Instances of GRN / SES value more than PO / SO value. 7. CWIP open for long time.
			All receipts are reviewed and approved by the personnel as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).	As per company policy	1. Check that the GRN is approved as per Authority Matrix. 2. Check the ACL and confirm that the same is updated as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse ERP receipt record during the review period to identify the following: 1. Unauthorised users performing transaction. 2. Conflicting transaction rights granted to same person.
		Unauthorized person can create receiving documents	All receipts are reviewed and approved by the personnel	As per company policy	1. Check that the GRN is approved as per Authority Matrix.	Unauthorised approval rights	1. ACL 2. Authority Matrix 3. 30 GRNs	Analyse ERP receipt record during the review period to

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			as per the approved Authority Matrix. Also, the same has been entered into ERP software in Access Control List (ACL).		2. Check the ACL and confirm that the same is updated as per Authority Matrix.			identify the following: 1. Unauthorised users performing transaction. 2. Conflicting transaction rights granted to same person.
		Terms and conditions of acceptance of goods at the factory gate (before the goods have been approved by quality/ control department) may be detrimental to the interests of company.	The receiving stamp that is used to acknowledge receipt of goods at the gate on Goods Receipt Note (GRN), bears the inscription *'goods are being received subject to count and quality procedures'*. Accordingly, liability would not accrue to the Company until these procedures are complied	As per company policy	1. Check that the GRNs are being marked with the stamp 'goods are being received subject to count and quality procedures'.	Appropriate stamp on the GRNs.	30 GRNs	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			with.					
		Inappropriate quality of material accepted	1. Before the GRN is sent to Accounts department for booking the liability or the goods are sent to store. Quality department is required to certify the quality of material received in accordance with the set guidelines. 2. The store clerk will not accept the goods unless the "QC checked" is stamped on GRN. 3. Also, Accounts department will not book the liability and process the payment unless the QC checked	As per company policy	1. Check whether the GRNs have been marked as approved by Quality control department. 2. Review exception report for the goods rejected due to quality constraints on the shop floor. Check all these goods are returned to vendors as per agreement. 3. If rejected goods are not returned, it should be recorded. 4. Monthly quality exception list is reviewed by authorised person.	Post QC - rejections	1. 30 GRNs 2. Exception report raised for post QC - rejections	Analyse Quality and Return to Vendor for following: - Delays in sending back rejected material to vendor. - Instances of GRN and issue of material despite quality rejection. - Quality are created by unauthorized person/ Absence of SOD.

Final	Sub-process	Risk Description n	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			stamped GRN is received by them. 4. In that case, quality check is not required for any item, the same should be a part of QC exceptions list which is reviewed monthly .					
			Access to certify the quality of material is restricted as per approved Authority Matrix in ERP.	As per company policy	1. Review Access Control List for access to personnel other than those authorised for certifying quality of the goods.	Access rights for certifying quality	Access Control List	Analyse GRN and Quality record during the review period to identify the following: 1. Unauthorised users performing transactions. 2. Conflicting transaction rights granted to same person.
		Policy may not be in place for sampling,	1. Policy in place for quality testing of	As per company policy	1. Check policy of sampling and	Sampling and quality methodology	Select 30 GRN to check quality	Analyse ERP Quality Records

356

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		methodology leads to improper quality.	required material including sampling, methodology and documentation of quality testing. 2. Quality inspection standards are defined for all materials. 3. Ensure that all steps are carried out as per company policy or ISO certification process for quality assessment and documentation.		methodology of quality testing is documented. 2. Check quality inspection for all material. 3. Inspection is carried out as per policy or ISO certification process.		sample taken and methodology used.	and check quantity transferred to unrestricted category or not (for issue purpose). Check quantity in restricted category and reason for same. Analyse ERP quality record of actual sample by defined sampling method.
		Project Material - Rejected material may not be placed separately and returned to vendor on timely basis leads to risk issue to	1. Any rejected work should be made good by contractor. 2. Any rejections are segregated and stored separately. 3. All	As per company policy	1. Physically verify rejected items and storage control to avoid issue for operation. 2. Check rejected item returned	Storing of rejected and return to vendor	4 Month MIS of rejected items. 20 Debit notes for rejected material.	Analyse ERP quality, GRN records and Vendor ledger to establish following: - Debit note raised to vendor or not for

357

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		floor and ownership.	rejections are supplied back to vendor on timely basis. 4. Department ensure timely return and recording of return. 5. Material is consumed only after Quality checks. 6. Perform assessment in case of high rejection in the material supplied by the vendor. 7. Debit notes should be raised immediately for all rejections and return to vendors.		and replaced by vendors on timely basis or not. 3. Verify return recorded on timely basis in books or not. 4. Ensure material consumed after quality check only. 5. Monthly assessment of vendor - wise rejection to take appropriate action against regular default vendors. 6. Debit note raised for rejected material and approved by appropriate authority. 7. Verify rejected material with advance paid vendors.			quality rejection. - GRN reversal in case of rejected material. - GRN records for replacement by vendor against same PO. - Material are issued after quality approval only.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		Delay in clearing and forwarding of imported assets.	The report on demurrage charges incurred due to delay in carrying and forwarding of imported capital items and is reviewed by Designated person monthly . Also, these charges are separately disclosed in the MIS for Sr. Management review.	As per company policy	1. Check the Demurrage charges paid and justification for the same. 2. Check approval of demurrage charges along with reason.	Demurrage charges due to delay in clearing.	Records of demurrage charges ledger balance. 30 imported invoices	NA
		Unauthorised or Inaccurate release of payments for transporter dues	1. All transporter claims are authorised by the designated authority prior to payment by the Accounts department . This is based on the agreements with the contractor / transporters.	As per company policy	1. Check the supporting for the claims viz. agreements, if any / rate contract. 2. Check reconciliation of purchase register with transporter invoice to avoid duplicate	Transporter charges authorization	30 transporter invoices or as per quantum of business of company.	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			2. Person different from purchase team is prepared a tracker of transporter invoice and reconcile it with purchase register.		booking. 3. Check lorry documents for freight payment.			
		GST Input Credit not availed / Short / Excess availed	Monthly reconciliation of GST Input Credit account and GST Input Credit register is done jointly by Stores and Accounts.	As per company policy	1. Check the GST Input Credit reconciliation for long outstanding items and check justifications and action for the same.	Periodicity of reconciliation and reasons for outstanding items.	3 months reconciliation	Analysis GSTR-2A report with purchase register to identify cases where GST credit available as per portal but invoice not booked or vice versa.
	Invoice Processing	Invoices may be booked incorrectly.	1. Before any invoice is approved for booking, Designated Authority performs a three-way match of the PO, GRN and Invoice 2. Capital Goods are recorded	As per company policy	1. Check that the invoice is supported by duly authorised PO and GRN. 2. Check compliance of accounting standard while booking of invoices.	3 way control PO, GRN and Invoice	50 invoices or as per quantum of transaction	Analyse and compare PO Records with GRN records to verify accuracy in booking value. Verify transporter charges GL or clearing & forwarding

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			as Fixed Assets as per AS10					or suspense GL where excess invoiced value (More than PO value) may be provided to verify approval process.
			1. Bank guarantee (Advance Bank Guarantee and Performance Bank Guarantee) are received for period upto defect liability. Retention is deducted as per agreement terms. 2. Labour cess deduction is made from bills. Electricity or water charges deducted from RA bills if provided by company.	As per company policy	1. Check whether PBG and ABG received and have sufficient time period for claim in case of default. 2. Check retention deducted and paid only completion of defect liability period. 3. Labour cess, electricity and water cess deducted from RA bills. 4. Retention and PBG will be released only after	Compliance with agreement terms	50 invoices or as per quantum of transaction	Analyse vendor wise/ PO wise PBG tracker to verify all PBG are active and renewed on timely basis before expiry in cases of work have not been completed. Analyse retention payment GL and contractor defect liability period from date of completion of work.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
					satisfactory performance approval certificate received from project team.			
			In case of emergency purchases, invoice is verified with the GRN and subsequent approval obtained for purchase from personnel authorised in terms of Authority Matrix.	As per company policy	1. Check that the invoice is supported by GRN and post-purchase approval from the personnel authorised as per Authority Matrix.	Emergency purchase approval	50 invoices or as per quantum of transaction	Compare Invoice dates and PO date to identify emergency purchase (Invoice date should be after PO date). Verify ERP records where invoices are booked without 3 way control, i.e., PO, GRN and invoice to check approval procedure.
		Same invoice may be booked more than once.	At the time of booking of invoice, invoice is defaced with the Stamp "Processed" by executive.	As per company policy	Check that the invoices are defaced at the time of booking.	Defacing of invoice to avoid duplicate booking	50 invoices or as per quantum of transaction	Analyse Vendor Invoices for following: 1. Incorrect / duplicate Invoices processed. 2. Check for same invoice

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
								amount during the same period for same vendor.
			1. Once an invoice is booked, the supporting documents viz. GRN, PO, Indent are attached with it. 2. Other document, i.e. measurement sheet, Quality sheet, engineer approval, site photograph of progress is verified by designated authority. 3. Bill of material is attached which show details of previous bill, current bill and total billing details. Invoices	As per company policy	1. Check that the invoice is supported by duly authorized PO and GRN. 2. Check other documents, i.e., measurement sheet, Quality sheet, engineer approval, site photograph of progress. 3. Bill of Material attached as supporting and invoice verified with it for accuracy.	Supporting documents related to capital items	50 invoices or as per quantum of transaction	Analyse POs value from ERP records and compare it with GRN value for accuracy in between.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			without these, cannot be processed.					
		Unapproved invoices are processed	The invoices before being processed are reviewed by designated authority.	As per company policy	Check the approval of designated authority on the invoice.	Invoice approval from designated authority.	50 invoices or as per quantum of transaction	Analyse GRN and invoice record during the review period to identify the following: 1. Unauthorised users performing transaction.
			Access rights to process the invoices are restricted to the personnel authorised as per the Authority Matrix and are entered in Access Control List (ACL) in ERP system	As per company policy	Check the Access Control List for the access rights given to the authorised personnel	Access rights	ACL	2. Conflicting transaction rights granted to same person.
		Delay in accounting of capital invoices	Statements received from the contractor are reconciled to the contractor accounts in the accounts payable subledger	As per company policy	1. Check the periodicity of contractor reconciliation for appropriateness thereof. 2. Sample check the pending	Timely booking of invoices	Reconciliation for 20 contractors	Analyse ERP data to compare invoice date, GRN date, Quality date, invoice booking date to verify timely

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			quarterly and differences are investigated. This is reviewed by Designated Authority.		items in the reconciliations for invoices pending for booking and confirm the reasons for same.			processing of invoice.
			1. For goods- The list of Goods Received Not Invoiced (GRNI) and the items with Quality Control are reviewed monthly to ensure that there are no delays in booking the liability. 2. For work- Monthly recompilation are prepared between work performed and actual billing by contractor.	As per company policy	1. Check aging of the Temporary GRN raised for the material with Quality Control department and the GRNIs. 2. Ensure that the same are accounted in the books as liability in the suspense accounts. 3. Monthly recompilation between work performed and actual billing approved by civil team or mechanical	Aging of GRN and material being held by QC	Records of GRN with QC Liability provides for non-booked GRNs or invoice or performed work.	Analyse ERP data to compare invoice date, GRN date, Quality date, invoice booking date: - to verify timely processing of activities - to check vendor liability booked on timely basis So that reconciliation gaps should be zero or minimum.

365

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
					team.			
		Booking of related expenditure and GST input credit along with invoice may not be booked.	1. GST Input credit are obtained for all eligible credits, and it is duly verified at the time of recording of invoices. 2. All the related expenditure, such as toll tax, cess, freight, etc., are recorded as capital cost of item/project. 3. Appropriate deduction and recording of TDS are done wherever applicable.	As per company policy	1. Check cenvatable credit provided along with invoice booking. 2. All related expenditure like toll tax and freight booked in cost of capital item/project. 3. TDS and other deduction as per law are done and recorded.	Credit booking and deduction	50 invoice and as decided with management	NA
		Delay in raising debit/ credit notes.	Statements received from vendors are reconciled to the vendor	As per company policy	1. Check the vendor reconciliation for the periodicity of reconciliation.	Timely issue of Debit / Credit Notes	Reconciliation for 30 vendors	Analyse time taken for issuing debit / credit notes from the date of booking of

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			accounts in the accounts payable subledger quarterly and differences are investigated. This is reviewed by Designated Authority.		2. Sample check the pending items in the reconciliations for debit / credit notes yet to be raised. Confirm reasons for the same.			invoices or date of receipt/ return of material.
		Unauthorized debit/ credit notes may be raised.	The debit / credit notes are approved by the person as per Authority Matrix. The same enteredin the Access Control List existing in the ERP system	As per company policy	1. Check that the access control list defined in ERP system is as per the approved Authority Matrix. 2. Check that adequate back up / supporting documents exist for issuing debit / credit notes.	1. Approvals for debit/credit noted 2. Reasons for issuance	30 debit / credit notes	Analyse number of debit / credit notes issued vis-à-vis number of purchases made. Analyse value of debit / credit notes issued vis-à-vis value of purchases made. To check efficiency of purchase.
	Accounting and payables	Unauthorised payments	1. The payment voucher with required supporting's is	As per company policy	1. Check that the Access Control list in ERP is as per the approved	1. Access Control List 2. Supporting	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	Analyse vendor payment record during the review period to

367

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			reviewed and authorised by the personnel authorised as per approved Authority Matrix. The Authority Matrix is enteredin the Access Control List (ACL) in ERP system. 2. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved. In case of cheque payment, when cheque is handed over to vendor representative and acknowledgement is obtained.		Authority Matrix. 2. Check that requisite supporting is attached with the payment voucher. 3. Check that the supporting is defaced for the approved vouchers. 4. Sign of vendor's representative.			identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
			At the time of	As per company	1. Check that there	1. Advance amounts in	30 vendor accounts	Analyse Vendor

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			processing a vendor invoice for payment, Designated Authority are required to identify and set off all the advances pending adjustment for such contractor or capital vendor.	policy	are no amounts pending adjustment for vendors where all the invoices have been paid. See justification for exceptions. 2. Scrutinise the vendor accounts / party accounts to check the cases of segregation of amounts to avoid authority matrix. 3. Vendor advance should be adjusted as er contract terms. 4. Check cases of advance paid contractor but work performed with slow pace, leads to financial loss to the company.	vendor accounts pending for adjustments, 2. Multiple payments on same or nearby date	and per business need	payment for following: 1. Same vendor on same date- and more than one payment 2. Check advances are adjusted as per contract terms. 3. Check advance paid but without bank guarantee against the policy of the company.
			The listing of vendor	As per company	1. Check the	Review of payment	30 vendor payment	Analyse vendor

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			payments is reviewed prior to release of payment by the personnel authorised as per Authority Matrix.	policy	evidence of review on the vendor payment list.		lists	payment record during the review period to identify the following: 1. Unauthorised users performing transactions 2. Conflicting transaction rights granted to same person.
			The personnel making the payment (either through cheque / DD / wire transfer) are authorised to do so as per the approved Authority Matrix.	As per company policy	1. Check the approval for authority to make the payment. 2. Check whether the same has been communicated to the bank.	Approval of payment to vendors	Authority Matrix	
			Management periodically reviews the returned paid cheques for unauthorised signatures, alterations and / or alterations.	As per company policy	1. Check the evidence of the management review.	Review of returned cheque	Returned cheques during audit period	Analyse total cheque issue during the period and returned to verify following: 1. Control at the time of issue of cheques. 2. Period for which cheques returned due to alteration/

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
								mismatch, etc.
		Payments are made to incorrect vendors.	1. The payment voucher with required supporting is reviewed and authorised by the personas per approved Authority Matrix. The authority matrix is entered in the Access Control List (ACL) in ERP system. 2. The supporting documentation is cancelled or defaced once it is reviewed and payment voucher is approved.	As per company policy	1. Check that the ACL in ERP is as per the approved Authority Matrix. 2. Check that requisite supporting is attached with the payment voucher. 3. Check that the supporting is defaced for the approved vouchers.	1. Access Control List 2. Supporting of deface	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	NA
			1. The listing of vendor payments is reviewed prior to release of payment by the	As per company policy	1. Check that the evidence of review on the vendor payment list.	Management review before release of payment.	30 vendor payment lists	1. Data analysis of the Open/Long pending advances which are not adjusted.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			person as per approved Authority Matrix. 2. Cheques / DD are restrict endorsed by the preparer to ensure that they are paid to specific payee.					2. Analyse data for Instances of delay in payment made to MSME vendors over 45 days. 3. Whether liability write off approval are obtained from management as per policy.
			Management periodically reviews the returned paid cheques for unauthorised signatures, alterations and / or alterations	As per company policy	1. Check the evidence of the management review.	Management review for returned cheque and reissue.	Returned cheques	Analyse total cheque issued during the period and returned to verify following: 1. Control at the time of issue of cheque. 2. Period for which cheques are returned due to alteration/ mismatch, etc.
		Credit terms may not be utilized	1. Payment are processed for	As per company policy	1. Check payment and credit terms with	Credit terms and weekly review of	check ledger of 10 major vendor	Analyse ERP vendor ageing of

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
		effectively.	approved invoices as per agreed payment terms to optimize during credit period and efficient utilization of working capital. 2. Vendor ageing is prepared and reviewed by the Designated Authority on weekly basis to ensure all overdue payments are processed.		vendors. 2. Review document of vendor ageing on weekly basis.	overdue.	10 weekly review of overdue payment	different month to verify payment made after utilizing credit terms to maintain working capital balance.
		MSME Vendor not paid on timely basis.	Payment to MSME vendors is reviewed and made within defined timelines as per terms of agreement or timelines defined under Micro, Small and Medium	As per company policy	1. Check ageing of MSME vendors on different date/ months.	Timely payment to MSME vendors	Check Ledger of 20 MSME vendors	1. Data analysis of the Open/Long pending advances which are not adjusted. 2. Analyse data for Instances of delay in payment made to MSME vendors over 45

