Guide on Risk Based Internal Audit Plan

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).

Internal Audit Standards Board
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Edition	:	February, 2015
Committee/Department	:	Internal Audit Standards Board
Email	:	cia@icai.in
Website	:	www.icai.org
Price	:	₹ 250/- (*Including CD*)
ISBN No.	:	978-81-8441-776-0
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110 002.
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra 282 003 February/2015/P1761 (New)

Foreword

Recent economic events and increased regulatory scrutiny have impacted the importance of understanding and managing the risks, which drive uncertainty about the organizational success. Effective risk management helps organizations to understand the risks they are exposed to, put controls in place to counter threats, and also to effectively pursue their objectives. In a nutshell, risk management is an important aspect of an organization's governance, management and operations.

In such a scenario, internal audit plays a very critical role by providing assurance that all the risks related to the activities of the organization are being identified, monitored and managed effectively. The Institute, from time to time, has issued guidance to help the members enhance their skill base and competencies in the area of risk management. This "Guide on Risk based Internal Audit Plan" is being issued by the Internal Audit Standards Board of the Institute of Chartered Accountants of India (ICAI) to provide guidance on developing and implementing an effective Risk Based Internal Audit Plan.

I would like to congratulate CA. Charanjot Singh Nanda, Chairman, Internal Audit Standards Board and all the other members of the Board on issuance of this publication which provides updated guidance on this important area. The objective is to help internal auditors in embedding risk based approach thereby enabling them to meet stakeholder's expectations.

I am confident that this Guide would help our members to play a leading role in promoting good risk management practices.

February, 2, 2015
New Delhi

CA. K Raghu
President, ICAI

Preface

In today's complex regulatory and compliance environment, while capitalizing on emerging opportunities, risk management assumes tremendous importance. Risk management systems encompass the policies, culture, processes, systems and other aspects of an organization that, taken together facilitate its effective and efficient operation by enabling it to assess current and emerging risks, respond appropriately to risks and significant control failures and to safeguard it's assets. Assessment of risks should support better decision-taking, ensure that the board and management respond promptly to risks when they arise, and ensure that shareholders and other stakeholders are well informed about the principal risks and prospects of the organization. Internal auditors undoubtedly play a leading role in helping their organizations achieve an integrated, organization-wide approach to risk management which ultimately helps to create, enhance, and protect stakeholder value.

Considering the above, the Internal Audit Standards Board of the Institute is issuing this "Guide on Risk Based Internal Audit Plan". Accordingly, the Board is withdrawing its pervious publication "Guide to Implementing Enterprise Risk Management" issued in 2008. Internal auditors can through risk based auditing provide feedback on the adequacy of internal control as well as they can provide a source of information for monitoring risk. Further, the cycle of continually assessing risk, efficiently planning audit activities, and effectively performing, delivering, and reporting audit activities can result in overall lower risk to the organization. This Guide comprehensively explains the concepts of Risk Based Internal Audit Plan and provides a step-wise approach to effectively implement the same in an organization. It includes detailed guidance on risk appetite, understanding business environment, preparing audit universe, risk identification, risk prioritization and rating, assessing control environment, deriving residual risk rating and finally developing internal audit plan. Further, for enhancing the understanding of the readers, an illustrative case study including all the steps to prepare the RBIAP has also been also provided in the guide.

At this juncture, I would like to place on record my sincere gratitude to CA. Amit Gupta, CA. Mohit Gupta, Shri Anurag Agarwal and CA. Sameer Mittal for sharing their experience and knowledge with us and preparing the draft of this Guide.

I would like to express my immense gratitude to CA. K. Raghu, President, ICAI and CA. Manoj Fadnis, 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. Shriniwas Y. Joshi, Vice Chairman, IASB, CA. Rajkumar S. Adukia, CA. Prafulla Premsukh Chhajed, CA. Sanjeev K. Maheshwari, CA. Dhinal Ashvinbhai Shah, CA. Shiwaji Bhikaji Zaware, CA. V. Murali, CA. S. Santhanakrishnan, CA. Abhijit Bandyopadhyay, CA. Sanjiv Kumar Chaudhary, CA. Atul Kumar Gupta, CA. Naveen N.D. Gupta, Shri Manoj Kumar, Shri P. Sesh Kumar and Shri R.K. Jain for their vision and support. I also wish to place on record my gratitude for the co-opted members on the Board, *viz.*, CA. R. Balakrishnan, CA. N. S. Ayyanagoudar, CA. Sunil H. Talati, CA. J. Vedantha Ramanujam and CA. Milind Vijayvargia and special invitees, CA. Nagesh D. Pinge and CA. Hardik Chokshi for their invaluable guidance as also their dedication and support to various initiatives of the Board. I also wish to express my thanks to CA. Jyoti Singh, Secretary, Internal Audit Standards Board and her team of officers for their efforts and inputs in finalizing this Guide.

I am sure that the members and other interested users will find this publication useful in discharge of their professional obligations.

February 9, 2015
New Delhi

CA. Charanjot Singh Nanda
Chairman, Internal Audit Standards Board

Contents

Chapter 1
Introduction

1.1 Traditionally, internal auditing was understood as one time exercise with limited documentation. Increase in the trend of frauds in the corporate sector over the last couple of decades has shifted the pendulum towards the need of a strong and robust internal auditing and internal control systems. Regulators have also become more vigilant towards the requirement of strong internal control system which resulted in the announcement of statutory obligations *viz.*, Sarbanes Oxley Act in USA, Clause 49 of Listing Agreement as per SEBI and recently notified Companies Act, 2013 and rules thereunder. This has put organizations under increasing pressure to identify all the business risks they face and to explain how they manage them.