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			Enterprises Development Act, 2006 or amendments thereafter (45 days), whichever is earlier.					days.
		GST credit reconciliation and payable more than 180 days.	Reconciliation of eligible GST credits on GST portal with GST Input credit available and deposited are performed periodically.	As per company policy	1. Check monthly reconciliation sheet of GST credit as per books with Portal and deposited.	GST reconciliation	3 Month reconciliation	Analyse vendor wise credit available at portal and credit availed/ booked by the company and reason for non-utilization/ booking and vice versa.
			If payment to vendors is not made within 180 days, then GST credit related to particular amount needs to be reversed.	As per company policy	1. Verify vendors ageing and identified cases where payments are outstanding by more than 180 days. 2. Check GST return and verify credit related to this vendor reversed in particular	GST credit reversal in case of non-payment within 180 days	1. Vendor ageing 2. GST returns for reversal purpose	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
					month or not. 3. Tracker should be maintained by the company for credit reversal and subsequent utilization after payment.			
		Duplicate payments	1. The payment voucher with required supporting is reviewed and authorised by the person as per Authority Matrix. The Authority Matrix is entered in the Access Control List (ACL) in ERP system. 2. The supporting documentation is cancelled or defaced, once it is reviewed and	As per company policy	1. Check that the Access Control list in ERP is as per the approved Authority Matrix. 2. Check that requisite supporting is attached with the payment voucher. 3. Check that the supporting is defaced for the approved vouchers.	1. Access Control List 2. Supporting	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			payment voucher is approved.					
		Non receipt of material against advances	The listing of Open POs is reviewed monthly to check the cases of delayed supplies/ contractor wherein advances have been released to them. This is reviewed by the person as per Authority Matrix.	As per company policy	1. Check the due dates in the open PO / Contracts. 2. Check the reasons for delays in supplies.	1. Open PO with corresponding advances 2. justification for delays	1. Open capital PO listing 2. Unadjusted capital advances GL	Analyse Capital PO list (where timeline of supply has been expired) and compare with capital advance GL to identify cases where advance unadjusted and vendor POs are also outstanding. Analyse advance with Bank Guarantee (BG) tracker for BG extension if advance pending for adjustment.
			Ageing of the party balances is reviewed monthly and account reconciliation is done	As per company policy	1. Check the debit balances appearing in the supplier's account and ageing thereof.	1. Approvals, 2. Amount, 3. Receipt of material 4. Due date	Vendors Account and the Advances Aging statement.	Analyse various figures reported in MIS vis-a-vis the details appearing in ERP

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			on a quarterly basis		2. Check whether any unauthorized advance has been given to the supplier (this needs to be checked with the justification provided and the Authority Matrix). 3. Check whether the advances have not been adjusted correctly while accounting for receipt of goods.			system to identify instances of incorrect reporting.
		Penalty may not be imposed and Extension of Time (EOT) may not be allowed to contractor for delay in supply or completion of contract.	1. Penalty are imposed on contractor in case of delay in supply or construction as per project terms. 2. If delay from manageme	As per company policy	1. Check LD deducted from RA bills of contractor if EOT not allowed. 2. Check EOT allowed and justification provided for delay.	LD deduction and EOT with justification	20 Sample for delay in supply and completion of contract.	NA

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	₹	Data analytics performed
			nt side, EOT (Extension of time) will be allowed and RA bill processed without deduction.		3. Action taken by management to avoid EOT next time.			
		Wrong Foreign exchange rates used for conversion of foreign currency invoices.	Weekly foreign currency rates are updated in the ERP system by the person as per the Authority Matrix. The rights to update the masters are restricted as per Authority Matrix	As per company policy	1. Compare the rates applied for invoice processing with the RBI rate.	Exchange rate applied as per RBI rate	Forex rates in 10 weeks	

Fixed Assets and Capex

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
Fixed Asset and Capex	General and entity level control	Authority matrix may not be prepared or approved from Board of Director (BOD).	1. The organisation has clear and comprehensive (up to date) Delegation of Authority (DOA)/ Delegation of Power (DOP) and Authority Matrix. 2. Authority matrix is approved by Board of Directors, defining the authorities for approving capital purchase transactions or performing various transactions during the purchase process. 3. To incorporate situations where emergency procurement needed.	As per company policy	Check capital item procurement DOA/DOP is available and approved by BOD for following activities. 1. Requisition for purchase of machinery, if any. 2. Opening of tender/ quotations for purchase of machinery. 3. Purchase order for purchase of fixed assets. 4. Comparative chart of technical	Approved DOA/DOP for capital purchase	Approved DOA/DOP from BOD	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					and financial bidding. 5. Quality check and its approval. 6. Issue of Debit note for return/ rejection of machine or for rate difference. 7. Authorisation of date of erection and commissioning of plant and machinery. 8. Ensure the PPE items comply with safety, regulatory and standards. 9. Asset requisition report indicating the payback period.			
		Inadequat	1. Document	As per	1. Check	1.	1. SOD	Analyse

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
		e Segregation of Duties and access rights which may result in fraudulent / unauthorised fixed asset transactions	defining appropriate Segregation of Duties (SODs) is in place. 3. Periodic Review of Segregation of Duties and Access rights is conducted.	company policy	documented SOD and Access right list 2. Verify same SOD and Access right also entered in system for approval of transactions. 3. Verify evidence of periodic review of SOD and Access rights in ERP system. 4. Check only authorized person have access to perform to fixed assets. 5. Verify the fixed assets transactions on a sample basis and trace them through	Documented SOD, Access right 2. Periodic review	2. Access right List 3. Half yearly review document	fixed asset transaction carried out during the review period to identify the following: 1. Unauthorised users performing transactions 2. Transaction rights granted to same person.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					the process to identify any instances where one person is responsible for multiple steps (intiating, approving and recording) 6. Check physical count of assets on a sample basis and reconcile the counts with Fixed assets register. See for discrepancies that might indicate unauthorized disposals or acquisitions. 7. Examine any documents related to			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					transfer of fixed assets between departments or location. Verify that transfers are properly authorized. 8. Review the system audit trial to identify any unusual or unauthorized activity relating to fixed assets, that may indicate fraudulent transactions. 9. Check the system access log to identify any unusual or unauthorized access.			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
		SOP may not be defined to ensure consistency and standardisation of operations.	1. The organization has clearly defined Standard Operating Procedures for fixed asset and capex in place. 2. Organization has defined Activities, Roles and Responsibilities, Key Performance Indicators (KPIs), Timelines and Frequency of activities along with various documents of capital transactions to be maintained .	As per company policy	1. Check SOP available and complete in all aspect of roles, KPI, Timelines and frequency of activities, etc. 2. Check when fixed asset SOP updated last.	Approved SOP and completeness	Updated SOP	NA
	Statutory compliance	Non-compliance of statutory requirements under different Acts.	All statutory requirements under various Acts complied.	As per company policy	Ensure proof for compliances of following: 1. Whether Schedule II of Companies Act, 2013, which relates to useful life of assets to compute depreciation has	Compliance under various act	Compliance checklist and review document .	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					been adhered to. 2. As per Schedule III of Companies Act, 2013, fixed assets are broadly divided into four categories, i.e. tangible assets, intangible assets, capital work in progress, and intangible assets under progress. 3. Whether the unit has complied with the provisions of the Factories Act, 1948 with regard to hazardous machine, machine in motion and			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					transmission machines, etc. 4. Whether hoists and lifts are properly maintained as per Factories Act 1948 and is thoroughly examined by a competent person at least once in every period of six months and a register is kept for this purpose. 5. Payment of Customs duty and custom clearance of imported machinery as per Customs Act, 1962 6. Deductio			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					n and payment of TDS for installation, fabrications and commissioning of plant and machinery, if applicable. 7. Whether the unit has obtained an appropriate certificate from Central Pollution Control Board (CPCB), if applicable. 8. Depreciation is not claimable on the amount equal to ITC/ Cenvat Credit if claimed against purchase of any			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					machinery. 9. Ensure the track on fixed assets for claiming input tax credit under GST ensuring proper documentation and reconciliation on input tax credit claims. 10. Whether a company is into real estate, check whether they complied as per the Transfer of property act. 11. Check whether the company has compiled with labour laws complied			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					with health and safety regulation.			
	Fixed Assets controls	Recognition of fixed asset may not be as per Ind AS 16 Property, Plant and Equipment	Fixed assets are recognized only if they have future economic benefit to the company.	As per company policy	1. Verify that cost of an item of property, plant and equipment shall be recognised as an asset if, and only if: (a) it is probable that future economic benefits associated with the item will flow to the entity; and (b) the cost of the item can be measured reliably. 2. Items such as spare parts, stand-by equipment and servicing	Recognition of asset as per Ind AS 16 requirements	1. 30 purchase invoice or 30% of high value asset purchase invoice during the year whichever is higher. 2. 20 installation certificate	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					equipment are recognised in accordance with this Ind AS when they meet the definition of property, plant and equipment. Otherwise, such items are classified as inventory 3. Check certificate / Undertaking of put to use			
		Fixed Asset balances may not be matched with general ledger balances	1. All fixed asset are recorder in books as and when received and updated in Fixed Assets Register (FAR) accordingly. 2. On monthly basis designated person review General Ledger (GL)	As per company policy	1. Whether the reported fixed assets balance agrees with the related account records in the general ledger. 2. Check periodic review of	Reconciliation between FAR and GL's	GL balances and FAR balances at cut of date.	Analyse items description in fixed asset register to ascertain various assets are correctly grouped in different heads as per nature.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
			balances with Fixed asset register prepare reconciliation for difference. 3. All transaction are supported by vendor invoices.		Fixed Assets Register (FAR) and ensure its timely updation. 3. Whether recorded fixed assets transactions tallies with the supporting documents, such as, vendor's invoice. 4. Check reconciliation between FAR and GL must be reviewed by designated person, and it should not have long pendency. 5. Whether complied with Ind AS 16 requirement or			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					not. 6. Check fixed assets balances with external parties. 7. Check fixed assets transactions are recorded in correct accounting period.			
		Fixed assets may be physically verified at regular intervals to identify unrecorded transactions, write off obsolete assets and gaps with FAR.	1. Company have policy of physical verification of fixed asset at regular intervals. 2. All fixed assets are marked with unique identification code. 3. Verification of asset are done along with identification of obsolete machinery.	As per company policy	1. Whether identification number is put on all the assets and cross verified with FAR. 2. Whether recorded fixed assets have been physically examined at regular interval and compare it with fixed assets register and	Physical verification controls	1. Latest physical verification report 2. Fixed asset register	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					discrepancies, if any, should be reported. 3. Check obsolete/ non-performing fixed assets are periodically identified and documented. An action plan for its disposal/ alternate use should be initiated.			
		Other expenditure related to fixed asset may not be capitalised along with assets	1. Expenditure incurred upto make an asset operational are capitalised along with asset i.e. Installation cost, commissioning cost. 2. Borrowing cost incurred upto date of capitalization also become part of fixed	As per company policy	1. Check recorded fixed assets are correctly classified as capital assets and certain expenses that are attributable for b that asset to its working condition	Capitalization of other related expenditure	Vendor invoice of 30 assets capitalised during the year along with cost sheets	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
			assets.		and use, are to be included in the cost. 2. Further the borrowed cost, if any, is also to be capitalized up to the first date of acquisition/ construction as per Ind AS 23. 3. Also considered foreign exchange fluctuation provision as per Ind AS 21. Ind AS 21 does not permit capitalisation of forex differences. 4. Check subsequent expenditure relating to an item of fixed assets			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					should be added to its book value only if they increase the future benefits. 5. A cost sheet should be prepared with a complete breakup of various cost incurred to make asset operational.			
		Disclosure of fixed asset may not provide complete details of gross, net and addition, deletion during accounting period.	1. Assets are disclosed with completed details of gross, addition, deletion and net value during accounting period. 2. Asset for disposal is shown at net realizable value or net book value whichever is lower.	As per company policy	1. Check material items retiring from use and held for disposal are to be stated at lower of net book value and net realizable value. Ensure that the cost of spare parts of obsolete machiner	Disclosure of all assets during accounting period.	Fixed Assets Register (FAR) with complete detail & general ledger of various asset.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					y is taken at nil value. 2. Check fixed assets are disclosed – gross and net value at the beginning and end of the accounting period showing addition, disposal, acquisition, etc.			
		Assets may not be insured to avoid losses in case of mis-happening	All assets are reinstated and reinstated values approved from appropriate authority for insurance purposes.	As per company policy	1. Check whether all the fixed assets are properly insured, and proper safety measures have been taken. 2. Assets should be insured by reinstated value instead of gross. Reinstate	Insurance of fixed assets	1. Insurance policy 2. Reinstatement values 3. Gross value of fixed assets	NA

396

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					ment should be approved by appropriate authority before insurance quotation. 3. Quotation should be obtained from different vendors and verify all clauses under different quotation and accordingly obtain insurance policy from vendor whose quotes match with business requirement. 4. Any significant asset purchased during the year should also be covered under			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					insurance policy by giving additional premium. 5. Proper records have been maintained for sending machinery for outwards repairs fabrication. Third party location should be insured also under insurance policy.			
		1.Disposal of fixed assets is not in accordance with Company Policy. 2. Assets identified for disposal may not be adequately safeguarded against theft or unauthoris	Company derecognised asset on 1. Disposal 2. When no future economic benefits are expected from its use or disposal	As per company policy	1. Check carrying amount of an item of property, plant and equipment shall be derecognised at the time of disposal. 2. Complied with other provision of derecognition as per Ind	Asset may not be derecognised	1. 20 sale invoices of asset and corresponding entry in Fixed Asset GL. 2. Sale Register	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
		ed use.			AS 16. 3. Check sale register to verify sale of asset and recognised as revenue.			
	Depreciation control	Useful life of assets may not be defined as per Company Act 2013 requirement and leads to inappropriate depreciation.	1. Useful life of assets are defined by considering life as per schedule II of Company Act 2013. 2. Depreciation method is followed on consistent basis.	As per company policy	1. Check useful life of tangible assets should not be ordinarily different from the useful life specified in Part C of the Schedule II of the Companies Act, 2013. 2. Check residual value should not be more than 5% of the original cost of the tangible asset. 3. Where a company adopts a	Compliance of Schedule II of Company Act 2013	1. Current year and previous year FAR to check useful life of asset 2. Depreciation schedule as per Company Act 2013.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					different useful life or uses a different residual value as above, the company is required to disclose such difference and provide justification, that it is supported by a technical advice. 4. Check depreciation methods applied are followed consistently. 5. Check for changes needs to be made to comply with the requirement of statute, change in accounting standard			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					and as needed for better presentation. 6. Electricity Company has to continue to charge depreciation in accordance with Electricity Act. 7. Depreciation on asset which is used in double/ triple shift is to be increased by 50% and by 100%, respectively. 8. Verify the basis of which useful life estimates are made			
		The depreciation method may not reflect pattern of future economic	Depreciation method is used by considering asset's future economic benefits are expected to	As per company policy	1. Check compliance of Ind AS 16, the depreciation method	Compliance with Ind AS 16 Property, Plant and Equipment	1. Analysis sheet of future benefits 2. Depreciation	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
		benefit from assets as per Ind AS 16.	be consumed by the entity.		used shall reflect the pattern in which the asset's future economic benefits are expected to be consumed by the entity. 2. Verify the depreciation method applied to an asset shall be reviewed at least at each financial year-end and, if there has been a significant change in the expected pattern of consumption of the future economic benefits embodied in the asset, the method shall be changed		schedule as per Company Act 2013.	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					to reflect the changed pattern. Such a change shall be accounted for as a change in an accounting estimate in accordance with Ind AS 8. 3. Check depreciable amount of an asset shall be allocated on a systematic basis over its useful life. 4. Check residual value and the useful life of an asset shall be reviewed at least at each financial year-end and, if expectations differ from			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					previous estimates , the change(s) shall be accounted for as a change in an accounting estimate in accordance with Ind AS 8, Accounting Policies, Changes in Accounting Estimates and Errors.			
	Impairment	Impairment analysis may not be performed by the company	On yearly basis, company is performed impairment analysis on assets.	As per company policy	1. Check how company reviews the carrying amount of its assets, how it determines the recoverable amount of an asset. 2. Check when company recognise	Compliance of Ind As 36, impairments of items of property, plant and equipment	Impairment analysis of the company	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					s, or reverses the recognition of an impairment loss. 3. Check other compliance as per Ind AS 36.			
	Income Tax Act, 1961	Non-compliance under Income Tax Act, 1961	Depreciation under Income Tax Act, 1961 is provided on percentage on Written Down Value as prescribed in Income Tax Rule, 1962.	As per company policy	1. Check whether depreciation is provided, based on block of assets. 2. Check whether depreciation is provided on the percentage on the written down value (W.D.V.) as prescribed in Rule 5(1) read with table of depreciation prescribed in Income Tax Rules,	Compliance with Income Tax Act,1961 requirement.	Depreciation schedule as per Income Tax Act	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					1962. 3. Depreciation for a period of less than 180 days is restricted to 50% of the amount calculated as above. 4. Other depreciation provision under Income Tax Act 1961.			
		Fixed Assets disposal/ transfers are not accurately calculated and recorded.	Company also complied Income Tax provisions in case of sale of asset	As per company policy	1. Check whether,if any, asset is sold discarded, demolished in the previous year then its written down value at the beginning of previous year be increased by actual cost of assets	Compliance with Income Tax Act 1961 requirement.	1. GL and calculation sheet of profit or loss on sale of asset 2. Capital gain working sheet 3. 10 sale invoice or 50% value of asset sold during the year whichever is higher.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					acquired in the same block during the previous year and be reduced by the sales consideration with scrap value, if any, and depreciation be provided on balance of such block. 2. Verify surplus arising on sale of capital asset is chargeable to tax as short-term capital gain by virtue of Section 50, these cases are: (a) When the written down value of a block of asset is reduced			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					to nil though all the assets falling in block are not transferred. (b) When a block of asset ceases to exist.			
	Intangible Asset	Non-compliance with statutory low requirement	Company complied with Company Act, 2013 and Income Tax Act, 1961 requirements.	As per company policy	1. Check schedule II of Companies Act, 2013 for the Intangible assets, the provisions of accounting standards applicable for the time being in force would apply (except in the case of intangible asset created under Build, Operate and	Depreciation on intangible asset	Depreciation schedule as per Company Act and as per Income Tax Act.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					Transfer (BOT) or Build, Own, Operate and Transfer (BOOT), etc.). 2. As per Income Tax Act Depreciation @ 25% is allowable on intangible assets, namely, know–how, patents, copy rights, trademarks, licenses, franchises, or any other business or commercial rights of similar nature. 3. Check the impairment tests for intangible assets. 4. Review the amortizati			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					on methods used for intangible assets.			
	Other Control	Due diligence decision on sale purchase of fixed asset may not be performed leads to wrong decision	Company performs proper due diligence in sale, purchase and maintenance of Fixed Assets	As per company policy	1. Check reasons and cost benefit analysis of such buying recorded. 2. Check in case of make/ buy decision, the calculation of actual cost. 3. Check that related party transactions are made at arm's length price. 4. Check whether, in case,replacement of any machinery is to be done, check reason for the same	Due diligence performed on various asset transaction	10 high sale invoices 20 high purchase Invoices	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					whether it is due to technological change or obsolescence of assets. 5. Check whether technical know-how is obtained for sophisticated machineries. 6. When any machine is scrapped, whether way of its disposal is ascertained and documented. 7. Whether break down analysis of assets is done. 8. Whether date-wise obligation for insurance and maintena			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample Size	Data analytics performed
					nce is observed.			
		Fixed Assets Register is not maintained and not reviewed at regular intervals.	There is a system of reporting various information on periodic basis and corresponding actions are taken by management.	As per company policy	1, Check pending requisitions for which Purchase Order (PO) is not raised. 2. Check list of pending Orders (Pos) for which supply is not made. 3. Check list of long outstanding advances to suppliers but fixed assets not supplied with capital commitments.	Periodic reporting and analysis	3 months	NA