1.2 Risk-based Internal Auditing (RBIA) allows internal auditor to provide assurance to the Board of Directors that risk management processes are managing risks effectively, having regards to the risk appetite of the organization. Risk-based internal auditing begins by reviewing the organizational objectives, then considers the risks that impact on the achievement of those objectives, and examines the methodologies in place to mitigate those risks. The only defence auditors have in instances of corporate failures is sufficient, appropriate audit evidence that proves their innocence. This audit evidence will be the result of a well-planned and performed audit. An audit plan, currently a risk-based audit plan, is therefore a crucial component in the planning of an effective audit.

Objective

1.3 This guide provides guidance on developing and implementing an effective Risk Based Internal Audit Plan in an organization. This guide would be meant for the individuals who are already an internal auditor, preparing to become one or responsible for overseeing and controlling the business function(s).

Chapter 2
Need for Risk Based Internal Audit Plan

2.1 Preface to the Standards on Internal Audit, issued by the Institute of Chartered Accountants of India defines the term "internal audit" as, "Internal Audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with an view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system."

Standard on Internal Audit (SIA) 1 "Planning an Internal Audit", lays down that the internal auditor should, in consultation with those charged with governance, including the audit committee, develop and document a plan for each internal audit engagement to help him conduct the engagement in an efficient and timely manner.

2.2 Standard on Internal Audit (SIA) 13 "Enterprise Risk Management" mentions that "The internal auditor will normally perform an annual risk assessment of the enterprise, to develop a plan of audit engagements for the subsequent period. This plan will be reviewed at various frequencies in practice. This typically involves review of the various risk assessments performed by the enterprise (e.g., strategic plans, competitive benchmarking, etc.), consideration of prior audits, and interviews with a variety of senior management. It is designed for identifying internal audit key areas and, not for identifying, prioritizing, and managing risks directly for the enterprise. The internal audit plan, which should be approved by the audit committee, should be based on risk assessment as well as on issues highlighted by the audit committee and senior management. The risk assessment process should be of a continuous nature so as to identify not only residual or existing risks, but also emerging risks. The risk assessment should be conducted formally at least annually, but more often in complex enterprises. To serve this objective, the internal auditor should design the audit work plan by aligning it with the objectives and risks of the enterprise and concentrate on those issues where assurance is sought by those charged with governance."

2.3 Internal auditor is expected to review business processes and various transactions to provide comfort to the management whether adequate internal controls are in place considering the nature and size of business operations. Considering the volume of the transaction and complexity of the business processes, it would not be possible to check 100% of the business transactions. The internal auditor usually, adopts sampling and judgment based on past experience and knowledge. However, this leaves a risk of gap in internal controls which may remain undetected. Accordingly, there is a need for auditors to follow risk based internal audit approach.

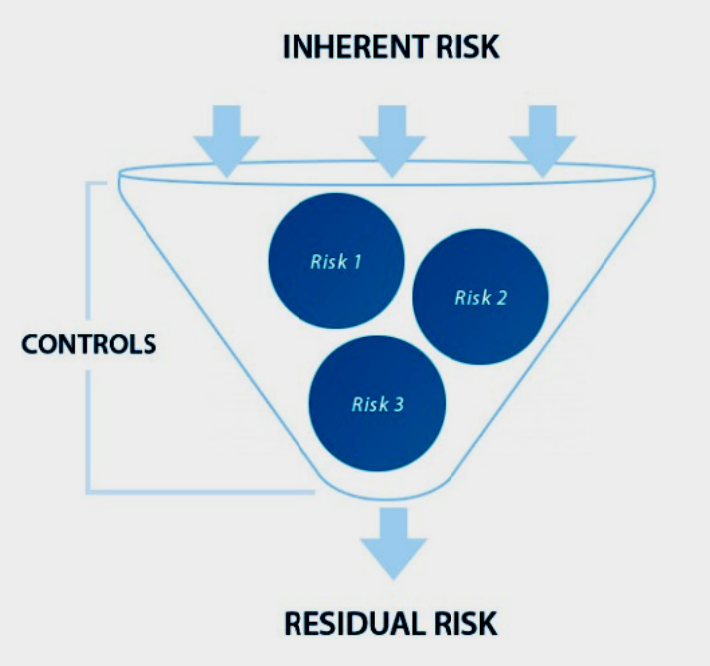
2.4 There are many challenges being faced by the internal auditors in performance of their duties. The major challenges include:

- Mismatch in the expectations from and output of the internal audit function;
- Audit risk;
- Practical implementation of audit standards; and
- Uncertainties due to changing environment – internal as well as external.

2.5 The internal audit function is, normally, expected to focus on areas of high risk, including both inherent and residual risk. The internal audit activity needs to identify areas of high inherent risk, high residual risks, and the key control systems upon which the organization is most reliant.

- Audit risk – Audit risk refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR).
- Inherent risk – These risks are “all pervasive in nature” meaning they are inherent in all business activities. Inherent risk is a risk in ‘raw form’ before any risk treatment/ mitigation activity has been applied to it.
- Residual risk – Residual risk is the level of risk that would remain untreated despite all mitigation efforts.

The figure below depicts the relationship between the inherent risk and residual risk.



2.6 Internal audit planning needs to make use of the organizational risk management process, where it has been developed by the organization. In planning an engagement, the internal auditor considers the significant risks of the activity and the means by which management mitigates the risk to an acceptable level. The internal auditor uses risk assessment techniques in developing the internal audit activity's plan and in determining priorities for allocating internal audit resources. Risk assessment is used to examine auditable units and select areas for review to be included in the internal audit activity's plan that have the greatest risk exposure.

Chapter 3
RBIAP Concepts

3.1 Risk Based Internal Audit Plan (RBIAP) is an important tool that helps internal auditor to respond to the challenges being faced by the internal auditor, and also enhances the quality of the services that the internal audit function provides. By following the structured approach for planning the internal audit, it could be easily concluded that:

- A proper evaluation has been done to identify and assess the risk vis-a-vis risk appetite of the company.
- Plan to respond to the risks are effective in managing inherent risks within the risk appetite.
- Increased focus and rigorous response to risks where residual risks are not in line with the risk appetite.

3.2 RBIAP is an approach to develop the internal audit plan in such a manner that all the business processes covering both financial as well as operational activities are reviewed by internal audit function within a defined time cycle, generally, varying from 3 to 5 years. Also, ensuring that appropriate consideration is made and adequate balance is ensured to the following:

- Risk underlying the business process.
- Value that the internal audit can provide to the organization.
- Effort involved in conducting the internal audit for a particular business process.
- Risk appetite of the organization.
- Coverage of all auditable areas within the defined time range.

Chapter 4
Responsibility for Developing RBIAP

4.1 The need to manage risks has become recognised as an essential part of good corporate governance practice. This has put organisations under increasing pressure to identify all the business risks they face and to explain how they manage them. In fact, the activities involved in managing risks have been recognised as playing a central and essential role in maintaining a sound system of internal control. While the responsibility for identifying and managing risks belongs to management, one of the key roles of internal audit is to provide assurance that those risks have been properly managed.

The Chief Internal Auditor, as designated by the audit committee, must establish a risk-based plan to determine the priorities and focus areas of the internal audit activity which are aligned to the business objectives and organization's goals. The prime responsibility of developing the Risk Based Internal Audit Plan is with the Chief Internal Auditor. The Chief Internal Auditor must prepare the RBIAP and review the same on annual basis in the light of changing business environment, processes, technology, etc. having impact on the prevailing risk for the Company and its control environment.

4.2 The RBAIP, thus, prepared by the Chief Internal Auditor must be approved by the Audit Committee. Audit Committee assesses the appropriateness of the process followed for development of the RBIAP to ensure that due consideration is given to the following:

- Consideration of all major risk for the company
- Business objectives
- Risk appetite of the company
- Inputs from the key managerial persons of the company
- Changes in the operational and regulatory environment.

Chapter 5
RBIAP — Development and Implementation

5.1 The internal auditor takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the internal auditor uses his/her own judgment of risks after consideration of input from senior management and the board. The internal auditor must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

5.2 Risk based internal audit planning includes formal annual planning, updating the plan before audit segments begin and periodic feedback from management and the audit committee regarding report content expectations. The internal audit scope is adjusted based on all of these factors and gives the internal auditor a keen ability to understand and react quickly to management and audit committee concerns regarding risk and audit coverage. Thus, there are two phases of successful implementation of the RBIAP. These include the following:

- Develop and approve RBIAP
- Implement and update RBIAP

5.3 Methodology for development of risk based internal audit plan can be divided into following steps:

I Develop and Approve RBIAP

(i) Define objective, criteria and risk appetite

(ii) Understanding the business environment and processes

(iii) Prepare audit universe

(iv) Risk assessment

  (a) Risk identification

  (b) Risk prioritization and rating

(v) Assess control environment

(vi) Derive residual risk rating

(vii) Develop internal audit plan.

II Implement and update RBIAP

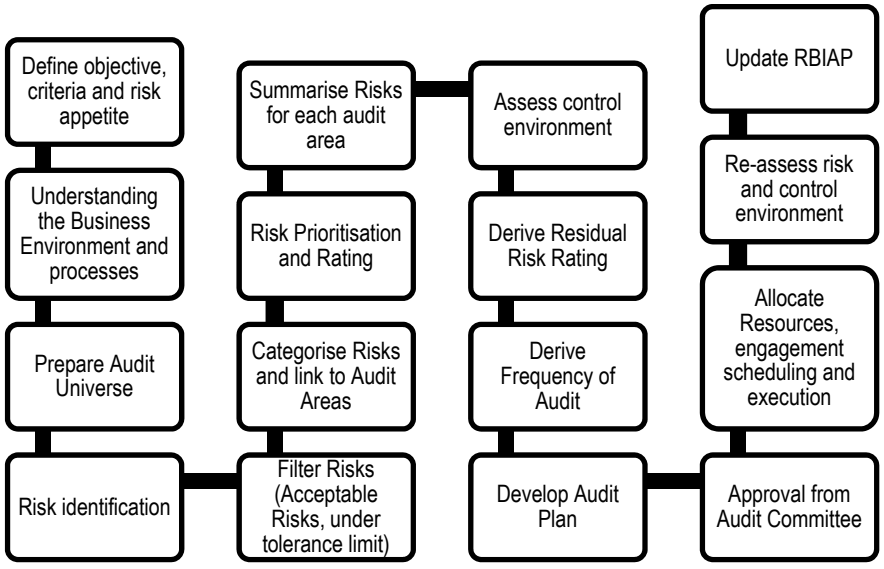
(i) Derive Annual Internal Audit plan

(ii) Allocate resources, engagement scheduling and execution

(iii) Re-assess risk and control environment

(iv) Update RBIAP.

Process of Risk Based Internal Audit Planning



Define Objective, Criteria and Risk Appetite

5.4 Internal Auditor need to first define the objective of preparing the risk based internal audit plan for a particular organization. There are varied factors that need to be considered while defining the objective of the exercise, these may include:

- Size and nature of business
- Complexity of the business process
- Resource constraint

- Time horizon which the organization considers appropriate for review of all the business processes.