Project Management

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Pre-Project Readiness	Business have domain expertise.	Risk of taking up projects which may not be financially or operationally viable or where the business does not have domain expertise. The business should do a preliminary study of the proposed project in terms of viability from (a) Financial (b) Operational (c.) Legal / Regulatory view and also consider whether the business has domain expertise in it.	Any project that needs to be taken should be assessed for its viability by the experts within the Company or with support of an external consultant. The decision to invest in new project vests with the Board of Directors. The Board of Directors may entrust to review the project viability to a committee of Directors.		Review whether the project has been approved by the Board of Directors after a due diligence is done and its viability is established.	Due Diligence of the Project	100%	
Pre-Project Readiness	Budgetary Allocation	Risk of adequate funds not being allocated or planned for the project.	Ensuring that the budgetary process includes consideration of new projects including tenure, possible borrowing costs, sources of		To review the budgetary process to ensure that the budget includes funds allocated for projects.	Adequacy of Budgetary Allocation.	100%	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			funds etc.,					
Pre-Project Readiness	Compliance to Environmental, Social and Governance requirements (ESG).	Risk of non-compliance with ESG factors which could later lead to possible shut down of the unit due to ESG related factors.	To review whether the Company has reviewed compliance with ESG regulations including pollution control norms, how the project would be useful to the community, diversified workforce, fair pay or remuneration and other factors.		Review critically decisions relating to type of equipment being procured, location of the plant, process expected to be adopted, etc., which may impact environment. To review the pay structure, gender diversification, medical and health insurance related aspects for the workforce, impact on the community around the unit. To also review the process of how the Governance (i.e., the Board) is considering investment in new project.	Review of ESG Factors	100%	
Pre-Project	Planning	Risk of Project	Review of		(a) Ensuring	Review of	100%	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Readiness		management without adequate planning of timelines and activities.	how the entire project is planned to include use of any project management tools, allocation of resources, activities and sub-activities being planned, review of the progress on a timely basis (say fortnightly / monthly) by the Board of Directors. *If there is any other committee managing the project, review the committee's report to the Board on project management and whether key issues are discussed, and action is taken to ensure the bottlenecks are removed.* Review of Actual Vs. Budgeted activities.		the project is managed within the timelines; (b) Ensuring the project is within the budgetary allocation; (c.) Ensuring that the Board of Directors monitor the progress of the project in a timely manner; (d) Review of the project progress report and compare the developments with the project report.	key project milestones.		
Project	Execution	Risk of project	Whether the		Review of	Review of	100%	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Management.	Stage	not being executed in the manner it was planned and there is delay in project execution leading to additional costs / investments, delay in obtaining the benefits it was expected and possible non-viability of the project if not done in time.	project management is continuously monitored by a dedicated team and whether the Board of Directors are appraised of the progress. Whether there is an audit or review done by a third party to certify the progress.		the project management techniques and whether those charged with governance are aware of the progress.	Project monitoring process.		
Project Management.	Execution Stage	Risk of taking alternative courses of action without formal approval process thereby delaying the project or incurring additional costs.	Any alternative courses of action or decisions should have been approved by the Board or delegated authority.		Review of all the alternative course of action with management approval.	Review of Project monitoring process.	100%	
Project Completion	Completion Stage	Risk of non-compliances with various laws and regulations to ensure commencement of operations.	The Company should have a checklist of all compliances that would be required and whether the same has been complied with or not should be reviewed by		Review of the checklist being prepared and ensuring the compliance.	Review of legal compliance	100%%	

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			the general counsel / legal expert.					
Project Completion	Completion Stage	Risk of not ensuring that all the aspects of project completion are complied with or not.	Project completion report should be prepared and submitted to the Board including (a) Budget Vs. Actual variances and reasons (b) Certifying that all regulatory approvals are obtained.		Review that the project is completed and certified in all respects.	Review of the closure process	100%	

Inventory Management

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
Inventory Management	Initialization	Stores in not functioning properly.	Stores functions are defined and documented.	1. Obtain a certified copy of the Trial Balance for the period under audit. Alternatively, extract the Trial Balance from the system. 2. Obtain: i. Key Result Areas/ Objectives of the Stores Function as well as of the Unit/ Category under audit; ii. An organogram of the Stores Function; iii. Delegation of Authority; iv. All policies, standard operating procedures, office orders, etc. which relate to the Stores Function. 3. Ask whether any work has been done on IT General Controls (ITGC) / Segregation of Duties (SoD) (in ERP environment) controls. Review the report thereof and modify the audit program accordingly. 4. Read the			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				internal audit report of the previous internal audit as well as any comments made by External Auditors and identify any unresolved issues for follow-up with Management. Review the status of such matters with Management and document the results of the same. *Note: There would be possibility that there would be other departments other than stores which would be involved in inventory management such as Quality, Production Planning & Control (PPC), Procurement depending on the company and industry. Ensure that the audit steps given above/ below are used wherever applicable.*			
Inventory Management	Initialization	Inadequate controls over inventory management	Inventory management procedure is defined and	A. Conducting an analytical review would reveal certain trends which would indicate			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			documented.	inadequate controls over inventory management. An indicative list has been given below: i. Comparison of Cost of goods sold with the Sales; ii. Identification of short receipts per inventory items/ vendor; iii. Comparison of rejections/ returns to vendors with the receipts; iv. Comparison of goods issue with the production planning. Further a trend analysis can be conducted to identify control weakness. An indicative list for trend analysis: i. Inventory turnover – how many days inventory has been maintained against the norms defined by the company; ii. Inventory ageing analysis: . percentage of inventory lying for more than 180/ 360 days; . percentage of inventory non-moving/ slow-moving for more than 180/ 360			

420

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				days; . percentage of inventory lying in damaged, expired, near-expiry, rejected locations etc., for more than 180/ 360 days; iii. %age of total inventory (RM/ PM/ FG) lying in damaged, expired, near-expiry, rejected locations, etc; iv. Disposals then reorder – multiple instances of any particular inventory item being prematurely designated as scrap and re-ordered; v. Rejections and Returns – Check whether there is an unusually high incidence of returns and rejections from any particular vendor.			
Inventory Management	SOP for Inventory management	1. SOP may not be defined to ensure consistency and standardization of operations including Segregation of Duties (SOD).	1. Organizatio n has clearly defined Standard Operating Procedures and Delegation of Authority (DOA) for inventory manageme	1. Check whether SOP is available and complete in all aspects of roles, KPI, timelines, frequency, MIS, Responsibility Assignments Matrix (RACI), etc. 2. Check when SOP was updated last and process of change management i.e.	1. Identify key metrics and performanc e indicators that are important for inventory manageme nt such as order fulfilment rate, lead		

421

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			nt in place. 2. Organizatio n has defined sequence of Activities, Roles and Responsibil ities, Key Performanc e Indicators (KPIs), Timelines and Frequency of activities along with various documents to be maintained for Inventory manageme nt (including adequate segregatio n of Duties)	proposal to change, acceptance and approval of amendment to SOP. Standard Operating Procedures for Inventory Management (including at-least the following): i. Detailed procedures for receipt, storage and movement of stocks; ii. Inventory levels (re-order level, minimum order level etc); iii. Stacking norms; iv. Inventory holding norms (ex. Domestic RM/ PM – 60 days; Imported RM – 90 days; Imported PM – 60 days etc.); v. Procedure to be followed for all of the important activities described above under Segregation of Authorirty (SoA) / DoA; 3. To benchmark the existing SOP with the companies from similar/different industries for process standardization. 4. To assess whether	time, stock turnover rate, DOA rate, etc.		

422

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				Delegation of Authority (DoA) mapped is in-line with current organization structure and updated to reflect current processes in-place, including but not limited to maker-checker-approver concept 5. Review the above documents from the point of view of: i. Segregation of duties; ii. Coverage; iii. Design of controls. 6. Check the coverage/ adequacy of the documented policy / manual / standard operating procedures (SOP) in respect of the above-mentioned areas. 7. Inquire as to when these policies were last updated / reviewed and when the next review date is – these should be reviewed at-least annually or whenever there's a significant change in business model, whichever is earlier. 8. If the Company does not have			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				formally documented policies/ guidelines or standard operating procedures, review available financial/ non-financial inventory information and conduct interviews with operating management to identify the significant processes in the Stores Function. Assess the risk due to absence of documentation (eg. In absence of SoP for inventory management, a high staff turnover in the stores function might indicate towards inadequately maintained inventory records) and accordingly modify the audit program; Also ascertain the extent of automation in the Stores Function. Basis the Key Result Areas/ Objectives, document the significant risks and mitigating controls. These should be tested in the Work Program, unless some are			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				clearly out of scope. Illustrative list of important activities which should definitely be mentioned in the SoA/ DoA: i. Approval for write-off from financial books/ physical destruction/ cycle-count adjustments/ shortages or excesses identified during quarterly or annual physical verification; ii. Approval for re-allocation of inventory from saleable to non-saleable/ damaged/ expired storage locations – usually this may be an automated process; iii. Approval for movement of inventory on Returnable Gate Pass (RGP) or Non-Returnable Gate Pass (NRGP).			
Inventory Management	Material master	1. Inadequate maintenance of material master and inadequate access rights relating to Additions,	1. Access to material master is restricted only to the authorized personnel of inventory department	1. Check access rights for creation/modification of Material master. 2. Check Approved request for material code creation/modification from user	1. Verify material master for any missing details. 2. Verify unauthorized creation of material codes.		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		Modifications and blocking of material codes 2. Incorrect data is updated in the material master 3. Shortage of material due to materials levels being not defined 4. Materials not routed for QC clearance or takes more time for QC clearance 5. Invalid/Inaccurate changes being made to the inventory management master file	or Master Data Management (MDM) team. 2. The material code is created based on approved request from user department. 3. Material master is reviewed on a regular basis and discrepancies noted, if any, are corrected. Logs of changes are generated from the system and approved. 5. Each of the materials has minimum level, maximum level, ROQ, ROP defined at master level.. Critical materials, if	department and creation/modification of material code in ERP by authorized personnel only. 2. Review material master change log and check whether same were done by authorized personnel only after approved request from user department. 3. Review the dates for requests for change with the log maintained for actual changes made.'- Check for any pending requests and ascertain the reasons thereof 4. Check maker-checker process for creation/modification of material code in ERP 5. Check whether periodic review carried out for Material master 6. Check process to carry-out material criticality assessment to identify critical materials/spares 7. Check whether all materials have ABC classification and inventory levels defined 8. Check whether	3. Verify duplicate material codes created for same items. 4. Verify whether correct valuation type selected. 5. Verify material master change log for any unauthorized changes. 6. Verify correct HSN code mapping and correct tax classification. 7. Verify QC enabled or not for material codes. 8. Verify whether safety stock, minimum stock, maximum stock, reorder level, lot size, etc. defined. 9. Verify correct cost Centre/		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			any, are identified and mapped for ABC classification. 6. System to be configured for not to allow creation of duplicate material code for same material. 7. Define requirement of QC clearance at material code level i.e. whether material is required to be routed through QC process.	defined materials are cleared via QC check before GRN or issuing for consumption	profit center selected for material code. 10. Verify turn-around time for QC clearance along with material pending in QC for longer time.		
Inventory Management	Material Requisition	1. Unauthorized preparation/ modification of material requisition slip 2. Inadequate inspection of material at entry gate	1. To have defined DOA/DOP for creation of material requisition slip and authorization of material requisition slip. 2. Material requisition slip is	1. Check documented SOD, access rights and whether they are followed or not 2. Verify conflicting access rights and inadequate SOD 3. Verify material requisition slip authorized by respective person as per DOA/DOP 4. Verify period review of	1. Verify that whether there is any conflicting access rights given to the user 2. Verify that whether DOA/DOP has been defined for MRS		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		raised for requisite material and quantity by authorized personnel only, while modification of requisition slip to be done only after proper justification and approval from HOD 3. To ensure that no material can enter factory gate without due inspection from security person	outstanding requisitions pending approval along with justification 5. Is there a system of preparing requisition slip by the production department to source the materials from Stores dept/ or is it automatically generated through the ERP System? In case it is automatically generated then ensure that the requisitions are created basis the Bill of Material loaded in the ERP System; 6. Review of instances wherein special requisition notes(outside BOM) have been issued and root cause analysis for the requirement and frequency for issuance of the same	3. Verify MRS prepared and approved as per defined DOA/DOP 4. Verify list of Material requisition slips pending for approval since long 5. Verify that whether all necessary details in MRS were mentioned or not		
Inventory Management	Material Issuance	1. Unauthorized preparation of issue note and/or delay in issue of material. 2. All	1. Access to inventory module is restricted to authorized personnel only.	1. Check list of persons having access right for issuance of material. 2. Check unauthorized issue of material. 3. Check delay in	1. Verify that whether there are any conflicting access rights given to user		

428

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		material issued may not be recorded or may not be recorded promptly. 3. Material issued physically is different from the one stated in requisition slip. 4. Materials issued may be accounted at incorrect price/rate. 5. Earlier procured material is not issued and leads to quality deterioration /pile-up. 6. Material specific to the Bill of Material (BoM) or maintenance is issued as general consumption. 7. Cost of material consumption is not recorded to the appropriate	2. Materials should be issued on a timely basis as per requisition and consumption to be recorded in ERP with no delay. 3. Segregation of duty between personnel preparing issue slip and one physically moving material and updating bin cards. 4. Based on the MRS prepared, system to auto-fetch quantities and rate of material issued. No manual intervention to be allowed for manually modifying rate or quantities while	issue of material. 4. Check material issuance without material requisition for materials wherein MRS is required to be prepared in ERP. 5. Check outstanding requisitions against which material issue is pending. 6. Check sample issue slips to verify that correct material is issued in ERP, along with delay in recording material issue in ERP as compared to actual issue of physical material. 7. Check pattern in which the material is being issued i.e. FIFO or LIFO 8. Check whether BoM material or maintenance spares are issued as general consumption. 9.Obtain an understanding of the process followed for issue of goods; obtain the system report of the issuance made during the audit period; 10. Check whether there is a system of updating the stock in system at	2. Verify that whether DOA/DOP has been defined for Material issue 3. Verify Material issue slip prepared and approved as per defined DOA/DOP 4. Verify list of Material requisition slips pending material issue since long 5. Check delay in material issue by comparing entry date and posting date and verify posting date with physical issue slip 6. Check rate of material issue is as per policy of company. (For e.g.; in case of		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		cost center.	posting material consumptio n. 5. Unless otherwise specified, the materials to be issued on FIFO basis. 6. Periodic review or system configurati on to be there to ensure that all materials are correctly issued against production/ maintenanc e orders.	the time of issue to the shop floor or is the same done at the end of the day. 11 Is there a system of Issue slips against each requisition slip; Are the receipts against the issues acknowledged by the shop floor in-charge; 12. Check the inventory movement from warehouse / shopfloor locations. In case of any transfers to locations other than those involved in production, seek explanation for the same 13.Select samples from the issues and ensure that each issue: : i. Issues are made as per requisition which is consistent with the latest Bill of Material; ii. Issues are approved as per the DoA; iii. Timely issue of goods; iv. Goods are quality approved; v. Issues are recorded in Material Issue Note; vi. Material is	moving average, compare moving average rate for the period with material issue rate) 7. Verify ageing of inventory to ensure that the material is issued on FIFO and inventory is not getting piled-up 8. Carry-out material movement analysis (in comparison with past 2-3 period) to see procuremen t, ageing, lead-time and consumptio n pattern of individual materials 9. Verify that BoM items and maintenanc e spares are issued against specific orders only i.e. production order or		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				issued in presence of quality dept. personnel; vii. Issue notes are acknowledged by the receiver; viii. Timely updation in Inventory system. 14. Inquire whether there has been any reversal of the issued goods. Obtain the system report of the reversal of the issues made during the year. Inquire on the reasons for the returns and approval process. In case of industries where back flushing is done. Understand the back flushing process and inquire on the process of identification of negative stock position.	maintenance order, and not as general consumption 10. Verify that all materials issued as general consumption have cost-centers mapped, while correct cost-centers are mapped to the department/ function to which the said consumption pertains		
Inventory Management	Material Return	1. Unauthorized return of material to stores 2. Incorrect valuation of returned material 3. Procurement and consumption	1. Material is returned to stores after appropriate authorizations 2. Appropriate accounting treatment is done for returned	1. Check material return rate is same as per material issue rate 2. Check that material return slip is authorised by appropriate authority along with adequate justification of material return. 3. Check whether	1. Check material return entry made against corresponding material issue slip 2. Check material return transferred to		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		of low quality of material	material 3. Root-causes of materials returned from production floor to be analysed to ensure whether there exists any quality issue in material supplied by vendor	material returned is transferred to blocked stock or not in case of damaged/rejected material 4. check correct entry is posted in ERP for material return against original material issue slip 5. Review the time taken in return of rejected material to the vendor and inquire into cases of undue delay; 6. Check that the rejected material which has not been returned to the vendor is stored separately from normal material; determine the ageing of such materials and understand reasons for items held since long time; (also determine the management guideline w.r.t. in what time rejected goods should be returned to vendors); 7. Review reasons for rejections and action taken. In case the Stores Department responsible for issuing Debit	blocked/restricted stock in case of rejected/damaged material 3. Check reversal of consumption entry in case of return of consumable items 4. Check frequency of material returns from specific user/department/machine 5. Check process of QC approval and technical verification before taking approval to scrap out, if any 6. Check that returned material is stored to same location/bin from which it was originally issued 7. Check that there is		

432

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				Notes / asking for replacements, verify whether they have been raised properly or not? Inquire whether production has been hampered because of rejections? Inquire as to who bears the cost of returning the rejected goods to the vendor and suggest possible changes in case the company bears the cost. 8. Check whether the debit notes have been passed directly in the FI Module and adjustment may not have been done in inventory stock ledger; 9. Check whether there has been subsequent reversal of rejected material and the same has been approved by Quality dept. based on documented justification. 10. Conduct a physical verification of the area where rejected goods are stored. Obtain the rejection report and verify the	no change in cost-center while recording material return i.e. cost-center opted for recording material return to be same as material issue 8. Verify that quantity of material return/consumption reversal does not excess the quantities of material issued till date		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				physical availability of the rejected goods. Inquire for missing items and the reason for the same. Identify long pending items in the rejection report and inquire the reasons for delay in dispatch/ liquidation/ destruction of said stocks			
Inventory Management	Inventory Valuation	1. Inventory lying with individual departments, at period ends, may not be considered for purpose of inventory valuation. 2. Inventory may be recorded at the incorrect cost under the entity's costing method (e.g., FIFO, LIFO, Average Cost, Standard Cost). 3. Inaccurate valuation of the stock being transferred	1. Inventory value as per MIS/Costing & Financials is reconciled to ensure accuracy. 2. Weighted Average Cost method is followed for inventory valuation & inventories at each month end are valued accordingly. 3. Material transfer from one unit to other are valued	1. To check which cost method is followed for inventory valuation 2. Transfer pricing rules are followed or not 3. Inventory value as per MIS/Costing & Financials is reconciled to ensure accuracy. 4. Check correct valuation type selected for all material codes at respective location 5. Check cost of transportation and other incidental cost incurred were considered for inventory valuation 6. Check whether correct variance posting entry for difference in standard price and actual price is posted 7. Check inventory	1. Compare value of inventory reflected in material module and finance module 2. Check inventory showing at zero value 3. check receipt of inventory at zero value 4. check difference in rate of inventory at receiving and supplying location in case of transfer of inventory (e.g.; material transfer from X		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		to other units, private parties or other organizations.	based on transfer pricing rules and reviewed at a level that identifies inventory age, status, expiration dating, etc.. On each month end while preparing monthly MIS & Financials to ensure accuracy of costing & valuation of such inter-site transfers. 5. Material disposals and rejections should be reviewed for trends, or signs that other inventory materials may be subject to obsolescence. 6. Decisions regarding materials under	showing at zero value 8. Check inventory valuation for non-moving and slow moving as per policy of the company 9. Check adjustment entry made in books of account for provision of diminution in value of inventory 9. Check correct disclosure of inventory valuation in financial statement as per applicable GAAP/Ind AS & correct disclosure of Inventory in Tax Audit report. 10. Check that inventory is valued at cost or NRV whichever is lower 11. Check that manual changes in inventory value should be done by authorized persons only 12. Check that value of obsolete material is reduced to give impact of obsolescence 13. Check the provision made in books of accounts for non-moving and slow-moving inventory items	location at Rs. 100 and material received at Y location at Rs. 90) 5. Verify calculation of standard price of inventory and check whether all necessary cost were considered to arrive at standard price 6. Compare material movement rate with standard price to identify material movement at other than standard price 7. Verify variance posting entry for difference in standard price and actual price 9. compare inventory valuation not more than its net realizable value.		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			QC/QA review should be documented and approved to support financial reserves or lack thereof.		10. Check log of changes in inventory value to identify unauthorized change in inventory value		
Inventory Management	Gate Inward/ outward	1. Material received in the company without authorization 2. Incorrect material is received as compared to what was actually ordered 3. Quantity of material received in excess or short as compared to purchase order	1. Gate inward entry is made in the system itself by the person verifying the material at gate 2. Qty cannot exceed the PO quantity and GRN cannot be prepared without gate inward entry 3. Gate outward should not be allowed without Returnable Gate Pass (RGP)/ Non-returnable Gate Pass (NRGP)/ sales	1. Check Gate inward register 2. Check whether all GRNs were made against gate inward only. Inquire if there are manual receipts of material without Gate Entry/ GRN. Verify the documentation maintained and the process of regularization of manual receipts and Identify the causes for manual receipt of material and inquire the action taken by the management to prevent such occurrences; 3. Check inward quantity in gate inward entry does not exceed PO quantity (inc. tolerance limit) 4. check delay in gate inward entry from gate inward date 5. Check delay in	1. Compare GRN quantity and gate inward quantity 2. Check total quantity inward during the period against PO with PO quantity 3. Check delay in gate inward entry from gate inward date 4. Check delay in GRN against gate inward entry 5. Check material inward without PO (emergency procurement) 6. Check		

436

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			invoice 4. Tolerance limits are defined in the system to restrict excess/shortage receipt of material	GRN against gate inward entry 6. check long aged pending GRN entries against gate inward date 7. check whether adequate adjustment entry passed for goods in transit in books on cut-off date/book-closure date 8. check SOD between person doing gate inward and GRN entry 9. Check Gate outward entry made only against RGP/NRGP/sales invoice 10. Select a sample & analyse the following: i. Ensure that a record is maintained at the Plant gate for all goods/ materials received at the Plant - Gate Entry Record is prepared; ii. Ensure that a Goods Receipt Note (GRN) or equivalent is prepared for every receipt of goods; iii. GRN is prepared against a valid Purchase Order (PO)/ Contract; (Check whether the IT	long aged pending GRN entries against gate inward date 7. Check whether adequate adjustment entry passed for goods in transit in books on cut-off date/book closure date 8. Check access rights for Gate entry and GRN with same user 9. Check access rights for RGP/NRGP /sales invoice and gate outward entry with same user		

437

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				system or the manual process, as applicable, allows a GRN to be prepared without a PO/ Contract); iv. Date of PO is before the date of GRN (to determine whether the client follows a practice of ordering verbally & preparing POs at the time of receipt of goods in Plant); v. Timely preparation of GRN subsequent to entry in Plant premises; vi. Timely inspection of goods received, by the Quality Dept.; vii. Timely availability of the material (in the system), for issue to production; viii. GRN quantity is after subtracting the Quality Sample – (understand how documentation/ accounting is done for sample quantity withdrawn by Quality for testing); ix. Compare details of Challan and Inspection Report with the copy of Purchase Order and investigate for			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				differences, if any; x. Quantity received matches quantity per Purchase Order, (or within acceptable tolerance limits as defined by client management); xi. In case receipts in excess of PO quantity then ensure that the Stores personnel accepts such excess quantity only once the PO is amended & re-approved per DoA xii. Ensure that all material receipts are updated in Inventory only after approval by Quality Dept.; (understand how it is ensured that no material can be received without quality testing – usually control is built-in in the material master in the IT System); xiii. In case goods are damaged in-transit, claims for insurance is put in as per the policy/ debits are made to the CFA / Transporter / Vendor; accordingly, xiv. Confirmation of receipt of goods			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				being sent to the Accounts department to facilitate passing of supplier's bills; (also check for review of GR/IR at the month end); xv. Check for ModVAT Benefit taken on the Input raw material at the time of receipt of material (also ensure that in case the Plant is located at an Exempt Location then ModVAT benefit should not be taken): xvi. In case of imported material ensure Bill of Entry & other necessary documents are available before accepting goods in the Plant premises. 5. Obtain a listing of PO's and quantities received against the same. Analyse the following: i. PO's are automatically closed/ blocked once 100% receipts have been made against the PO, to ensure that further supplies cannot be made; ii. The time period for which POs are			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				'open' & determine the reasons thereof; 6. Obtain the list of GRN reversals and verify the following: i. The reason for reversal; ii. Approval for reversal; iii. Supporting documentation; iv. For the selected samples verify if subsequent GRNs have been generated and are genuine			
Inventory Management	Returnable Gate Pass/ Non-Returnable Gate Pass	1. Material moved outside the company without authorization 2. Material being stolen or missing from the third-party location 3. Sub-contracted material cannot be made available on required date 4. Levy of interest and penalty under GST law if material	1. Only authorized personnel can access RGP/NRGP functions in ERP. 2. Unless authorized, gate pass cannot be printed. In absence of printed gate pass, goods will not be allowed to exit factory gate. 3. Continuous monitoring to be done for material sent of RGP basis.	1. Check DoA/ DoP for preparing RGP/NRGP 2. Check whether RGP/NRGP created as per defined DoA/ DoP. 3. Check long-aged outstanding RGP 4. Check delay in return on material on RGP basis along with justification 5. Check penalty clause for delay in return of material in the PO of contractor and whether same is followed or not. 6. If material is not received back within 1 yearyears3 year for Input goods or	1. Check whether RGP/NRGP created from ERP or not. 2. Check delay in return of material sent against RGP and check appropriate action taken for reversal of GST credit in case of delay beyond specified time limit 3. Check release of RGP/NRGP		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
		cannot be returned within the time-limit defined in GST law 5. Materials returned back on RGP are not recorded or reconciled 6. Material actually received back is different than what was agreed to be received back on RGP	In case of any change in expected date of return, proper approval to be obtained from concerned HOD 4. Periodic confirmations to be obtained from third-party vendors (sub-contractors) to confirm quantities of material lying with them 5. In case of any mismatch in physical material quantity with books, immediate actions to be taken 6. Materials sent on RGPs should be received back against same reference of RGP	capital goods respectively, GST credit is required to be reversed and added to output tax liability. Check whether same is followed or not.	and extension of due date, if any followed in ERP 4. Check turn-around-time for material returned back from vendor		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			only, while all RGPs to be periodically reconciled				
Inventory Management	Inventory Reconciliation	1. Differences in physical and book stock may not be identified. 2. Unauthorized adjustment of difference in book stock and physical stock 3. Material adjustments are posted at incorrect/manually updated rate 4. General ledger inventory balances are inaccurate/ unsupported.	1. At periodic interval, physical verification of inventories is carried out by Internal/external parties at all sites wherein physical quantity is reconciled with book quantity at all sites for all categories of materials 2. To make sure that all items are covered under physical verification once in a year 3. Adjustment to inventory quantities by way of write-offs	1. To check book stock is periodically & regularly reconciled with physical stock. 2. Write-off/ write back are duly approved as per authority matrix. 3. Conduct surprise physical verification (PV) of inventory 4. Check documents of physical verification and verify that whether the noted differences were approved by appropriate authority, along with root-cause analysis 5. Obtain periodic physical verification sheets,and review the reconciliation thereof with Book Stock. check i. Is there a written guidelines for PV and it is circulated to the concerned team members. ii. Ensure that the frequency of the physical count is	1. Verify material adjustment movements and its frequency to identify certain pattern/user /department doing it frequently 2. Verify the rates at which such write-offs and write-backs are posted.		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			or write-backs are approved by appropriate authorities	adequate. iii. Ensure that the counts are performed by employees whose functions are independent of the physical custody of inventories and record-keeping functions. iv. Verify availability of documentation of the PV, reconciliation with book stock, approval of senior management and adjustment with book stock. v. Inquire if significant differences between physical counts and detailed inventory records investigated before the accounting and inventory records are adjusted to match the physical counts. vi. Is there any time gap between physical verification and adjustments made to the stock ledger? vii. Understand the cycle count procedure. viii. Select samples of the cycle count			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				conducted and ensure compliance with procedure. ix. Identify instances of consistent high difference for particular items. Inquire for the actions taken by the management for the identified casuals. x. Ensure that the movement of inventory adequate controlled during the physical count to ensure proper cut off.			
Inventory Management	Slow-moving/Non-moving Items	1. Inventory build up in stores leading to high carrying costs and working capital being blocked. 2. Incorrect representation of financials due to lack of provisioning policy	1. ERP contains requisite data for non-moving & slow-moving items. However, no controls in place to restrict procurement of items already available in inventory. 2. Such items are reviewed on quarterly basis and if required, such items	1. Check clear policy or practice on disposal related to non-moving and slow moving inventory goods. 2. Check periodic review document relating to review of slow-moving & non-moving inventory 3. Check inventory ageing report to identify non-moving/ slow-moving inventory 4. check whether inventory with expired shelf life considered or not (if available). 5. Analyse the stock holding period of each category of items	1. Compare slow-moving & non-moving inventory with inventory ageing 2. Verify open PO and PR for non-moving inventory 3. Verify movements of shelf-life expiry materials in ERP 4. verify system controls to block the material approaching expiry to		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
			are transferred to other sites for consumption.	and compare the same with the company guidelines. Through discussions with the management identify and isolate items where inventory may have been built up for strategic reasons. 6. Inquire into cases where the inventory holding is significantly at variation with established norms. Discuss the analysis with the management in detail. 7. Steps to carry out stock holding analysis: i. Obtain the closing stock details for 6 to 12 month-ends; determine the average daily stock; ii. Obtain the total consumption (RM/PM) or sales (FG) for the same 6 month period; determine the average monthly consumption; iii. Determine the number of months' inventory from above; iv. Identify instances of high	restrict further consumption/sale of the same		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				inventory holding where the no. of months is also high and discuss the same with Stores/ Production/ Procurement personnel to understand the reasons thereof; v. Document the exceptions/ deviations noted; 8. Determine if the management regularly receives and reviews reports on ageing of inventories as well as slow/ non-moving items. 9.Inquire about the existence of any obsolete/-damaged inventory. Check the authorization for categorizing such items as obsolete/ damaged inventory and action being taken by management for liquidation of such items. 10. Scrutinize the stock ledger for the audit period and identify items which have: i. Either not been issued; or ii. Where the receipts are significantly in excess of the issues iii. Review an			

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				ageing of such items along with the value thereof. iv. Discuss the plan of action of the management on the utilization of such slow/ non-moving inventory. 11. Tour warehouse areas and inquire about any items that appear to be old, outdated or would be considered scrap			
Inventory Management	Inventory Insurance	1. Inventory may not be insured to avoid losses in case of mis-happening	1. Stock Fire floater Insurance policy for inventory cover risk of fire and burglary policy for inventory to cover risk of theft is taken 2. Value of sum insured under insurance policy is approved by appropriate authorities	1. Check whether all the location are covered under insurance and proper safety measures have been taken. Ensure that the insurance cover in respect of the average value of inventory is adequate and includes all categories of stocks 2. Value of sum insured should be approved by appropriate authorities 3. Quotation should be obtained from different vendors and verify all clauses under different quotation and accordingly obtain insurance	1. Compare actual value of inventory as per books with declaration value for the policy period and check whether excess premium is paid by company or not 2. Verify the treatment of inventory/adjustments in the books in case of any mis-happening noted, if any.		

448

Process	Sub-process	Risk Description	Control	Test Performed	Attributes Tested	Sample Size	Data Analytics Performed
				policy from vendor whose quotes match with business requirement 4. Declaration for average value of inventory should be filled with insurance company on periodic basis as per policy terms and conditions and at the time of expiry of policy excess premium should be received back by the company			

Cash and Bank

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Cash and Bank	Entity level controls	Inadequate Segregation of Duties and access rights which may result in fraudulent / unauthorised transactions	1. Segregation of duties relating to the following transactions: a. Authorization of cash / bank transactions b. Physical handling of cash c. Issuance of cheques and online payment d. Recording of cash and bank transaction in books of account, e. Preparation of Bank Reconciliation Statements. 2. Access rights (Write / Read / Delete / Modify) to various peoples in the organization is reviewed periodically	As per company policy	1. Check documented SOD and Access right list for various activity of cash and bank transactions. 2. Verify evidence of periodic review of SOD and Access rights in ERP system. 3. Verify same SOD and Access right also entered in system for approval of cash and bank transactions.	1. Documented SOD, Access right 2. Periodic review	1. SOD 2. Access right List 3. Half yearly review document	Analyse transaction carried out during the review period to identify the following: 1. Unauthorized users performing transactions 2. Conflicting transaction's rights grated to same person. There has to be a separate report on roles assigned to each of the users and then analysis of conflicting roles and responsibilities to be reviewed.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			to ensure appropriate SOD and avoid any unauthorized transactions. 3. Periodic Review of Segregation of Duties and Access rights is conducted. Interim rotation of the duties are done periodically by management.					
		Authority matrix may not be prepared or approved from Board of Director (BOD).	1. Proper authorization of cash and bank transactions as per Delegation of Authority 2. Board of Directors defines the authorities for approving & performing cash and bank transactions.	As per company policy	1. Check cash and bank transactions' DOA/DOP is available and approved by BOD. 2. In case of any authorized signatory leaving the Company, whether list of authorized signatories is revised timely with proper Board Resolution and intimated to bank.	Approved DOA/DOP for cash and bank	Approved DOA/DOP from BOD	1. Identify transactions for unusual high value compared to other transactions and seek valid authorization and documentary evidence. 2. Analyse transactions to identify possible split to circumvent payment authorization limits as per Delegation of Authority and bank signatories

Internal Audit Checklist

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
								as per Board Resolution.
		SOP may not be defined to ensure consistency and standardisation of operations.	1. The organization has clearly defined Standard Operating Procedures. 2. The organization should define sequence of activities, Roles and Responsibilities, Key Performance Indicators (KPIs), Timelines and Frequency of activities along with various documents to be maintained for performing cash and bank transactions.	As per company policy	1. Check SOP available and ensure completeness of it in all aspect of defining roles, KPI, Timelines and frequency of activities, etc. 2. Check date when SOP was updated last.	Approved SOP and completeness	Updated SOP	NA
		Review system may not be in place to mitigate risk of inappropriate cash and bank transactions.	1. The organization has set up an appropriate Management Information System (MIS) for regular monitoring of operations and financial	As per company policy	1. Check MIS for monitoring of cash and bank transaction are appropriate and cover exception transaction.	1. MIS 2. RSM 3. Fraud assessment activity	MIS for 3 months Action and step taken to identify and control fraudulent activity.	Analyse various figures reported in MIS vis a vis the details appearing in ERP system to identify instances of incorrect

452

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			activities by senior / top management. 2. Appropriate Risk Management System (RMS) is in place to identify and mitigate various risks related to project activities of the organization. 3. Appropriate Fraud Risk Assessment activity is conducted, and fraud risks are identified along with relevant controls to avoid any fraudulent transactions.		2. Check RMS in place to identify and mitigate risks and its functioning related to cash and bank transaction. 3. Check fraud risk assessment activity conducted on frequent basis and controls deployed are effective.			reporting.
			1. Reports are generated as per the requirement of management along with exceptional reports.	As per company policy	Verify reports generated meet the management requirements. Also verify following must be part of reporting:	Reporting and action on exception	Monthly Exception reports for 3 month	1. Analyse cash transaction for any cash payment more than prescribed limit for cash payment. 2. Analyse

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			2. Reports are reviewed by designated reviewing authority and actions are taken on exceptions accordingly.		1. List of stale or dishonored cheques. 2. List of long outstanding 'cheques issued but not yet presented' and cheques sent for collection but not yet collected. 3. List of authorized signatories to bank accounts 4. List of all bank account with balances including those closed during the year 5. Relevant ledgers for all cash and bank accounts. 6. List of blank cheques signed and received by the branch.			cash transaction for any cash receipt of more than prescribed limit for cash receipts.
	Cash Balance and control	Physical cash may not match with balance as shown in books	1. The organization has policy of daily recording of cash and	As per company policy	1. The auditor should carry out physical verification of cash on	1. Daily recording and reconciliation	Monthly cash physical verification reports.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			reconciliation of cash transaction with books are done by designated authority2. Surprise cash physical verification is done by independent cross functional authority. 3. Multi-currency notes are exchanged within define timeline.		surprise basis to assess if the cash balance tally with the books of account. 2. The auditor should examine whether the cash balance shown in the financial statements reconciles with the results of the physical verification after taking into account the cash receipts and cash payments between the date of the physical verification and the date of the verification. 3. Obtain surprise physical verification document to review frequency of process. 4. Internal auditor should examine whether torn	2. Surprise cash verification		

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					and mutilated currency notes are exchanged within a define timeline as per policy.			
		All cash of same location may not be verified at same time that may lead to cash balance of one entity may be presented in others.	All cash balance in the same location for all entity are verified at same time.	As per company policy	1. All cash balances in the same location should be verified simultaneously. 2. Where petty cash is maintained by one or more officials, all officials concerned deposit the entire petty cash on hand on the last day with the cashier. 3. Check whether the cashier also handles cash of sister concerns, staff societies, etc. In such a case, cash pertaining to them should also be verified at the same	Simultaneous verification of cash at same location.	Monthly cash physical verification reports.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					time.			
		Cash Insurance Policy may not cover the cash handle at different time and cash in transit	1. Company has cash insurance policy against cash balance maintained. 2. Company have cash transit insurance policy of sufficient value to cover depositing and withdrawal of cash. 3. Company also have cash fidelity insurance.	As per company policy	1. Check cash in hand at various instances should not be under insured against policy obtained by the company. 2. Check cash deposit and withdrawal transaction during audit period to insure satisfactory cash transit insurance policy. 3. Verify cash fidelity insurance policy.	Cash insurance policies	Cash insurance policies	1. Analyse transactions for cash deposit in bank and cash withdrawal from bank, if exceeded the limit as per cash in-transit insurance obtained by the Company. 2. Analyse cash balances to identify, if the cash holding exceed the limit of cash in-hand insurance policy obtained by the Company.
		Other control for cash surveillance not available.	1. Accounting of collections and payments are done on timely basis 2. Camera of surveillance of the place designated for cash handling / movement are placed	As per company policy	1. Verify various cash receipt and payment document and check whether accounting of collections and payments are done on timely basis 2. Check whether	Safe custody of cash	30 payment and receipt document or depend on no. of business transaction. Check auto alert record for	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			accordingly. 3. Cash is stored and locked in safe custody of authorised person only. 4. Managing keys for the cash safe are allowed to designated person. 5.Maintenance of register recording the handing over the keys when the cashier goes on leave etc., to another person. 6. Cashier being sent on compulsory leave for 20 days in a year and another person to act as cashier. 7. System are in place for auto alert for all cash and bank transaction.		camera surveillance of the place designated for cash handling / movement are placed accordingly. May also verify backup and monitoring of camera recording. 3. Verify cash is stored and locked in safe custody of authorised person only. 4. Verify keys are in control of designated person and check who will be authorised in absence of that person define or not. 5. Verify system of auto alert for all cash and bank transaction. Check whether auto alerts are sent to designated person.		1 month	
		All cash	All cash	As per	1. Check	Unauthoris	1. ACL	Analyse