5.5 Internal auditor need to define the criteria that would be used for developing the internal audit plan. It would include the following:

- Risk categorization
- Risk assessment criteria
- Criteria for assessing the control environment
- Criteria to priorities and decide the frequency of audit.

5.6 It is very critical that the criteria for developing the RBIAP are documented in advance and approved to avoid any subjectivity on the outcome of the exercise. The key factors that need to be kept in mind while finalizing these criteria include the following:

- *Inherent risks* – ensure all inherent risks are identified and assessed.
- *Residual risks* – ensure all residual risks are identified and assessed.
- *Mitigating controls*– ensure elements of control environment (e.g., level of automation, governance structure, etc.) are identified that could be linked to the individual events and/ or risks.

5.7 Internal auditor need to interact with the senior management and take a view on the risk appetite of the organization. Risk appetite of the organization can significantly impact the criteria that need to be used for the development of RBIAP. A Risk Based Internal Audit Plan should ensure that it covers all unacceptable current risks where management action is required. These would be the areas with high residual risks, i.e., high inherent risk and minimal key controls or mitigating factors. These would be the areas that senior management should get audited immediately. Identification, assessment and prioritization of the audit areas is dependent on the residual risk for the organization, which is monitored and evaluated in the light of risk appetite of the organization.

Risk rating depends on the criteria set by the organization to assess *and prioritise its risk. Depending on the risk appetite of the organization, it could mean financial loss of ₹1 Lac could be 'minor' for a large PSU with annual profit of ₹500 crores but it could be major for an organization with annual profit of ₹50 Lacs.*

Risk Categorization

5.8 According to the Internal Control Framework issued by The Committee of Sponsoring Organizations (COSO) of the Treadway Commission, risk can be categorized as under:

- Operational – Risks that impact the efficiency and effectiveness of the operations of the organization are categorized as operational risk. E.g., process delays in completing the activity, customer dissatisfaction, inadequate fund management, excess payment, etc. Some companies further categories operational risk into financial risk and non-financial risk depending on the direct impact of risk.
- Reporting – Risk of incorrect financial reporting. Internal control weaknesses which may result into incorrect financial reporting are categorized at reporting risk, e.g., inadequate cutoff procedures, lack of senior management review of financial statements, etc.
- Compliance – Risk that may result in non-compliance to the applicable regulatory requirements. E.g., delay in submission of taxes and returns, operating without obtaining the required licenses, etc. These may result into possible fines and penalties being imposed on the organization.

5.9 Organizations also classify the risk under the additional category depending on the nature of the business, e.g., a company operating in energy sector could categories the risk as under:

- Operational
- Financial
- Health, Safety and Environment
- Compliance
- Reporting

Company operating in the technology intensive sector could categories the risk as under:

- Operational
- Financial
- Technology
- Compliance
- Reporting

Risk Assessment Criteria

5.10 Risk need to be assessed in terms of severity of the impact that may come to the organization in the event of risk occurrence. Assigning the rating to the risk depending on the assessed severity is termed as risk prioritization. The typical risk prioritization is done on the scale of 1 to 5 as mentioned below:

- Score 1 - Insignificant
- Score 2 – Minor
- Score 3 – Moderate
- Score 4 – Major
- Score 5 - Critical

Criteria for Assessing Control Environment

5.11 The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility; organizes and develops its people; and the attention and direction provided by the board of directors. The typical control environment assessment is done on the scale of 1 to 5 as mentioned below:

- Score 1 – Very strong
- Score 2 – Strong
- Score 3 – Moderate
- Score 4 – Weak
- Score 5 – Almost missing.

Understanding the Business Environment and Processes

5.12 As per the requirement of Standard on Internal Audit (SIA) 1 “Planning an Internal Audit”, The internal audit plan should be comprehensive enough to ensure that it helps in achieving of the above overall

objectives of an internal audit. The internal audit plan should, generally, also be consistent with the goals and objectives of the internal audit function as listed out in the internal audit charter, as well as the goals and objectives of the organisation.

5.13 The key to effective risk-based auditing is for the internal auditor to begin the planning process with a thorough understanding of the business process for the area under review. In combination with feedback from management and the audit committee, business objectives are reviewed, specific risks that could cause management not to meet those business objectives are identified, and controls established by management to mitigate these risks are evaluated. These business objectives, risks and controls should also be reviewed in relationship to the entity wide business objectives, risks, and controls to assist in developing comprehensive corporate decisions.

Below mentioned is a simple framework that can assist in understanding the business environment:

(i) *Understand where the company is:* Really understand. Taking complete stock of a company's current situation – as regard to product innovation, customer buying patterns, PR branding, what are you selling and what you can sell.

(ii) *Compare the company with the leader in the business:* A critical comparison with the market leader will bring out the areas where most attention needs to be paid, because most often, the leading business has read the business environment right.

(iii) *Engage with stakeholders:* Constant dialogue with all stakeholders will lead to understanding the company's niche and positioning in the competitive market.

5.14 SIA 1 further defines the steps that could be followed for obtaining the knowledge of the business. The internal auditor should obtain a level of knowledge of the entity sufficient to enable him to identify events, transactions, policies and practices that may have a significant effect on the financial information. Following are some of the sources wherefrom the internal auditor can obtain such knowledge:

- Previous experience, if any, with the entity and the industry.
- Legislation and regulations that significantly affect the entity.
- Entity's policy and procedures manual.