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
		transaction may not be authorised to avoid suspicious transaction	transactions are reviewed and approved as per the approved Authority Matrix. Also, the same has been enteredinto ERP software in Access Control List (ACL).	compan y policy	that cash transactions are approved as per Authority Matrix 2. Check the ACL and confirm that the same is updated as per Authority Matrix	ed approval rights	2. Authority Matrix 3. 30 POs	Audit log of modification of cash transaction during the review period to identify the following: 1. Unauthorized users performing transactions 2. Conflicting transaction rights granted to same person.
			1. Audit logs are generated for changes in cash transaction in the system 2. Process is in place to monitor audit logs to identify any inappropriate / suspicious activity.	As per compan y policy	1. Check recording of audit logs for all cash transaction in system. 2. Verify mechanism in place to review audit logs.	Audit Logs of cash transaction	1. Audit logs 2. monthly review on logs- 3 Month.	
	Bank balance and control	Bank reconciliatio n statement may not be prepared or authorised for deviation from book balance.	1. The organization is obtained balance confirmation for all bank account including closed and dormant. 2. Bank reconciliation statements are prepared	As per compan y policy	1. Obtain independent confirmation from the bank for all bank accounts including dormant accounts as well as accounts closed during the	Bank reconciliati on statement and review	BRS for 3 months	Analyse transaction with reversal for proper authorization and reasons and ensure that the same are not manipulated to circumvent Bank Reconciliatio n Statement

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			on weekly basis by designated person and reviewed by authorised person. 3. Un-reconciled entries are identified and reason for non-adjustment are documented. 4. All reconciliation and evidence of review are verified and signed by person other than person who is responsible of receipt and payment.		year. 2. Verify whether Bank Reconciliation Statement is prepared at appropriate frequency and the same is reviewed by the authorized person for timely action on unreconciled items. 3. Long pending un-reconciled items should be verified in detail with adequate documentary evidence justifying the authenticity of transaction and reason of appearing open in bank reconciliation statement. 4. Review and approval of all reconciliations and investigation of unusual reconciling items by an			or hide any unauthorised transactions.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					official not responsible for receipts and disbursements, including recording evidence of the review and approval, by signing the reconciliation.			
			Bank reconciliation statements are prepared on a regular r basis and entry of reconciliation are posted on regular basis of bank statements to maintain books upto date.	As per company policy	1. The bank statements of the relevant period should be examined to insure whether cheques issued by the entity but not presented for payment, and cheques deposited for collection by the entity but not credited in the bank account, have been duly debited/ credited in the subsequent period. 2. Where the auditor finds that post-	Updation of books with bank statements.	2-month Bank statement of 3 banks with BRS or Depend on total number of banks.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					dated cheques are issued by the entity, he should verify that any cheques pertaining to the subsequent period have not been accounted for as payments during the period under audit.			
		Records of fixed or other deposits may not be maintained for monitoring/ examination.	Designated persons prepare record of all deposits and certificate are maintained in safe locker.	As per company policy	In respect of fixed deposits or any other type of deposits with banks, the relevant receipts/ certificates, duly supported by bank advice, should be examined and must match with books records. Verify control of safe custody of certificate or document to designated person.	Control over deposit documents	Verify all deposits certificates	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
		Unauthorized inter-company deposits	Inter-company deposits made are backed by board approval.	As per company policy	Inter-company deposits made are backed by board approval, and are done at annual average rate per annum of public sector bank.	Inter company deposits	List of intercompany loan and deposits	NA
		Financial loss on account of variance in rates agreed with the bank vis a vis charged by bank	Designated person of Finance reconciles the rate charged by the bank with the rate agreed, variation if any is communicated to the bank.	As per company policy	1. Monthly reconciliation is prepared by designated person 2. Check deviation reported to bank and corresponding action taken by bank.	Rates charges by bank	Month reconciliation statement.	Analyse calculated amount and formula etc for accuracy of amount charges by bank and calculated by finance.
		Control over banking document may not be effective	1. The organization booked collection when cheques deposited with bank for collection instead of cheques in hand. 2. All signed blank cheque are kept in safe locker with	As per company policy	1. Where post-dated cheques are on hand on the balance sheet date, verify that they have not been accounted for as collections during the period under audit. 2. Verify any signed blank	Control over cheque	Verify all reconciliation entry with cheque copies for latest month	1. Analyse bank transactions with duplicate cheque number 2. Analyse cash and bank transactions suspicious of duplicate payment viz same amount, same party,

463

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			designated person. 3. All stale cheque entries are reversed. 4. All remittances are provided in books and reconcile with bank statement on regular basis.		cheque inventory is kept in safe. Person must be authorised by BOD or designated authority for same. 3. Examine suitable adjustments are made in respect of cheques which have become stale as at the close of the year. 4. Remittances shown as being in transit should be examined with reference to their credit in the bank in the subsequent period. Finds that such remittances have not been credited in the subsequent period to ascertain the reasons for the same. Should also			and date.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					examine whether the entity has reversed the relevant entries in appropriate cases.			
	Petty cash & Imprest	Control over petty cash and imprest transaction may not be effective	1. Company has defined limit of imprest to employees. 2. Company defines nature of transaction for which imprest paid through cash. 3. Company has a policy of payment of petty cash expenses.	As per company policy	1. Is petty cash maintained for reasonable amount, verify imprest provided as per actual business need or lying idle. 2. Check the system prohibit payment of cash for transaction which may normally be paid by cheque. 3. Are all payments supported by vouchers? 4. Are imprest vouchers cancelled upon reimbursement to prevent reuse? 5. Are reimbursement cheques	Imprest control testing.		1. Analyse imprest transaction for timely settlement. 2. Verify expense incurred by all employees who are using Pre-imprest policy during audit period or imprest lying idle. 3. Analyse cash transactions for any imprest issue / settlement of more than prescribed amount as per company's policy.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					drawn only in favor of the petty cashier (custodian)? 6. Whether all petty expenses are paid as per the petty expense policy of the Company? 7. Timely settlement of the imprest balances needs to be ensured.			
	Valuation and Disclosure	Disclosure of cash and bank balance not as per accounting policies and disclosure requirement of Company Act, 2013.	All cash and bank balances are valued and disclosed as per accounting policies and statutory requirements.	As per company policy	1. Verify that cash and bank balances have been valued and disclosed in the financial statements in accordance with recognized accounting policies and practices and relevant statutory requirements, if any. Further cash and bank balance is to be disclosed as 'cash and cash equivalent'	Valuation and disclosure requirement	Financial statement	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					as per Schedule III of Companies Act, 2013. It is to be disclosed under the head: (i) balance with banks, (ii) cheques/ drafts in hand, (iii) cash on hand. 2. Further as per Companies Act, 2013 the following additional disclosures are also required to be made: (i) Earmarked balance with banks e.g., unpaid dividend. (ii) Balance with banks held as margin money/ security against borrowings. (iii) Bank deposits with more than 12 months maturity. (iii)			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					Temporary advance should not be included in cash and bank balance.			
	Payment	Unauthorized or Inaccurate recording of bank payment	1. Every day concerned person extract a list of outstanding invoices due for payment. On due date of invoice (as per payment term) designated person print Cheque/ RTGS/ NEFT (as required), generate payment advice, bank payment voucher and post entry in system. 2. After that all details are sent to approving authority for verification. Authority checks all relevant details entered in payment voucher and party account and make	As per company policy	1. Advances - Verify payment voucher cannot be generated without PO reference and beyond PO value. 2. Other payments - Designated person generate outstanding liability and payment due dates. - Basis of liability select payee and amount from outstanding list generated. - Payment list approved from designated person for payment processing. Insure following - All bank	Bank payment and control	20% advance payment 10% other payment or Depend on quantum of business and nature of transaction.	Analyse advance payment transaction with PO records and verify all advance payment should be processed after approval of PO only and within PO limits.

468

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			signature on payment advice, payment voucher and cheque/RTGS if within his limit. If approval of cheque/ RTGS /NEFT is not within his limit then same wosendsent to Controlling Head/ CFO or designated authority for approval. Once cheque gets approved same would be handed over to respective dept. for realizing payment to vendors. 3. However in case of RTGS, after getting approved RTGS copy, Designated person prepare RTGS/NEFT details and upload the same to bank site and will		payment should be routed only through payables account. - Verify that no modification in the payee account details at transaction level. - automatically retrieve cheque number from cheque master maintained in system after approval of payment advice. - Bank payment vouchers cannot be back dated.			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			receipt statement from bank on next working day. 4. Manual cheques can also be issued and later on same would be linked with system.					
			1. The payment voucher with required supporting is reviewed and authorised by the personnel authorised as per approved Authoritiy Matrix. The authority matrix is entered in the Access Control List (ACL) in ERP system 2. The supporting documentation is cancelled or defaced, once it is reviewed and payment voucher is approved.	As per compan y policy	1. Check that the ACL in ERP is as per the approved Authority Matrix. 2. In case of any authorized signatory leaving the Company, whether list of authorized signatories is revised timely with proper Board Resolution and intimated to bank. 3. Check supporting documents properly defaced and identified by cheque number at the time of	1. Access Control List 2. Supporting of deface	1. Access Control List 2. Authority Matrix 3. 30 Payment vouchers	Na

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					signature.			
		Unauthorized use/ access to cheque inventory may lead to financial losses or unauthorised online payment.	For ERP based control 1. Cheque Inventory is maintained in ERP, as and when payment is created in the ERP with Cheque as the payment mode, cheque number is auto populated 2. To ensure cheque serial number wise control, Tracker of payment through cheques is maintained and on daily basis the same is reviewed 3. Cancelled cheques if any kept for period of three months and the serial is also voided in the ERP 4. All cheques which are	As per company policy	1. Cheque whether the serial wise cheque inventory is maintained or not, ensure that the missing serial (if any) are Inventory is maintained in ERP, 2. Conduct a system walkthrough to ensure that cheque number is auto populated 3. Whether the stationery for cheques required for computerized cheque printing are under the safe custody. 4. Identify whether physical verification of unused cheques is carried out on a periodic basis 5. Check whether there is a	Control over cheques in ERP or online payment.	Latest Cheque Inventory	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			issued but not presented to the bank within the prescribed time of three months, reversed and credited to stale cheque account. 5. In case of online bank payment dual authorization is implemented.		process of reconciliation of cheque stationery with ERP and the same is duly carried out 6. Whether reconciliation of void cheques' report generated from ERP with actual void cheques is carried out and all void cheques are filed separately, and their details are updated in a file. 7. Verify stale cheque account and reissue of cheque to vendor against. 8. Check dual authorisation controls for on-line bank transactions.			
			For Manual Control 1. Cheque Inventory is maintained Manually, as and when	As per company policy	1. Whether in case of manual cheque processing, the unused cheque	Control over Manual cheque		NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			payment is created cheques are used in sequential no. and approved by designated authority. 2. To ensure cheque serial number wise control, Tracker of payment through cheques is maintained and on daily basis the same is reviewed		stationery is kept under safe custody of the senior officers 2. Whether a manual cheque inventory register is maintained by Manager Corporate Accounts in respect of inventory of the computerized cheque stationery and kept under lock and key. 3. Whether cheque receipt registered in updated timely and monitored for timely account and deposit of cheques in bank. Sample cheque transactions with deposit slips. 4. Check safeguards such as, restrictive crossing of cheques, use of pre-			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					printed, pre-numbered forms in case of manual accounting system 5. Cheques should be authorised by Joint signatories.			
			1. Payment method other than cheque are also managed with same control as of cheques. 2. If transactions are put on hold due to "stop payment" instructions, then corresponding entries are also reversed.	As per company policy	1. Other remittances by bank transfers or letters of instructions (e.g., TTs, MTS, and standing instructions) subject to the same controls as cheque payments. 2. Check when "stop payment" instructions are issued, the original entries are also reversed immediately. Verify cases were delay in reversal after stop payment instruction.	Control over other than cheque payment	50 cases of payment other than cheque method.	NA
		Unauthorized or	1. Authorised controls over	As per compan	1. Verify only some	Cash payment	50 cash payment	NA

474

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
		Inaccurate recording of Cash payment	cash payment processing and recording. 2. Cash payment vouchers cannot be back dated.	y policy	payments can be made in cash like small Inward freight, employee travelling, advance to employees, payment to small vendors where they have no bank accounts etc. on getting approval as per DOA. 2. Verify cash payment vouchers to insure manual control over cash payments approvals.	control	vouchers or as per business quantum and need.	
	Receipt	Unauthorized or Inaccurate recording of bank receipt	1. Cheques are collected by the concerned team i.e. marketing, sales, they arrange to submit to bank and simultaneously prepare PFA (Payment Forwarding Advice) to	As per company y policy	Following step to be performed 1. Verify posting of multiple collection against same UTR number 2. Verify that no modification in the customer account	Bank receipt and control	20% advance payment 10% other payment or Depend on quantum of business and nature of transaction.	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			finance for updation in customer account. 2. In case of RTGS/NEFT/ Net banking, tracking of payment is done through daily bank statement and accordingly whenever payment stands credited, the same receipt is recorded customer account. 3. Ageing is prepared by designated department are being sent to the concerned team fortnightly for follow up.		details at transaction level. 3. Verify posting of collection against blocked customer 4. Bank receipt vouchers cannot be back dated.			
			1. The receipt voucher with required supporting is reviewed and authorised by the personnel authorised as per approved Authority Matrix. The authoritiy	As per company policy	1. Check that the ACL in ERP is as per the approved Authority Matrix.	1. Access Control List	1. Access Control List 2. Authority Matrix 3. 30 cash vouchers	NA

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			matrix is entered in the Access Control List (ACL) in ERP system					
			1. Organization receives postdated cheques and blank cheques from vendors/customers as a security. 2. All cheques are maintained under safe locker in custody of authorize person.	As per company policy	1. Verify adequate system in place to store and retrieve Post Dated cheques and blank cheques obtained as security. 2. Physically verify security cheques with security tracker and to identify expired cheques.	Control over cheques as Security	Security Tracker	NA
		Cash receipt may not be deposited in bank on daily basis create risk of theft	1. All cash collected during the day are deposited in bank on same day or at earliest on next day. 2. Excess cash more than define limit by management deposited in bank.	As per company policy	1. Verify in case of multiple cash collection points (viz. in case of retail outlets), whether adequate Cash Management Services is obtained from the bank for timely banking.	Timely deposit of cash in bank	2 Month cash receipt vis a vis deposits slip/bank statement.	Analyse daily cash balance from cash record to identify cash maintenance more than define limit.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					2. Check all cash receipt are deposited in bank on daily basis or cash exceed as per define limit by management.			
	Bank balance Management	High balance maintained in account and not utilised properly to save or earn interest	Organization verify transaction in bank account, if account idle from long period and have balance are closed after approval from management.	As per company policy	1. Check all bank account and transaction in them. 2. Verify if bank account is not operative from long time and reason for non closure.	Dormant account and closure	Listed bank account and GL	NA
			Organization has proper approval policy for transfer of balance from one bank to another bank account.	As per company policy	Verify approvals of transfer from one ban to another bank.	Approval for transfer within banks	20 interbank transaction or as per business need	NA
			Organization has policy to review balance in major bank account daily and decision of transfer of balance or	As per company policy	Analyse Bank transactions to identify any idle bank balances which could have been	Utilization of funds	GL of Major bank account	Analyse Bank transactions to identify any idle bank balances which could have been utilized for

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			convert into FD are taken by considering future collection and due payments.		utilized for repayment of loans or depositing in the OD / CC limit account.			repayment of loans or depositing in the OD / CC limit account or converted into short terms FDs.
	Statutory Compliance	Non-compliance with statutory requirement leads to penalty.	Organization has system of proper training for the purpose to complied with various rules and regulation under Income Tax Act 1961, Company Act, 2013 to avoid non-compliance under any of these Acts.	As per company policy	While verifying cash and bank transaction, due consideration should be given to following. 1. The unit has repaid loans/ advances/ deposits in cash of Rs. 20,000 and above in contravention of Section 269T of Income Tax Act, 1961? 2. The entity has received loans/ advances/ deposits in cash of Rs. 20,000 and above in contravention of Section 269SS of Income Tax Act 1961? 3. The entity	Statutory compliance	GLs of cash and bank	1. Analyse cash transaction for any cash payment more than prescribed limit for cash payment. 2. Analyse cash transaction for any cash receipt of more than prescribed limit for cash receipts. 3. Analyse transactions to identify possible split to circumvent payment authorization limits as per Delegation of Authority and bank signatories as per Board Resolution.

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					has made any cash payments against expenses above Rs. 10,000 (or Rs. 35,000 for goods carriages) in contravention of Section 40A (3)/ 3A of Income Tax Act, 1961? 4. The entity received an amount of Rs. 2 lakh or more in dealings of cash transaction in aggregate from a person in a day or in respect of a single transaction or in respect of transactions relating to one event or occasion, in contravention of Section 269ST of the Income Tax Act, 1961? 5. The Company has passed Board resolution for			

Process	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					authorization the signatories to Bank Account as per Section 179(3) of Companies Act, 2013?			