- Minutes of the meetings of the shareholders, board of directors, and important committees of the board such as, audit committee, remuneration committee, shareholders' grievances committee.
- Management reports/ internal audit reports of prior periods.
- Newspaper/ industry journals.
- Discussion with client's management and staff.
- Visits to entity's plant facilities, etc., to obtain first hand information regarding the production processes of the entity.
- Visits to the entity's department where the accounting and other documents are generated, maintained, and the administrative procedures followed.

Prepare Audit Universe

5.15 The first important step towards putting the RBIAP on papers is the documentation of the Audit Universe. The Audit Universe is to be prepared on the basis of the business understanding obtained under previous step.

SIA1 defines audit universe as "Audit universe comprises the activities, operations, units etc., to be subjected to audit during the planning period. The audit universe is designed to reflect the overall business objectives and therefore includes components from the strategic plan of the entity. Thus, the audit universe is affected by the risk management process of the client. The audit universe and the related audit plan should also reflect changes in the management's course of action, corporate objectives, etc."

Professor Brian Cox writing in the Wall Street Journal in April 2013 explained "Quantum theory tells us that the universe we experience emerges from a bewildering, counterintuitive maelstrom of interactions between an infinity of recalcitrant sub-atomic particles." Defining the internal audit universe is much simpler than that, although the principles may well be similar.

5.16 In simple terms, audit universe can be termed as the set of all auditable units/ departments/ business process and audit areas, collectively called as auditable entities. Preparation of audit universe and selection of auditable entities in the audit universe is the most critical activity which lays the foundation for developing a robust and effective Risk Based Internal Audit Plan.

The important factor which could affect the selection of an auditable entity under the audit universe are:

(i) Organization vision, mission and objectives: The audit universe can include components from the organization's strategic plan. By incorporating components of the organization's strategic plan, the audit universe will consider and reflect the overall business objectives. Inputs from senior management and board should be obtained and assessment of risk and exposure affecting the organization should be carried out.

(ii) Expectations from the internal audit function: Audit universe need to factor all the expectations from the internal audit function. The internal audit plan, audit execution and the outcome of the internal audit process depends on the quality and comprehensiveness of the audit universe to gather all the expectations, focus areas and results expected from the performance of the internal audit activities.

(iii) Organization structure and set up: Organisation structure need to be understood while identifying the auditable entities. In case of highly centralized operations, more attention should be given to the auditable units at corporate, while in case of decentralized operations separate auditable entity need to be identified for plant/ branch/ regional office locations as applicable.

(iv) Geographical location of the organisation: Geographical location of the business set up also plays a key role in selection of units. Every location need to have a consideration and some place in the audit universe, however the identification of auditable unit need to be evaluated in consideration with other points. E.g., in case of regional office with smaller size of operations and lesser number of transactions, regional office can be considered as one auditable entity and all the business processes can be reviewed at that particular regional office together. However, if the scale of operations are larger, locations would need to be split into further functional areas e.g., Procurement - RO, Sales & Marketing – RO, HR and Payroll – RO, etc.

(v) Scalability of the operations: Scale of business operations should also be factored while deciding an auditable entity. Auditing an entity with very low scale may not be cost effective to be audited separately and may not give the actionable results as it would fall in the comfort range of the risk appetite of the organization.

(vi) Organic linkage between the business process/ sub processes: It is becoming increasingly important, to perform the objective study and conduct end to end review of a business process so that organization level impact on the identified gaps can be assessed and more objective decisions could be taken by the management on the basis of result of the internal audit activities. Hence, it is vital to study the linkage between business process and sub process. E.g., it is more effective to review the complete process of Procure to Pay (P2P) so that financial implication and complete process gaps could be identified. Review of the procurement process or payment process in isolation would not provide effective root causing and implication assessment of the internal audit gaps noted during the review.

(vii) Sufficiency to justify cost of control: Internal audit function acts as a control activity and keeps the regular check on the functioning of the business activities. Internal audit requires a team of qualified professionals with expert knowledge on the subject matter. With the increase in the expectations from and responsibilities of internal audit professional, the cost of the internal audit function is also increasing. It is important to keep the adequate balance in the cost of the internal audit review and benefit envisaged to realize from the review. Hence, cost of internal audit should be kept in mind while identifying the auditable entities.

5.17 It is important to understand that it's not the size of the audit universe that matters rather it is the extent of the focus for the internal audit plan in strategic and operational terms.

Having understood the key factors to be kept in mind and the objective of preparing the audit universe, let's have a quick glance at the steps that need to be followed for developing the audit universe.

(i) Discussion with Management: Perform detailed discussion at all the level of senior and top management including the board members to understand their expectation, objectives and key focus areas.

(ii) Sketch Audit Universe: Prepare the initial sketch of the audit universe containing the list of identified business process and auditable entities that need to be audited by the internal audit function.

(iii) Assess objectives for identified auditable entities: Align the objective of the internal audit with the objectives of the business and assess the objectivity of reviewing the identified auditable entities. The category of such objective could be:

(a) Reliability and integrity of financial and operational Information

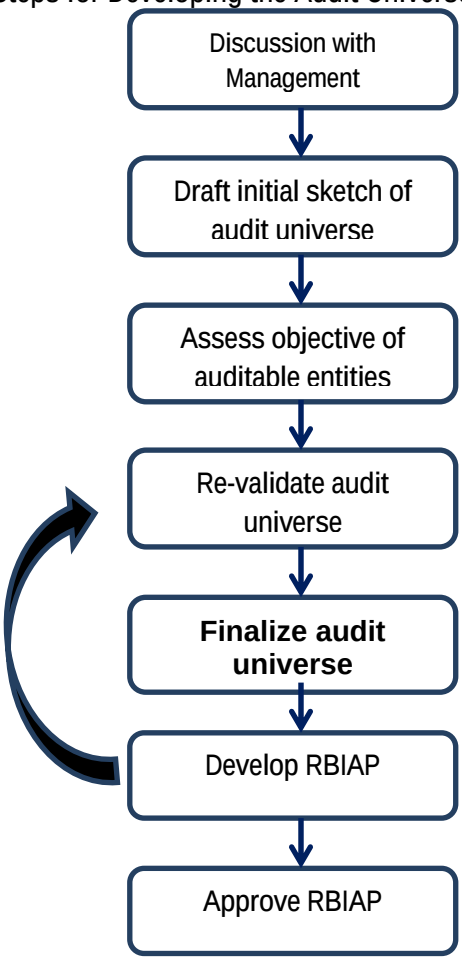
(b) Effectiveness and efficiency of operations

(c) Safeguarding of assets

(d) Compliance with laws, regulations, and contracts

(iv) Re-validate Audit Universe: The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the organization. The validation exercise is pervasive and continuous in nature until the annual plan is finalized and approved by the audit committee/ board.

Steps for Developing the Audit Universe



5.18 Following are some illustrative audit universe:

(i) Illustrative Audit Universe of a Manufacturing Company:

Sr. no.	*Department*	*Business Locations*			
		Corporate Office	*Plant*	*Branch Office 1*	*Branch Office 2*
1	Order to Cash			✔	✔
2	Procure to Pay		✔		
3	Human Resource and Payroll	✔			
4	Finance and Accounts	✔	✔		
5	Production		✔		
6	Logistics and Distribution		✔	✔	✔
7	Capital Expenditure	✔			
8	Plant Maintenance		✔		
9	Information Technology	✔			
10	Warehouse Management			✔	✔
11	Statutory Compliances	✔	✔		

(ii) Illustrative Audit Universe of a Oil and Gas Company:

D. Sr. no.	*Department*	*P. Sr. No.*	*Process*	*Business Locations*		
				Corporate Office	*Plant*	*Depot*
1	Contracts	1.1	Tendering and RFQ	✔		
1	Contracts	1.2	Contracting and Ordering	✔		
2	Plant Operations	2.1	Production and Distribution		✔	
2	Plant Operations	2.2	Operation and Maintenance		✔	

D. Sr. no.	*Department*	*P. Sr. No.*	*Process*	*Business Locations*		
				Corporate Office	*Plant*	*Depot*
2	Plant Operations	2.3	Safety and Environment		✔	
3	Drilling	3.1	Drilling		✔	
4	Information Technology	4.1	IT Security	✔	✔	
4	Information Technology	4.2	ERP and other applications	✔		
5	Geology & Reservoir	5.1	Geology & Reservoir		✔	
6	Research and Development	6.1	Research and Development		✔	
7	Material Management	7.1	MM - Planning & Receiving		✔	
7	Material Management	7.2	MM - Depot		✔	✔
7	Material Management	7.3	MM - Inventory Handling and Storage		✔	✔
8	Well Logging	8.1	Well Logging		✔	
9	Finance and Accounts	9.1	Financial Planning and Analysis	✔		
9	Finance and Accounts	9.2	Treasury	✔		
9	Finance and Accounts	9.3	Financial Reporting	✔	✔	
9	Finance and Accounts	9.4	Asset Management		✔	
9	Finance and Accounts	9.5	Payables		✔	

D. Sr. no.	*Department*	*P. Sr. No.*	*Process*	*Business Locations*		
				Corporate Office	*Plant*	*Depot*
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔	
9	Finance and Accounts	9.7	JV Operations	✔		
9	Finance and Accounts	9.8	Taxation		✔	
10	Human Resource	10.1	Recruitment		✔	
10	Human Resource	10.2	Learning and Development		✔	
10	Human Resource	10.3	Separations		✔	
10	Human Resource	10.4	Payroll Process		✔	
11	Projects	11.1	Planning and Investment	✔		
11	Projects	11.2	Execution and handover		✔	
12	Business Development	12.1	Business Development	✔		
13	Exploration & development	13.1	Exploration & development		✔	

Risk Assessment

5.19 The objective of the risk assessment is to assess the level of risk in the various business processes. Risk assessment focuses on the business environment, regulatory environment, organisation structure, organizational and business environmental changes and specific concerns of management and the audit committee to determine the areas of greatest risk. It also serves to aid the internal auditor in evaluating the control design to determine

the desired audit scope. Risk assessment includes risk identification and then risk prioritization based on defined criteria.

Risk Identification

5.20 Risk identification is the process to identify all possible risk in the auditable entities identified at the time of preparation of the audit universe. This includes evaluation of 'what can go wrong' in the particular process attached with the identified auditable entity which can have any adverse impact on the organization. The adverse impact could be in the form of possible financial loss, operational inefficiency and ineffectiveness, statutory non-compliance, incorrect reporting, etc. The quality and effectiveness of the risk assessment depends on the comprehensiveness and completeness of the risk identification exercise.

5.21 The first step in the risk identification exercise is to identify the event which may affect the entity positively or negatively in achieving its objectives. Such events may be classified as risk and opportunities depending on its impact on the organization. Risk identification is followed by risk filtration steps. Risk can be all pervading; they can surface from the most obscure to the most obvious (but overlooked) areas. Similarly, their outcomes can also be from the immaterial to highly significant. These are the matters which are quite difficult to appreciate or evaluate at the time of risk identification and are therefore best left for the next state (Risk Prioritization). Nevertheless, given the practical limitations, some level of judgment will have to be applied in deciding what to include and what to exclude at the identification stage. Here, to ensure that no important matters are overlooked, it is always safer to begin by initially including all the risk and then filtering out everything which appears to be obviously insignificant and with remote probability of occurrence.

Risk Prioritization

5.22 The identified risk need to the prioritized based on the pre-defined criteria (*Refer step 1 - Define objective, criteria and risk appetite*). The typical risk periodization is done on the scale of 1 to 5 as mentioned below:

- Score 1 - Insignificant
- Score 2 – Minor
- Score 3 – Moderate

- Score 4 – Major
- Score 5 - Critical

5.23 There are various factors that could affect the risk prioritization and rating. Following factors need to be kept in mind while performing the risk prioritization exercise:

(i) "Auditable" risks associated with/ mapped to the business process, entity or location

(ii) Risk of non compliance (penalty, etc.)

(iii) Magnitude of Financial Loss

(iv) Significance of threat to Health, Safety & Environment (HSE)

(v) Risk to reputation of organisation

(vi) Possibility of fraud/ misappropriation

(vii) History of frauds or irregularity

(viii) Management's assertion on impact

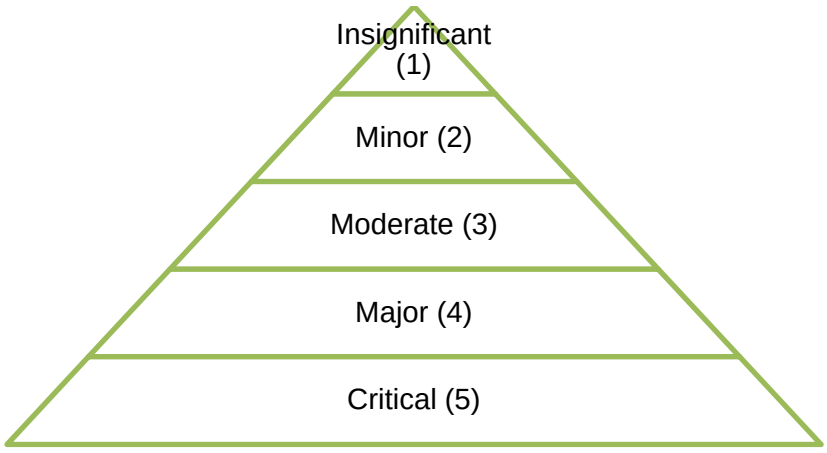
(ix) Magnitude of impact on organisational profitability

(x) Stability of IT systems

(xi) Complexity (volume of business, nature of business)

(xii) Results of earlier audits external/ internal

Risk Rating Pyramid



5.24 The preliminary risk rating can be assessed and interpreted using the below mentioned methodology.

Preliminary Risk Rating	Description	Illustrative parameters for Assessing
1	Insignificant	• Process risks with insignificant risk on the organization. • Non-compliance with minor penalties. • Impact of very low financial loss. • No major threat to Health, Safety & Environment. • No history of fraud/ misappropriation • Minor impact on organizational profitability. • Stable IT and ERP systems.
2	Minor	• Process risks with minor risk on the organization. • Non-compliance with minor penalties. • Impact of minor Financial Loss. • No significant threat to Health, Safety & Environment. • Minor fraud/ misappropriation. • Minor impact on organizational profitability. • Stable IT and ERP systems.
3	Moderate	• Process risks with tolerable risk on the organization. • Non-compliance with major financial penalties. • Impact of significant financial loss. • Possible threat to Health, Safety & Environment. • Possible fraud/ misappropriation. • Tolerable impact on organizational profitability.

Preliminary Risk Rating	Description	Illustrative parameters for Assessing
		• Stable IT and ERP systems.
4	Major	• Process risks with major risk on the organization. • Risk of reputational impact to organization. • Non-compliance with major financial penalties or prosecutions. • Impact of Major Financial Loss. • Significant threat to Health, Safety & Environment. • Repeated fraud/ misappropriation. • Major impact on organizational profitability. • Deficient IT and ERP systems.
5	Critical	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization. • Risk with impact on going concern of the organization. • Non-compliance with major financial penalties and prosecutions. • Impact of High Financial Loss. • Significant threat to Health, Safety & Environment. • Repeated fraud/ misappropriation with major financial or reputational consequences. • High impact on organizational profitability. • Missing IT and ERP systems.

5.25 Some techniques of risk assessment are explained below:

- Interviews: Internal auditor need to conduct interviews at all levels of management to identify the possible risk that could occur in the

particular process as per the experience of the management personnel. Internal auditor can assess the level of understanding of the organization's process, policies, systems used and controls in place during these interviews. This would help them in assessing the control environment around the particular auditable entity. We would discuss more about the control environment later in this chapter.

- Surveys: Internal auditor can perform surveys to identify and assess the gravity of the risk and its possible impact on the organization. An important aspect of the survey is to prepare a qualitative questionnaire that would help in identification of the qualitative risk and its impact. The target audience need to be selected carefully while performing the survey so that results are not biased.
- Workshops: The Internal auditor can also perform workshops with the selected managerial persons to identify the risk in the particular process and ask them to rate them based on the defined methodology. There are many tools that may be used to perform these workshops effectively.
- Past events: The activities performed by the internal auditor during the business understating stage can also give lot of information to the auditor to identify the possible risks for the organization. This could include past events, annual report and directors statement, past internal audit reports, risk register, etc.
- Internal auditors experience: Experience of the internal auditor also plays a key role in identifying the possible risks in the particular process of the organization. The gravity of the risk identified by the auditor from his experience can be moderated by using the techniques specified in the above mentioned bullets.