Treasury Management

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Treasury Management	Initialization	NA	NA	NA	1. Obtain the Policy on Treasury Management as approved by the Board. 2. Obtain a copy of Accounting Manual or Standard Operating Procedures. 3. In case such a manual or SOP is not available, obtain an understanding of the banking process and the BRS preparation/ review process. 4. Obtain Authority matrix for Delegation of Authority w.r.t. operation of bank accounts, BRS, etc. 5. Obtain a certified copy of the Trial Balances as on the	Overview and Understanding of Treasury operations	None	1. Analyse cash flows, investment transactions and foreign exchange transactions to detect anomalies, unusual patterns, or unauthorized activities. 2. Identify discrepancies that further investigation.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					opening and cut off dates for the audit period. 6. Identify all balances with banks, whether current account, deposit account, etc. 7. Discuss the nature and the purpose of each bank account with the CFO or any other senior person from the client's side, to identify any inoperative accounts and understand any specific purpose for which they are maintained. 8. For the last year, year, plot a bird's eye view of the total number of bank accounts (E.g. Current Account, Deposit Account, etc.) vis a vis Balance Confirmation			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					s available. Be alert for any trend, e.g. confirmation a particular bank balance not being received. Inquire into any unusual trends. 9. Ensure that there is clear bifurcation of responsibilities to ensure that no single individual has complete control over all aspects of treasury functions. 10. Distinct roles for activities such as cash management, payment approvals, investment decisions and reconciliation are defined.			
Treasury Management	**Risk management framework and governance (including Treasury Policy)**	Absence of a Standard Policy/ Risk Management Framework may lead to person specific decisions/ actions.	Treasury objectives and risk appetite should be clearly defined in policy document.	Treasury Head	1. Obtain copy of Treasury Policy and assess whether it is updated and approved by the appropriate	Duly Approved comprehensive Treasury Policy and Risk Control Matrix	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					authority. 2. Whether the policy align with the organization's overall financial objectives and risk appetite. Check whether the policy address various financial risks, including liquidity risk, interest rate risk, credit risk, and foreign exchange risk. 3. Check whether clear roles and responsibilities are defined for treasury personnel.			
Treasury Management	**Segregation of Duties**	Lack of segregation of duties over keys, cash/ funds activities.	Segregation of duties is enforced through organisational structures, user access in the treasury/payment systems and	Treasury Head	1. Verify the Segregation of duties is implemented to the extent that it is possible, given the number of staff available in finance related	Segregation of Duties in Treasury Activities	100%	1. Identifying unusual patterns in transaction data such as large or frequent payments. 2. Analysing access permission and identify any individual

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			procedural documents. There should be an effective segregation of key duties including dealing, settlement, and accounting/ reconciliation. These segregations need to be further strengthened if the treasurer executes transactions. This segregation is reinforced through procedures documentation and position descriptions.		functions. 2. Compensating controls such as senior management oversight are used.			having excessive access to sensitive data or systems
Treasury Management	**Bank Account Management-Opening and Closing of Bank Account**	Unauthorised personnel may open or close bank accounts.	The Board has approved authority matrix to enter/ terminate bank relationships, including opening and closing of bank accounts.	Treasury Head	1.Confirm that the Board of Directors or other authorized body has explicitly authorized the approval authorities for entering, terminating, and	Authorized Opening/ Closing of Bank Account, Review of Inactive bank accounts	100%	None

486

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			(e.g. Bank accounts can be opened or closed only by resolution of the Board of Directors or other authorized body or official). Inactive bank accounts are reviewed and closed. When a signatory is no longer authorized to access the account, the bank should promptly remove their access. This prevents unauthorized individuals from conducting transactions.		managing bank relationships. 2. Identify the list of Bank Accounts Opened and closed during the period by reviewing the Trial Balance (current and previous period). Verify that these were duly approved. 3. Confirm that inactive bank accounts (those not actively used) are identified and reviewed periodically and check whether there are clear criteria or guidelines for classifying accounts as inactive.			
Treasury Management	Bank Account Management- Authorized Signatory	Unauthorized person act as a signatory for bank accounts. Fraudulent	Signing Limits are clearly established/ stated. There must be two	Treasury Head	Ensure that there are dual signatories (for both online and cheque	Signatories to Bank Account	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
		or Incorrect payments are made.	authorized signatories (e.g. A senior management level non-financial functionary and Corporate Treasurer/ Assistant Treasurer). Signatories for cash disbursements can be added only by resolution of the Board of Directors or other authorized body or official		payments) for each bank account and the same has been approved by the Board.			
Treasury Management	Bank Account Management - Compliance to GAAP	Compliance with bank account restrictions is timely reported to management and necessary disclosures as per applicable GAAP are not made.	I - Corporate Treasury maintains up-to-date record of all bank accounts opened/ closed with their name, locations; name, titles and functions of local signatories; and rationale for opening/clo sing an	Treasury Head	1. Verify that Corporate Treasury maintains a comprehensi ve record of all bank accounts, including those that have been opened and closed and check that the records contain relevant information, such as, the bank's name, location,	Complian ce and Disclosur es relating to Bank Account	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			account. A separate general ledger account is maintained for each bank account. II – Management responsible for monitoring compliance with bank account restrictions (e.g. those in case of Foreign Currency accounts), periodically reviews the compliance status. Adequate guidelines have been drawn for capturing necessary information for financial statement disclosures (i.e. compensating balances, overdrafts, restrictions on cash balances,		account numbers, and purpose of each account. 2. Verify that a separate general ledger account is maintained for each bank account and check that the general ledger accounts are properly labelled and identified. 3. Verify that the recording and presentation of bank accounts in the general ledger comply with relevant accounting standards and principles. 4. Ensure Compliance to all bank related restrictions.			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			etc.)					
Treasury Management	Recording of Bank Transactions-Authorization of payments	Adherence to authorisation process may not be verified effectively by the banks for accounts.	I - List of authorised signatories are available with the Accounts Officials. The same are configured in the banking Portal. Specimen signature cards are available with the finance department so as to verify the signatures of appropriate authority before making for payment. All the payments should be in compliance with statutory requirements.	Treasury Head	1. Evaluate the process for approving payments, including the appropriate authorization levels and documentation required for different payment types (for online payments, Cheque Payments). Check whether Host to Host based payment process has been implemented. 2. Evaluate controls in UPI Payments, Receipts like transaction Limits, Real-time Notifications, Transaction Reconciliation, etc.	Appropriate recording of Bank transactions	100%	1. Apply data analytics to detect potential fraudulent activities, such as unauthorized payments or unusual patterns in bank transactions. 2. Perform trend analysis to identify deviations from normal behaviour.
Treasury Management	Recording of Bank Transactions - Physical control over	Cheque instruments may be mishandled/mis-utilized.	I - Adequate control over inventory of cheques is maintained. All cheques are marked	Treasury Head	1. Evaluate the controls over physical cheques. 2. Ensure that only authorized	Control over Physical cheques	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
	cheques		as account payee. Further for all the banks, access to stock of unused cheques is controlled. The details of inventory of cheque (including unused cheques) is maintained in Excel Sheet/ records (control sheet).

II - As generally, the banking system sequentially allots cheque numbers, in order to cancel a cheque the same needs to be cancelled in the system which can be done only by designated person in Finance Department. Cancelled cheque are clearly | | personnel can write, sign, or handle checks. 3. Ensure that access controls to restrict access to cheque-writing software or tools has been implemented. 4. Ensure that account reconciliations are performed to ensure all issued cheques are properly recorded and accounted for. | | | |

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			marked and inventory of cancelled cheques maintained. In case a cheque gets misplaced, cheque is voided in the System and at the same time, a stop payment advice is sent to the bank concerned.					
Treasury Management	Recording of Bank Transactions - Appropriate Account	All receipts may not be correctly /timely accounted for (by the cut-off date).	The transactions to be conducted through each bank account should be adequately defined. (All capital receipts are deposited in corporate bank account and are utilized for specific purposes on immediate basis. All working capital receipts are deposited in division bank accounts.	Treasury Head	Scrutinize the transactions in each bank account and ensure that all capital receipts are deposited in corporate bank account and are utilized for specific purposes on immediate basis, all working capital receipts are deposited in division bank accounts. Verify whether payment accounts should be separate	Recording of Bank transaction on appropriate accounts	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			Payment accounts should be separate from collection accounts for better monitoring and control over funds).		from collection accounts.			
Treasury Management	**Recording of Bank Transactions - Stale cheques**	Stale cheques may not be reversed to show incorrect bank balance.	The stale cheques are reversed on monthly basis to a separate account termed as "Stale Cheques Payable Account" maintained for this purpose. No direct transfers to Party's Account is made. Amount lying in the "Stale Cheques Payable Account" which is three years old is transferred to the Party's Account.	Treasury Head	Verify whether the stale cheques are reversed in the separate account on a monthly basis.	Reversal of Stale cheques	100%	None
Treasury Manageme	**Estimation of Working**	All receipts may not be	Normal working	Treasury Head	Review the effectiveness	Estimation of	100%	1. Assess the accuracy of

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
nt	**capital Requirements**	correctly /timely accounted (by the cut-off date).	capital funds should be reviewed at the month end for accuracy and completeness. Periodic financial reports are reviewed by Management, with comparison to budgeted amounts or other financial data for reasonableness of cash and bank balances.		of the fund forecast preparation and review procedure. For sample month obtain the forecast and review the underlying assumptions and facts.	Working capital requirement		cash flow forecasts by comparing forecasted values with actual cash flows over a specified period. 2. Identify areas where forecasting accuracy can be improved, and explain deviations.
Treasury Management	**Bank Reconciliation**	Transactions may not be recorded either by mistake or intentionally.	Bank reconciliation is performed by person independent of banking transaction and accounting. (In cases where independent treasury operating systems are used, a three-way reconciliation is between bank	Treasury Head	For each BRS selected in the sample, ensure that: 1. The person responsible for reconciliation is not a cheque signing authority. 2. The person does not have cash handling responsibility. 3. The	BRS performed by Independent Person	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			statement, treasury system and the ledger balances).		person does not have bookkeeping responsibility. 4. Adequate maker-checker controls are in place.			
Treasury Management	**Bank Reconciliation**	Transactions may not be recorded either by mistake or intentionally.	Reconciliations between bank statements and general ledger are performed on a regular basis and reviewed & approved by management. Reconciling items are found and corrected as necessary.	Treasury Head	1. Review each BRS: a. For evidence of review by a person independent from person responsible for reconciliation. b. To ensure that the review was conducted on a timely basis. c. Check whether the date of preparation, date of review and date of approval are captured in the BRS. d. Ensure that resultant actions are documented (as minutes, or emails, etc.) and check whether	BRS prepared and reviewed for all bank accounts	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					these have resulted in the desired result (e.g. clearance of old items, rectification of errors/ omissions, etc.) e. For the type of reconciling items. Inquire in detail unusual items (E.g. Payments appearing in Bank Statement but not in the Bank Book, etc.) f. For 'Cheques Issued but Not Presented' check subsequent clearance of these, on a 100% basis. Be alert of any unusual trends/ occurrences (E.g. Large number of vendor cheques or employee cheques appearing as un-presented for unusually long periods,			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					High value vendor cheques appearing as un-presented for unusually long periods, etc.) g. For 'Cheques Deposited But Not Cleared' check subsequent clearance of these on a 100% basis. h. From the original Bank Statement of the subsequent month, pick up a sample of cheques that were cleared in the first 2-3 working days. Trace these back into the BRS of the previous month. These cheques should reasonably be appearing in the BRS as 'Cheques Issued But Not Presented'. i. Specifically inquire into reconciling			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					items that are over 60 days old. j. Review Bank Charges, if material. Ascertain if these are checked independently w.r.t. the agreement with Bankers or whether the entry is simply picked up from the BRS and effected in the Bank Book. 2. For all BRSs tested, reconcile the opening bank balance of the subsequent period with the closing balance of the period under audit. 3. Inquire regarding the procedures in place when the persons performing and/ or supervising the reconciliations are absent at their			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					workplace. Ensure that any substitute persons deployed are competent, compatible with their duties assigned duties and are fully aware of how the reconciliations are to be performed and supervised. 4. Out of the sample, select a few (To Be Agreed with Client and Engagement Manager/ Partner) BRS for a detailed verification. For such BRS, trace: a. The balance as per Bank Book with the Bank statement b. Each individual reconciling item into the underlying source record c. Check			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					arithmetical accuracy of each group of reconciling items as well as the BRS itself. 5. In cases where BRS has not been prepared due to opening and closing balances being the same, obtain Bank Statement for the entire audit period to ensure that there were no activities during the period. A good control practice is to prepare a formal BRS for such accounts as well. 6. Similarly, for accounts explained to be non-operative, check whether if a formal BRS was prepared. Further, obtain and review the			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					original Bank Statement for the entire audit period to ensure that there were no activities during the period. 7. For the bank accounts selected, ensure that Bank Statements are supported by bank's balance confirmations, else the bank balances/ statements should be verified online. Proofs of such online confirmations should be retained in the working papers. If none of the above two procedures are performed, this fact should be clearly stated as a limitation in the audit			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					report. 8. For all balances on deposit account(s), ensure that the original deposit certificates are supported by bank's balance confirmations, else the deposits should be verified online. Proofs of such online confirmations should be retained in the working papers. If none of the above two procedures are performed, this fact should be clearly stated as a limitation in the audit report. 9. For all balances on deposit account(s), check the: a. Due dates of payment of interest			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					b. Rate (simple or compounding) c. Calculations of 'Interest Accrued & Due' as well as 'Interest Accrued But Not Due' d. Ensure correct accounting thereof, including Tax Deducted at Source e. Ensure correct disclosure thereof. 10. Review the Bank Book with the Bank Statements for each bank account selected for any unusual entries (e.g. inter-bank transfers, cash deposits, etc.) for a period of 5 days before and 5 days after the 'cut-off' date, i.e. the period end. Specifically determine			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					that: a. Transfers between each bank were recorded in the same period, i.e., all transfers prior to the year-end were recorded in each ledger before the year end, and vice-versa for post year end transfers. b. Transfers not affected by banks within the same accounting period in which these were initiated, are properly reflected as reconciling items in the BRS. 11. Review the trend in balances with banks (on various accounts). In case the entity seems to be holding			
Treasury Manageme	**Petty Cash transactio**	Incompatibl e tasks may	Physical cash	Treasury Head	1. Review the controls for	Physical verificatio	100%	1. Perform initial data

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
nt	ns	be assigned (to the same individual) resulting in non-detection of errors and omissions	verification is conducted daily and physical verification sheets are signed by a person independent of the cashier. Surprise checks are made by Internal/ Statutory auditors.		Physical cash verification 2. Count undeclared petty cash and document it. a. From the above, make an assessment of the control of petty cash funds.	n of cash		exploration to understand transaction volume, frequency, and patterns over time. 2. Analyse frequency and amount of cash replenishments. Evaluate the need for optimization.
Treasury Management	Petty Cash transactions	Incorrect/ incomplete cash transactions may be recorded in the general ledger.	The cash ledger is reconciled with the general ledger. Discrepancies are found, corrected, and reprocessed as necessary on a timely basis. The reconciliations are reviewed and approved by appropriate management.	Treasury Head	Evaluate the procedure of reconciliation of the cash ledger with general ledger. Physically verify the cash balance, cash Ledger and General Ledger balance during the audit.	Reconciliation of cash ledger with general ledger	100%	None
Treasury Management	Petty Cash transactions	Unauthorised disbursements may be	I - Company has clearly defined levels of	Treasury Head	Determine the appropriateness of petty	Approval of Petty cash Transacti	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
		made.	authority for approving and/or executing different types of cash transactions. Monetary limits have been set for approval and execution of transactions by individual. II - Authorizations and monetary limits are regularly reviewed and updated as changes occur. All updates are communicated both internally and externally in a timely manner.		cash expenditures in accordance with company policies and procedures by Judgmentally selecting a sample of petty cash reimbursement vouchers. Check the following: 1. They have been properly executed. 2. The expenditures are appropriate. 3. The expenditure was approved by an authorized signatory.	on		
Treasury Management	**Fund Management**	Capital funds may be utilized for working capital requirements or vice versa	Application of long-term capital funds and short term working capital funds should be monitored	Treasury Head	1. Check the process of review of application of funds (Long term and short term) for the audit period. 2. Ensure	Application of Long-term Funds and Short term working capital funds.	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			periodically.		that the short-term Working capital requirement is met through short term working capital funds and long term capital requirement is done through long term capital fund.			
Treasury Management	Borrowings	Unauthorized debts are made in the company's name	Every borrowing should be approved as per the authorization matrix (and the approval limits).	Treasury Head	1. Obtain and review the organization's borrowing policies, procedures, and guidelines to understand the framework within which borrowings are made. 2. Review the borrowing authorization and approval process to ensure that it is in line with the organization's governance structure and clearly defines roles and responsibilities for borrowing	Authorization of Borrowings	100%	Key Performance Indicators (KPIs): 1. Set the KPIs to measure treasury performance, such as cash conversion cycle, return on investments, or debt ratios. 2. Monitor KPIs over time to identify trends and deviations.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					decisions. 3. For the borrowings of the company, check whether borrowing was approved as per the authority matrix.			
Treasury Management	**Borrowings**	Interest on borrowings or other transactions such as redemption, conversion of debt or accrual of interest may not be timely or accurately recorded.	Management reviews periodic financial reports, with comparisons to budgeted amounts or other financial data, for reasonableness of expenses associated with debt. Unusual variances are researched and corrected as necessary. Reviews could include: - Interest expense - Interest expense by debt facility, including effective rates	Treasury Head	1. Assess the organization's interest rate risk management strategies, including the use of hedging instruments, to mitigate exposure to interest rate fluctuations. 2. Ensure that the Management reviews reasonableness of expenses associated with debt.	Review of expenses associated with Debt	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			- Accrued interest payable.					
Treasury Management	**Borrowings**	Borrowing terms or obligations may not be adequately met resulting in liabilities severe then that accounted in normal course.	All borrowing restrictions are formally monitored and compliance assessed regularly by a cross section of management including legal, accounting and treasury personnel. Questions or grey areas may be escalated to outside legal counsel for additional consideration and advice.	Treasury Head	1. Verify that all borrowing agreements and related documentation are complete, accurate, and compliant with relevant laws and regulations. 2. Verify the organization's compliance with debt terms or, loan agreements, and other contractual obligations related to borrowings.	Compliance with Debt agreements.	100%	None
Treasury Management	**Investments**	Unauthorised personnel may execute investment transactions.	I – The company has a defined investment strategy converted into guidelines. These Investment Strategies Guidelines	Treasury Head	1. Obtain the investment strategy/guidelines/Standard operating procedure. Ensure that these are reviewed by the Board. 2. Understand the defined	Approved investment strategies / guideline	100%	Investment Performance Analysis: 1. Evaluate the performance of investment portfolios by analysing returns, yield calculations, and risk measures. 2. Compare

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			should be timely reviewed by the Board. II - The company has also clearly defined levels of authority and monetary limits for approving and/or executing different types of Investments. All investment trades are approved by authorized person only. Further, these monetary limits and guidelines should also be consistent with Companies Act requirements. (Section 185, Section 186 of the Companies Act, 2013, etc.) III -		levels of authority and monetary limits for approving and/or executing different types of Investments.			investment performance against benchmarks and industry standards.

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			Authorization and limits are regularly reviewed and updated as changes occur and communicated both internally and externally in a timely manner.					
Treasury Management	Investments	Unauthorised personnel may execute investment transactions.	The purchase of self-directed financial instruments, including but not limited to, stocks, bonds, notes, debentures, certificates of deposit, commercial paper or the local investment of excess cash requires the prior approval of the Corporate Treasurer. Investments initiated by the Corporate Treasurer	Treasury Head	Obtain the list of investments done during the audit period. Check whether these investments are approved by authorized persons.	Approval of investment as per defined procedures	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			are subject to the approval of the Chief Financial Officer.					
Treasury Management	Investments	Accounting (valuation) and disclosures as per applicable GAAP may not be made.	I - Management obtains mark-to-market valuations for trading and available for sale securities as per applicable GAAP. These valuations should be independent and readily verifiable. II - Management also reassess the appropriate classification for all debt and equity securities.	Treasury Head	1. Review the investments to ensure they are appropriately classified as per accounting standards (e.g., held-to-maturity, available-for-sale, or trading). 2. Confirm that the accounting treatment of investments complies with relevant accounting standards, such as Indian Accounting Standards (IND AS 109) or Generally Accepted Accounting Principles (GAAP). 3. Check for any reclassifications of investments and ensure they are supported by	Appropriate valuation and accounting of Investments	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					proper documentation and approvals.			
Treasury Management	**Writing of Instruments - Letter of Credit / Bank Guarantee/ Bills Payable**	The Bank Guarantee/ LC/ BP may be opened without proper authorisation	I - Bank Guarantee/ LC is opened by Appropriate Designated Authority after receiving approved requisition from respective dept. and the same is approved by authorised signatories. II - Standard LC terms is drafted in consultation with the legal department. Any deviation from the same is adequately vetted by legal. Expiry status is monitored by Appropriate Designated Authority.	Treasury Head	Before issuing the instruments, Verify that all instruments are issued and authorized by persons with the appropriate authority, as per the organization's delegation of authority policy. 2. Review the written instruments and ensure that they are complete and contain all required terms and conditions. 3. Validate the accuracy of details such as the beneficiary's name, amount, payment terms, and expiry date, etc. in the instruments. 4. The Bank Guarantee/ LC/ BP opened	Authorization of The Bank Guarantee/ LC/ BP	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					during the audit period. Very if the same was approved as per the defined guidelines.			
Treasury Management	**Insurance**	Insurance coverage may not be renewed or may be rendered inadequate	Guidelines for asset (value wise) and risk (type of insurance) coverage are laid out clearly. The responsibility for obtaining and managing the same is also clearly specified. Cost benefit analysis for not covering an asset should be prepared and reviewed by an appropriate management level.	Treasury Head	Ensure that Guidelines for insurance are formally laid down and are approved.	Guidelines for insurance	100%	None
Treasury Management	**Insurance**	Insurance coverage may not be renewed or may be rendered inadequate	The Insurance Manager reviews the list of assets (including Additions or Deletions of	Treasury Head	1. Review the organization's insurance policies. 2. Understand the terms, coverage limits,	Adequacy of Insurance, accuracy of premium, robustness in	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			Interest) periodically and updates the terms of insurance if required.		deductibles, exclusions, and other key provisions of each policy. 3. Examine insurance policy documents. 4. Ensure that policies are valid, up-to-date, and accurately reflect the organization's details and coverage. 5. Identify any gaps or areas of underinsurance that need to be addressed (based on the value insured vs actual value of the asset). 6. Verify that insurance premiums are accurate. 7. For any damages/loss verify that claims are reported promptly, and that supporting documentation is provided.	claims process		
Treasury Management	**Forex Management -**	Hedging strategy may not fully	I - Organization's overall	Treasury Head	1.Understand the Hedging Strategy:	Review of Hedging Strategies	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
	Hedging	offset the underlying exposure, resulting in ineffectiveness.	hedging strategy, including the objectives, types of risks being hedged (e.g., currency, interest rate, commodity), and the financial instruments used for hedging (e.g., derivatives, options, forwards) is clearly documented II - Organization's hedging policies, procedures, and guidelines are comprehensive, well-defined, and aligned with the organization's risk appetite and strategy.		Gain a thorough understanding of the organization's overall hedging strategy, including the objectives, types of risks being hedged (e.g., currency, interest rate, commodity), and the financial instruments used for hedging (e.g., derivatives, options, forwards). 2.Review Hedging Policies and Procedures: Examine the organization's hedging policies, procedures, and guidelines to ensure they are comprehensive, well-defined, and aligned with the organization's risk appetite and strategy.	, Policies and Procedures		

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					Note: Conducting an audit of forex hedging requires specialized knowledge and expertise in risk management, financial instruments, accounting, and regulatory requirements. Engaging professionals with experience in foreign exchange risk management and auditing can help to ensure the audit is thorough and effective.			
Treasury Management	**Forex Management - Hedging**	Risk of entering into an unauthorized forward contract, leading to additional financial commitments to other parties and resulting in additional foreign exchange	The Treasury Manager based on careful analysis of the market, decides upon the best course of action for the Company to limit loss on foreign exchange	Treasury Head	1. Review the documentation for hedging instruments and contracts to ensure they are properly executed, authorized, and in compliance with accounting and regulatory	Approval of Hedging transactions	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
		loss.	fluctuations. The Treasury Head authorizes the Booking Confirmation and forwards a copy to the Bank.		standards. 2. Evaluate the approval process for initiating hedges, including proper authorization levels and documentation of rationale. 3. Verify the accuracy of fair value measurements and accounting treatment of hedging instruments in accordance with accounting standards.			
Treasury Management	Forex Management - Hedging	Risk of inadequate review and analysis on profitability on account of forward contracts entered by the Company, leading to incorrect decision making and resulting in additional foreign exchange loss.	The Chief Financial Officer verifies the Profitability Workings against the Forward Contracts entered.	Chief Financial Officer	1.Review the process for communicating hedge-related information to relevant stakeholders, including senior management and the Board of Directors. Assess the clarity and accuracy of disclosures related to hedges in	Review of profitability of forward contracts	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					financial statements. 2. Examine the organization's process for periodically reviewing the effectiveness of hedges and making necessary adjustments based on changing circumstances.			
Treasury Management	Forex Management - MIS Reporting	Forex transactions and positions reported to management may not be accurate	Treasury managers regularly reports on its Forex risk management activities both within and outside of the Treasury managers organization. On a monthly basis, Treasury prepares and circulates a report that includes details on underlying exposure data by currency and exposure	Treasury Head	1. Examine the process for communicating foreign currency-related information to relevant stakeholders, including senior management and the Board of Directors. 2. Assess the clarity and accuracy of disclosures related to foreign currency transactions in financial statements. For the audit period, obtain the MIS reporting on	Reporting of Foreign Currency Transactions	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			type; net exposure position; hedge coverage levels vs targets and forecast accuracy/variance analysis. The report shall further be validated and used for forex accounting and disclosures.		Forex Transactions.			
Treasury Management	Forex Management - Reinstatement	Forex reinstatement may not be as per Accounting Standards	The accounting treatment of Forex Reinstatement should be done in compliance with Ind AS 21.	Treasury Head	1. For the transaction during the audit period, verify the accurate valuation of foreign currency transactions in accordance with applicable accounting standards. 2. Review the accounting treatment for foreign currency gains or losses and confirm compliance with reporting requirements.	Reinstatement of forex currency liability	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Treasury Management	**Forex Management - Compliance**	Mechanisms to ensure compliance may not be robust.	Compliance areas related to foreign currency transactions are adhered to supported with adequate documentation. Examples of common compliance considerations related to foreign currency: FEMA, Anti-Money Laundering (AML) and Know Your Customer (KYC), Taxation and Withholding, Customs and Trade Compliance, Transfer Pricing, Intellectual Property and Royalties, Data Privacy and Cross-Border Data Transfer, Export Controls and	Treasury Head	Gain understanding of the applicable forex compliance requirement for the entity. Ensure that all the applicable compliances are adhered.	Compliance to Forex related regulations	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			Sanctions etc. *Note: These requirements may vary based on the jurisdiction, industry, and specific circumstances of the organization.*					

Borrowings

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
Borrowings	Initialization	NA	NA	NA	1. Obtain the Standard Operating Procedures relating to borrowings. From the Trial Balance and the relevant GLS, identify the list of borrowing (Opening balances, new borrowings etc.) Understand the nature of the borrowings, such as the purpose, type (term loans, revolving credit, bonds, etc.), and terms and conditions (interest rates, maturity dates, repayment schedules, etc.).	Overview and Understanding of Borrowings	NA	1. Analyse borrowings to detect anomalies, unusual patterns, or unauthorized activities. 2. Identify outliers or discrepancies that may warrant further investigation. 3. Develop Key Performance Indicators (KPIs) to measure treasury performance, such as cash conversion cycle, return on investments, or debt ratios, etc.. 4. Monitor KPIs over time to

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
								identify trends and deviations. 5. Analyze interest expense trends over time to identify any significant fluctuations or deviations from expectations.
Borrowings	Borrowing Authorization and Approval	Unauthorized debts are made in the company's name	Every borrowing should be approved as per the authorization matrix (and the approval limits) There clear guidelines for the types and amounts of borrowings that require higher management approval.	Treasury Head	1. Obtain and review the organization's borrowing policies, procedures, and guidelines to understand the framework within which borrowings are conducted. 2. Review the borrowing authorization and approval process to ensure that it is in line with the organization's governance structure and clearly defines	Authorization of Borrowings	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			Approval levels for modification of existing borrowings are clearly laid down.		roles and responsibilities for borrowing decisions. 3. For the borrowings of the company check whether they were approved as per the authorization matrix			
Borrowings	Interest and Principal Payments	Interest on borrowings (or such other transactions as redemption, conversion of debt or accrual of interest) may not be timely or accurately recorded.	Management reviews periodic financial reports, with comparisons to budgeted amounts or other financial data, for reasonableness of expenses associated with debt. Unusual variances are researched and corrected	Treasury Head	1. Assess the organization's interest rate risk management strategies, including the use of hedging instruments, to mitigate exposure to interest rate fluctuations. 2. Ensure that the Management reviews reasonableness of expenses associated with debt 3.For the borrowings as on the date of the audit (or during the	Review of expenses associated with Debt	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			as necessary. Reviews could include: - Interest expense - Interest expense by debt facility, including effective rates - Accrued interest payable.		audit period) : i) check whether the interest and principal payments made in accordance with the terms of the loan agreements. ii) Check whether there is a process to reconcile interest and principal payments with loan agreements and amortization schedules. iii) Ensure that the accounting entries for interest expense and principal payments accurately recorded. iv) Check that the borrowings are accurately reflected on the balance sheet, including their current and			

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
					long-term portions v) Ensure that borrowing transactions properly documented, including contracts, agreements, and amendments. vi) Evaluate the accuracy and completeness of borrowing-related expenses, such as arrangement fees, legal fees etc. and the capitalization and amortization of the same.			
Borrowings	Loan Agreement Compliance	Borrowing covenants may not be adequately met resulting in liabilities severe then that accounted in normal course	All covenant restrictions are formally monitored, and compliance is assessed regularly	Treasury Head	1. Ensure that the loan agreements reviewed to ensure that the terms and conditions are accurately reflected in the organization's financial	Compliance with Debt Covenants	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			by a cross section of management including legal, accounting and treasury personnel. Questions or grey areas are escalated to legal counselor for additional consideration and advice.		records. 2. Check whether the covenants, terms, and restrictions outlined in the loan agreements are being monitored to ensure compliance 3. Ensure that there is a process to notify relevant parties in case of potential covenant breaches.			
Borrowings	Segregation of Duties	Lack of segregation of duties over key cash/funds activities.	Segregation of duties is enforced through organisational structures, user access in the treasury/payment systems and procedura	Treasury Head	1. Ensure that adequate segregation of duties maintained between individuals responsible for initiating, authorizing, and recording borrowing transactions	Segregation of Duties in Borrowings	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
			l documents. There should be an effective segregation of key duties including dealing, settlement, and accounting/reconciliation. These segregations need to be further strengthened if the treasurer executes transactions. This segregation is reinforced through procedures documentation and position descriptions					
Borrowin	Compliance	Whether the	To ensure	Board of	Review of the	Compliance	100%	None

Final	Sub-process	Risk Description	Control	Control Owner	Test Performed	Attributes tested	Sample size	Data analytics performed
gs		Company's Board of Directors have approved the loan limit?	that the funds are borrowed by specific authority and for specific purpose.	Directors	Minutes of the Meeting of the Board of Directors.	with Debt Covenants		

Direct and Indirect Taxation & GST

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
Direct Taxation	Related Party Transaction	Payment to related party may not be at arm's length price	Defined process for approval of related party payment that includes the following: - technical and commercial evaluation by cross functional teams - approving authority, - justification for transaction with single party such as special qualification, achievement or experience. <	1. Check the approval for payment to related party and supporting documents thereof. 2. Check approval for commercial evaluation and supporting documents thereof. 3. Check justification for exceptions, if any, approval from the Board / Members, as required by regulations including Companies Act 2013 and SEBI.	1. Approvals for evaluations, 2. Supporting for evaluations	All related parties	1. Payment to Related Party vis-à-vis non-related party 2. Excess payment without any special qualification, achievement or experience.	Whether the unit has incurred any expenditure to a person specified in Clause (b) of Section 40A(2) of Income Tax Act, 1961. Verify whether they are reasonable and not excessive having regard to fair market value of such goods/ services/ facilities.
Direct Taxation	Cash Payment	Payment to vendors in cash	Payment in cash shall be prohibited or minimized	1. Check the Cash Ledger for payments made 2. Check	1. Approvals for cash payment	All the cash payments	Data Analytics to be done on all expenses including cash book	Whether the unit has made any cash payments against expenses above Rs. 10,000 (or Rs. 35,000 for

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
				that cash payment is authorised 3. Verify cash payment is not exceeding the limits			to ensure compliance. Data analysis needs to be done to ensure the payments are not split in a manner that this can contravene the provisions.	goods carriages) in contravention of Section 40A (3)/ 3A of Income Tax Act, 1961, i.e., payment otherwise than through account payee cheque or account payee bank draft
Direct Taxation	Payment within due dates	Payment may not be made within due dates	There shall be system for payment in timely manner	1. Check the due dates for various payments 2. Check whether the payment is made within the due date.	1. Supporting documents 2. Approvals	All such payments	Check the 'Due Date of payment' vs. 'actual date of payment'.	Whether the unit has certain payables in the form of tax, duty, cess or fees, employer contribution to provident fund and other funds, bonus, interest or loan and borrowings from banks and public financial institutions, etc. Verify whether such payments have actually been made on or before the due date of filing of Income Tax Return otherwise the same will be disallowed under Section 43B of Income Tax Act, 1961.
Direct Taxation	Repayment of loans/ advances/	Payment may be made in	Such payment shall not be	1. Check the cash Ledger for	1. Approvals for cash	All such payments	Data Analytics to be done on	Whether the unit has repaid loans/ advances/

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
	deposits	cash	made in cash	payments made 2. Check that cash payment is authorised 3. Verify cash payment is not exceeding the limits.	payment		all expenses including cash book to ensure compliance. Data analysis needs to be done to ensure the payments are not split in a manner that this can contravene the provisions.	deposits in cash of Rs. 20,000 and above in contravention of Section 269T of Income Tax Act, 1961.
Direct Taxation	Receipt of loans/ advances/ deposits	Receipt may be taken in cash	Such receipt shall not be accepted in cash	1. Check the cash Ledger for payments received. 2. Check that cash receipt is authorised. 3. Verify cash receipt is not exceeding the limits.	1. Approvals for cash receipt	All such receipt	Data Analytics to be done on all expenses including cash book to ensure the compliance. Data analytics to be done to ensure the payments are not split in a manner that this can contravene the provisions.	Whether the unit has received loans/ advances/ deposits in cash of Rs. 20,000 and above in contravention of Section 269SS of Income Tax Act, 1961.
Direct Taxation	Furnishing of PAN by vendors	PAN may not be given or may be incorrect.	Take the self-attested copy of PAN card	Check the PAN of vendor in the system with the copy of PAN Card.	PAN card copy of the vendors	30 vendor's PAN		Verify whether the compliance of Section 206AA of Income Tax Act, 1961 has been made with regards to furnishing of

533

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								PAN.
Direct Taxation	TDS related matters	TDS related non compliances	Timely compliance	1. Check that TDS is deducted as per appropriate rates 2. Check that payment of TDS is paid on time. 3. Check TDS return is submitted on time. 4. Check TDS certificates issued to the vendors on time.	1. Supporting documents 2. Approvals	Any 4 months	To analyse all the expense accounts / payments data to ensure TDS provisions have been correctly applied.	Verify the compliance of issues relating to TDS on salary, rent, commission, interest, payment to contractor, payment of fees to professional/ technical person, sales of goods etc. and observe the following: o Deduction of TDS at correct rate. o Deduction and Deposit of TDS within time. o Filing of TDS return in time and as per procedure prescribed. o Issue of TDS certificate. o Receipt of Form 15G/ 15H and entry in system. o Filing of Form 15G/ 15H with Income Tax Department as per Rule 29C of Income Tax Rules, 1962.
Direct Taxation	TCS related matters	TCS related non-compliance	Timely compliance	1. Check that TCS is collected as per appropriate rates 2. Check that payment of	1. Supporting documents 2. Approvals	Any 4 months	To analyse receipt accounts / data to ensure TCS provisions have been correctly applied.	Verify whether Tax Collected at Source (TCS) at the prescribed rates on sale consideration of Alcoholic Liquor, Tendu leaves, Timber, forest

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
				TCS is paid on time 3. Check TCS return is submitted on time. 4. Check TCS certificates issued to the vendors on time.				produce, scrap, minerals, parking lot, toll plaza, mining and quarrying, motor car, foreign currency, overseas tour package, goods are collected as per section 206C and observe the following: o Collection of TCS at correct rate. o Collection and Deposit of TCS within time. o Filing of TCS return in time and as per procedure prescribed. o Issue of TCS certificate.
Indirect Taxation	Registration	Registration related non-compliance	Proper Compliance	Check registration compliance as per law	Registration Certificates	All certificates		(1) Whether the entity has registration certificates for the principal place and separate registrations for all other places. Ensure that simultaneous registration under CGST/ SGST/ IGST is taken in the same state and places of business in other states. PAN based registration is compulsory except for non-residents.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								(2) Whether the details of business are correctly and completely mentioned/ declared in the Registration Certificate. (3) Whether the principal place of business has been correctly declared in the Registration Certificate and all places of business in other states in the respective Registration Certificates. (4) Whether all the products, traded/ manufactured have been declared in the Registration certificates
Indirect Taxation	Issue of Invoice	Issue of invoice not as per law	Proper issue of Invoice	Check process of issue of invoice	PO, Invoices and agreements	50 invoices		(1) Ensure that time of supply of goods shall be earlier of: - Date of issue of invoice by the supplier - due date for issue of invoice by the supplier, - date on which payment to be entered in books of supplier and date on which payment is credited in the

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								bank account of supplier. (2) Whether invoice or bill is not issued without supply of goods and/ or services. (3) Whether invoice or bill is not issued without supply of goods and/ or services. (4) Whether taxable goods are transported with the E Way Bill along with invoice/delivery challan, etc. (5) Whether invoice is raised under E Invoicing system if turnover in a year exceeds 5 crores. (6) Whether Letter of Undertaking is filed for export without payment of duty. (7) Whether original invoice is available in case of cancelled invoice (8) Whether receipt voucher is issued to the customers in case of advance received against services and GST is paid on the same.

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								(9) Whether payment voucher is issued to the vendors in case of services or goods covered under RCM. (10) CGST & SGST or IGST is charged as per the Place of Supply Provisions on the invoice. (11) Whether invoice has been signed by the authorised person.
Indirect Taxation	GST Returns	Filing of incorrect GST returns	Proper filing of GST Returns	Check GST Returns	GST Returns	All returns		(1) Whether all Monthly Returns/ Quarterly/ Annual Return have been filed with all Annexure within the prescribed time or within the extended period as per Form GSTR-1 to Form GSTR-11 as prescribed under Return Rules (Proposed). Tally it with both the monthly payments and as well as the ledger entries of the relevant dates. (2) Review the return and check whether the return is accurate as to input credit, output tax payable,

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								valuation of goods and carry forward of credit, etc. (3) whether the returns filed are complete and accurate in all respect and has been validated by other person.
Indirect Taxation	Valuation and Rates	Incorrect rate of GST or valuation	GST is charged on correct value and as per proper rates	Check Invoices to ensure correct rates and valuation	Invoices	50 invoices	to check system level controls on using the rates and modification.	(1) Whether GST (Goods and Service Tax) has been charged on sale of goods traded/ manufactured at correct rates. (2) Whether GST has been charged on sale of waste product/ discarded product/ assets at correct rates. (3) Whether GST has been charged on sale of fixed assets at correct rates. (4) If the rates applied are different, take a copy of the authority/ notification under which such change is approved. For example: Composition Scheme, GST Notifications, etc. (5) Log of changes in the

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								system relating to rates, application, etc.
Indirect Taxation	Books of accounts	Records as per GST law may not be maintained.	Proper records are maintained	Check the books of accounts	Books of Accounts			(1) Whether all the records and Books of Accounts, required to be maintained, are available at the location. (2) Whether books of account and other documents are kept, maintained and retained in accordance with the provisions of this Act
Indirect Taxation	Input Tax Credit (ITC)	Avail and utilize in eligible ITC	Only eligible ITC is taken with proper documents.	Check ITC invoices	Invoices	10-50 invoices p.m.		(1) Whether the unit has purchased goods only from the registered dealer. GST registration number should be there on invoices and Tax Invoices must be in prescribed format as per the Invoice Rules. (2) Whether full credit of GST is availed till date, that is input credit of GST for all the purchases is available in the electronic credit ledger. (3) Whether GST credit is correctly carried forward

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								from previous month to next month in every Monthly Return as well as Annual Return. (4) Whether ITC is correctly claimed on input and capital purchases eligible for claiming input credit, i.e., whether the input tax carried is in books only based on proper Tax Invoice from the vendor with GST Number and all other relevant details mentioned on the invoice. (5) Whether Input tax credit taken and/ or utilized is against actual receipt of goods and/ or services (6) Whether ITC is reversed on goods distributed as free samples / gifts / goods lost / stolen / destroyed / written-off / donations made etc (7) ITC is availed as per conditions mentioned in Section 16 of the CGST Act and rules thereof. Also, the same shall be cross-

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								checked with GSTR-2B & GSTR-2A. (8) Blocked ITC as per Section 17 (5) of the CGST Act, 2017 shall not be availed.to check system level controls on maintaining vendor master, system level controls in ensuring programing on whether input credit can be taken or not etc., should also be checked.
Indirect Taxation	Payment within due dates	Payment of GST not on time	Payment of GST on time	Check Challans	Challan	All challans		(1) Whether the unit has reconciled the variance between GST payable as shown in books of accounts and the amount paid. Variances should be documented and corrective action to be taken. (2) Whether the unit maintains acknowledged Tax challan and deposit of CGST, SGST and IGST is made under the correct head of account. (3) Whether the unit deposits GST (CGST/ SGST/

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								IGST) dues within due dates under properly filled challan/ Bank Transfer with proper acknowledgement and check that the amount appears on Electronic Credit Ledger. (4) Ensure GST payment would become due, earliest of conditions mentioned: (i) receipt of advance (ii) issuance of invoice (iii) completion of supply. (5) Ensure that CGST/ SGST/ IGST payment is paid by 20th of the succeeding month on monthly basis for taxpayers and on quarterly basis for composition tax payer. (6) Whether amount collected as tax erroneously in contravention to the provisions of this Act is due to the credit of the appropriate Government, (7) Whether the

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed	Process Metrics
								compliance of tax to be paid under reverse charge mechanism is done,

Corporate Social Responsibility

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
CSR	CSR Committee	Non-compliance with provisions of Companies Act, 2013	CSR committee is constituted as per Companies Act	1. Ensure that constitution of CSR Committee as per Companies Act, 2023. 2. All the policies and projects undertaken are passed through CSR Committee. 3. Check that Certificate issued by CFO relating to CSR Expenditure for the year.	1. Minutes of CSR Committee Meeting. 2. Approval on CSR Policy of Company. 3. Approval on projects undertaken. 4. CFO Certificate for CSR.	100%	NA
	CSR Projects	Projects undertaken under partnership with NGO's or other CSR Groups may leads to misutilisation of funds.	Independent practitioners report is obtained. Credentials of all CSR Partners are checked. Utilisation certificate is obtained from NGO.	1. Check whether Independent Practitioner's Report on such partners is obtained as per law. 2. Check the credentials of all CSR Partners - whether the activity being carried out by them is permissible	1. Independent Practitioner's Report of all partners. 2. Detailed study on background of every CSR Partner. 3. News related to every CSR partner in previous years. 4. Utilisation certificate	100%	NA

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				under the CSR Act, does the NGO have a registration certificate, do they offer income tax exemptions, do they have audited financial statements, are they having enough experience to handle the proposed projects, are they on panel with any national CSR hub, are they eligible to carry out the proposed CSR activities, or do they have any achievements or awards to their credit. 3. Check the persons on board of such CSR Partner and their credibility. 4. Ensure that the respective CSR Partner does not have any past black	obtained from NGO		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
				image or relation to any scandal. 5. Check whether utilisation certificate is obtained from NGO on regular basis and also check for authenticity of the certificate.			
		Projects undertaken are as described under Schedule VII and are eligible for CSR expenditure, if not may lead to disallowance and penalty	Projects are selected from the list given in schedule VII of Companies Act	Ensure that all the projects going on for a Financial Year are as per projects described in Schedule VII of Companies Act.	Check projects and match them to projects mentioned under Schedule VII of companies act	100%	NA
		Projects undertaken are not related to business	Projects are selected from the list given in schedule VII of Companies Act	Check the nature of projects undertaken and see if this is related to business activity	Check projects and match them to projects mentioned under Schedule VII of companies act and also check whether these are in any ways related to	100%	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
					business activity		
		CSR Projects undertaken are not controversial which can offend some consumers and lad to criticizing of company	Projects are selected after adequate due diligence	Check for Controversies to any project is aimed around it's target areas which can be checked through CSR Project Reports.	Project reports of all projects.	100%	NA
	CSR Expenditure	All the expenditure done is valid and not leads to wrong payment.	All the expenses are approved by CSR committee. Adequate supporting documents are attached with invoices.	Check supporting of all the payments with their bank payment proofs, approvals and beneficiary names. Check sample invoices in details along with all approvals and supporting to ensure authenticity of expenses.	Bank Statements of CSR, Beneficiary ID of every CSR Project, Invoice Supporting.	50%	NA
		Expenditure done on CSR is in excess to requirement of Law which could have been spent	CSR expenses are closely monitored by CSR committee.	Compare the actual amount spent on CSR to amount required to be spent as per law and define a deviation level	Financials of the Company	100%	NA

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		on profitable opportunities, more employees, research, technology, etc., an opportunity cost. **OR** Expenditure done on CSR is less in comparison to amount to be spent on CSR as per law which may lead to penalties in future.		to save opportunity cost of company.			
	CSR Unspent Amount	Delay in transferring of unspent amount to Prescribed fund under Schedule VII may lead to Consequences as per law.	CSR funds utilisation is closely monitored by CSR committee	Check bank statement and see whether unspent amount if any is transferred to prescribed fund within the defined timelines	Bank Statement.	100%	NA
	CSR Accounting	Tax Implications of CSR Expenditure which can affect	CSR accounting is done by persons having adequate knowledge and same is	1. Ensure that Expenses under donation are not claimed as CSR Expenditure. 2. Ensure that	Income Tax Computation and Financials	100%	NA

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		Income Tax payment.	reviewed by head F&A	Expenses done under CSR Expenditure are not taken as deduction while computing Income Tax under Sec 80G. 3. Check that CSR Expenditure is reversed while computing taxable income.			
	Assessment/ Survey Reprot on Effectiveness	Benefits are not reaching to the target audience.	Third party/in - house assessment/ survey is done on regular basis to take feedback on the project	1. Take report of assessment/survey done and see if there is any adverse finding and action taken on the same	Assessment/survey report	100%	NA

Human Resources – Hire to Retire

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
Hiring	Staff Planning	Risk of not planning the need for staff or staff movement, which later could be a bottleneck in the operations. Risk of hiring a greater number of resources than required or not hiring adequate resources.	The Company should plan for the resource requirements at the beginning of the year and have a strategy accordingly.	Whether the Company has planned for the resource requirements in consultation with HR and relevant operations team.	Planning	100%	
Hiring	Staff Planning	Risk of creating positions or designations which are not approved.	HR Head should approve any position or designations as per organisation hierarchy and also the job descriptions. Where new positions are created to ensure the organisation hierarchy and job description is amended or incorporated, as the case may be, it should be duly approved.	Review of how the new positions is created or amended.	Creating new job positions.	100%	
Hiring	Communication on Need of	Risk of not communication	The HR Head should have a	Whether there is a strategy in	Communication	100%	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
	Resources.	through the right channels to ensure that the need for the resources is adequately publicised.	strategy on whether to go for campus interviews (freshers), internal references, web portals, social media or HR consultants to communicate the need for the resources.	place to communicate the need for the resources.			
Recruitment	Short-listing Candidates	Risk of not selecting the right candidates for interview.	Ensuring that the short-listed candidates meet the criteria of job description and qualifications.	Review of the process of short-listing candidates.	Process of short-listing	Sample	
Recruitment	Interview	Risk of hiring candidates without assessing their skill sets.	Company should interview the candidates before hiring. The interview could be a single interview or multiple rounds depending on the need which also includes (a) academic / technical (b) Personal round etc.,	Whether interviews are being conducted and documented with the results. Typically, the Company should have a standard checklist to rate (a) communication (b) punctuality (c.) dress code (d) academic qualification etc., and note down the results of interview.	Documentation of interview.	Sample	
Recruitment	Selecting the	Risk of hiring candidates	Company should ensure that for	Process of selecting the	Process of selecting	Sample	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
	candidate	without assessing their skill sets.	key positions say Manager and above, the selection is carried out by at least 2 staff to ensure there is agreement on the candidate's suitability.	candidates.	candidate.		
Recruitment	Fixing Remuneration	Risk of agreeing to a remuneration not commensurate to the job or skill set.	Company should have a standard policy on remuneration to be paid for each designation. Unless it is an exceptional case where the management decides for higher remuneration due to lack of resources/skill set in the market, or talent exhibited by the candidate etc.,	Fixing remuneration to the candidates.	Remuneration	Sample	
Master Document	Master Documentation	Risk of details of employees not available in a singular place leading to risk of using incorrect data for payroll and other calculations.	All employee related details should be maintained in a system (software / application) or in hard copy files for each employee. The file should contain (a) Employee CV / Resume (b) Interview Result (c.) Copy of appointment letter	Review of the personal files of the employee and ensuring its completeness.	Completeness of Documentation.	Sample	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			(d) Statutory details like nomination for gratuity and provident fund (e) Acknowledgement by the employee on Code of Conduct (f) Tax details etc.,				
Performance Review	Monitoring	Risk of not monitoring whether the employee is working up to the expected standards. Low performance would impact productivity.	Company should do an annual performance review (may be half-yearly also if required). The Head of the Department and the immediate manager should review the performance with the key performance indicators and give feedback on improvement.	Review of how the performance is reviewed and how KPI's are given to the staff.	Performance Review.	Sample	
Training	Training and Upskilling	Risk of employees not knowing how to work with new technology or new skills would lead to Company delivering a lower quality service / good and could be 'out of market'.	Company should ensure there is a training calendar prepared and they recruit either internal consultants or external consultants /experts to train staff on different domain.	Review of training schedule, attendance, appointment of experts, feedback received, inclusion of seeing whether the training has helped in achieving KPI etc.,	Training.	Sample	

554

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
Disciplinary Action	Ensuring compliance with Code of Ethics and Policies.	Risk of employees not knowing how to work with new technology or new skills would lead to Company delivering a lower quality service / good and could be 'out of market'.	Company should have a policy on action to be taken for violation of Code of Ethics and non-compliance with Company's policies / procedures.	Review of how the Company has ensured compliance with Code of Ethics and Company's policies and procedures including review of how the disciplinary cases are handled.	Disciplinary Action being taken.	Sample	
Promotion	Promoting the right candidate	Risk of employee not being promoted as per the Company's policy / practice / judgement of the management leading to dissatisfaction of employee leading to lower productivity.	Company should have a policy on circumstances when an employee gets promoted and what are parameters to be considered.	Review of the promotion process and whether the management has reviewed the skill set, knowledge level, experience, and performance of the employee in past before promotion is given. If it is a management discretion, the same needs to be documented.	Process of promoting employee.	Sample	
Increments	Changes in remuneration.	Risk of employee not giving increments as per the Company's policy /	Company should have a policy on circumstances when an employee gets increments and what are	Review of the increment process and whether the management has reviewed the skill set,	Process of giving increments to employee.		

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
		practice / judgement of the management leading to dissatisfaction of employee leading to lower productivity.	parameters to be considered.	knowledge level, experience and performance of the employee in past before increment is given. If it is a management discretion, the same needs to be documented.			
Full and Final Settlement	Termination formalities.	Risk of not paying the employees dues like Gratuity, Leave Encashment etc., or incorrect payment to the employees.	All Full and Final settlement should be calculated by HR and reviewed by another staff (Accounts Department). Further, the Company should ensure that all the departments concerne provided 'no objection' including IT (for laptops / cell phones / internet connections), Administration (to deactivate physical access), Payroll (to ensure all loans are recovered and there are no payables), etc.,	Review of the full and final settlement process and ensure that all the dues are paid within the statutory guidelines / company's policies.	Review of settling employee dues.	100%	

Human Resources – Payroll Management

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
Payroll Calculation	Attendance recording	Risk of remunerating an employee without ensuring attendance to work.	The presence of an employee in the office should be monitored through an attendance management system either bio-metric or face recognition or manual signature record, as required by law / company's policy. Any late comings to the Office should be explained by the employee and the Head of the Department / Manager should approve the same. If there are continuous late comings, there has to be a policy on the action to be taken i.e., fixed amount to be deducted	Review of the attendance system and also review whether the software / hardware systems are working as specified or desired.	Attendance	Sample basis depending on the number of employees, industry etc.,	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			from salary or leave to be deducted, etc.				
Payroll Calculation	Leave Management	Risk of granting leaves to employee which is not as per Company's policy or without approval.	Company should have a policy for leaves including casual leave, medical or sick leave, maternity and paternity leave, emergency leave, etc. Based on the policy the leave applied by the employee should be approved by the designated authority.	Whether the leave credit and utilisation is as per company's policy.	Compliance with the Policy.	Sample basis depending on the number of employees, industry etc.,	
Payroll Calculation	Payroll Processing	Risk of processing payroll with incorrect input data.	1. The input data provided by the HR to the payroll includes: (a) Attendance (b) leave details (c.) specific additions/ deletions (d) Changes in master file, etc. Payroll department would process the salaries	1. Payroll details to be traced to the master/ personal file of each employee to ensure that the payroll processing is accurate. 2. Review of head count reconciliation and variance of payroll.	Accuracy and completeness of payroll processing.	100%	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			based on the updated employee master data including any information provided by HR accordingly. 2. Analytical procedure of Head Count to be done to ensure that the difference between last month's payroll and current month's payroll is explained.				
Payroll Calculation	Payroll disbursement	Risk of payroll being disbursed to the wrong person. Risk of Fraud of disbursing payroll to a wrong bank account.	Company should ensure that all the payroll disbursement is through banking channels only. The payroll statement prepared by the payroll department should be reviewed by the Accounts department and then send a list containing list of employees and payment	Review of the payroll processing including the process of transfer of files between departments and ensuring maker-checker concept is effective.	Operating effectiveness of payroll. Processing	100%	

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			to be made to the treasury team. The treasury team should disburse the payroll based on the authorisation matrix given to the bank.				
Payroll Calculation	Payroll disbursement	Risk of incorrect statutory deductions	Company should ensure that the statutory deductions are deducted and remitted to the designated authority of the Government within the timeline stipulated by law.	Review of compliance of (a) Accuracy of deductions (b) Punctuality of making remittances to the Government.	Compliance with Labour Laws	100%	
Payroll Calculation	Payroll disbursement	Risk of non-deduction of loan amount given to employee	Company should ensure that any loan given to employee is deducted from the payroll as per the sanction terms.	Recovery of loans given to employees is as per the Company's policy.	Compliance with Company's policies.	100%	
Payroll Function Outsourced	Outsourcing of Payroll Function	Risk of third-party service provider not being able to render the service as desired.	Company should do due diligence of the vendor before selecting for outsourcing payroll	Review of the vendor onboarding procedure and due diligence on the quality of the service	Due Diligence	100%	

560

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested	Sample size	Data analytics performed
			processing.	that the vendor renders.			
Payroll Function Outsourced	Internal Controls at third party vendor location.	Risk of third-party service provider not being able to render the service as desired.	Company should ensure (as part of contract) that the service provider's internal controls are subjected to independent audit and such audit report is made available for review by the company.	Review of the independent auditor's report on the internal control exists in the service organisation.	Review of Audit Report and observing for discrepancies.	100%	

Foreign Currency Transactions

Process	Sub-process	Risk Description	Control	Test Performed	Attributes tested
Foreign Currency Transactions	Transaction Risk	Cost effective method is not used for payment of duty. Ineffective foreign currency risk management system.	The method of payment of import duty is selected after due diligence so that the risk may be mitigated and can implement hedging strategies. Eligibility for Merchandise Exports from India Scheme (MEIS) can be explored.	Check whether payment is made in accordance with guidelines prescribed by the Company. If not, then check the payment mode in sample contracts and compare the cost of undertaking Foreign Currency Transaction.	FCT Contracts and Policy
		Currency hedging is not done.	Hedging is done on the basis t of current market trend and outlook of market.	Check hedging terms and conditions are satisfied while making payment.	Hedging document for each contract, Supporting of Actual payment and rates thereof.
		Booking rate is higher than the current Spot Rate	Regular monitoring of terminal and cross checking of rates before booking is done. -To obtain rates from bank and make comparison between rates offered by different bankers.	Compare spot rate with rate of booking and Check, if any, deviation.	Booking rate
		Excess payout due to currency fluctuation.	Close monitoring is done on payout.	Check whether any change in foreign currency rate is immediately updated in ERP.	ERP date along with Foreign Currently fluctuation details
	Transaction Risk	Adequate terms not mentioned in export contract.	During export, payment terms may include credit terms with rates	Review of export contract and check whether companies'	Export contracts

		which mitigates the adverse effect of change in forex rates due to time delay in execution of transaction and receipt of payment. <	interest is adequately protected.	
	Adequate due diligence is not done for export parties	Parties with which transactions are undertaken should have credibility in market so that payment is not defaulted.	Check credit rating of a company on Crisil or with any other credit agency.	Crisil database or reports of company from respective credit agency.
	Translation Risk	Non-compliance with provision of Ind AS	In preparation of consolidated Financial Statement, there is a risk of translation of Financial Statements of subsidiaries in currency of holding company.	Check Financial Statement conversion with Ind AS 21.	Ind AS 21 and Financial Statement of foreign subsidiary as consolidated.