Prepare Risk Register

5.26 The consolidated form of all risks is referred to as "Risk Registers" since all such identified risks most often get listed in the form of a register. The typical contents of the risk register are listed below.

Contents applicable and filled till the stage of risk assessment are as follows:

(i) Auditable Entity

(ii) Sub Process

(iii) Risk Description

(iv) Risk Category

(v) Risk Rating

Illustrative format of the Risk Register is as follows:

Sr. no.	*Auditable Entity*	*Sub Process*	*Risk Description*	*Risk Category*	*Risk Rating*
1	Order to Cash				
2	Procure to Pay	Procurement Planning	Procurement beyond the defined budgetary limits.	Financial Loss	4
3		Vendor Selection	Inadequate vendor selection due to non-compliance to procurement policies and procedures (incl. tendering)	Financial Loss	4
4		Ordering	Increased cost of procurement due to ineffective negotiation/comparison of commercial bid submitted	Financial Loss	5
5		Receiving			
6		Quality check			
7		Invoicing			
8		Accounts payables			
9		Payment processing			

** Information included in the above format is illustrative.*

The next step toward documentation of risk based internal audit plan is to document the detailed risk register containing the list of all the risks identified and the preliminary risk rating.

5.27 The next step is to prepare the summarized risk register. The objective of preparing the summarized register is to arrive at the consolidated risk rating for an auditable entity and assess the overall inherent risk in the auditable entity. There are two techniques which may be used for arriving at the summarized risk register:

(i) Arithmetic mean of preliminary risk rating: In this method, arithmetic mean of all the identified risk ratings are is calculated to arrive at the consolidated risk rating. Considering the simplicity of the technique, this is the most widely used technique to arrive at the summarized risk register.

(ii) Weighted average of preliminary risk rating: In this method, weights are assigned to all the identified risk on the basis of statistical computation of the probability and quantification of possible risk on the organisation. Weighted average of all the identified risk ratings is then calculated to arrive at the consolidated risk rating.

Illustrative Format of Summarized Risk Register

Sr. no.	*Auditable Entity*	*Sub Process*	*Risk Description*	*Risk Category*	*Risk Score*	*Consolidated Risk Rating*
1	Procure to Pay	Procurement Planning	Procurement beyond the defined budgetary limits.	Financial Loss	4	3.25
2		Vendor Selection	Inadequate vendor selection due to non-compliance to procurement policies and procedures (incl. tendering)	Financial Loss	4	
3		Ordering	Increased cost of procurement due to ineffective negotiation/comparison of commercial bid submitted	Financial Loss	5	
4		Receiving	Risk of receiving more than the ordered quantity	Financial Loss	3	
5		Quality	Risk of accepting the	Operation	4	

Sr. no.	*Auditable Entity*	*Sub Process*	*Risk Description*	*Risk Category*	*Risk Score*	*Consolidated Risk Rating*
		check	inferior quality of material	al/ Financial		
6		Invoicing	Risk of delay in invoice processing	Operational	2	
7		Accounts payables	Duplicate vendor codes	Operational/ Financial	3	
8		Payment processing	Risk of delay in payment processing	Operational/ Financial	1	

Assess Control Environment

5.28 Preliminary assessment of the risk provides the understanding and evaluation of inherent risk. Assessment of inherent risk alone is not sufficient to identify the audit areas requiring the larger focus from the internal audit function. The inherent risk need to be factored with the mitigating controls and the control environment around the underlying processes that could reduce the level of residual risk. Hence, it is vital to perform the assessment of control environment around the identified risks. The control environment thus assessed provides the assessment of the 'likelihood' factor of the identified risk.

Assessing likelihood of the happening of an event comes with its own challenges. It is relatively easy to put in place a pre-set methodology for the actual measurement of the rating by taking some percentages and assigning them on 1 to 10 rating. However, what's most difficult is the foresight required to actually determining the probability of the risk. One technique used commonly is the history of past occurrence and the periodicity of those occurrences, which can help to get a better grasp over the probability.

5.29 Some of the examples of situations that might influence the assessment of control environment are as below:

- Inappropriate pay, reward and incentive structures which contribute to inappropriate behavior or excessive risk-taking.
- Increasing employee turnover leading to insufficient experience and less reliable execution of controls. This may be the result of a number of failures in the control environment.
- The absence of a defined code of conduct and ethics and/ or a whistleblower policy, absence of a process to evaluate the effectiveness of the code of conduct and ethics policy, a high number of reported frauds, or management over-ride of controls which can lead to inappropriate activity that is not detected and addressed timely.
- Board's capability and structure for effective governance.
- Key managers making business decisions without considering the related risks; management may not exhibit risk and control consciousness in its decision making.
- Processes relating to defining job descriptions for key positions may be weak, background checks and/ or reference checks are not consistently performed, or the organization has difficulty hiring and retaining qualified individuals.

5.30 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the updated Internal Control – Integrated Framework in 2013. The framework states "The control environment is the set of standards, processes and structures that provide the basis for carryign out internal control across the organisation. The board of directors and senior management establish the tone at the top regarding the importance of internal control including expected standards of conduct. The control environment comprises the integrity and ethical values of the organsation; the parameters enabling the board of directors to carry out its governance oversight responsibilities; the organisational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigour around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control."

5.31 There are various factors that could affect the assessment of control environment and its rating.

Following factors need to be kept in mind while performing the assessment of control environment as mentioned below:

(i) Existence of preventive or detective control to mitigate risks associated with/ mapped to the business process, entity or location.

(ii) Legal compliance framework

(iii) Appropriate and established IT Control environment

(iv) Governance structure/ monitoring Mechanism

(v) Documented policy and procedures

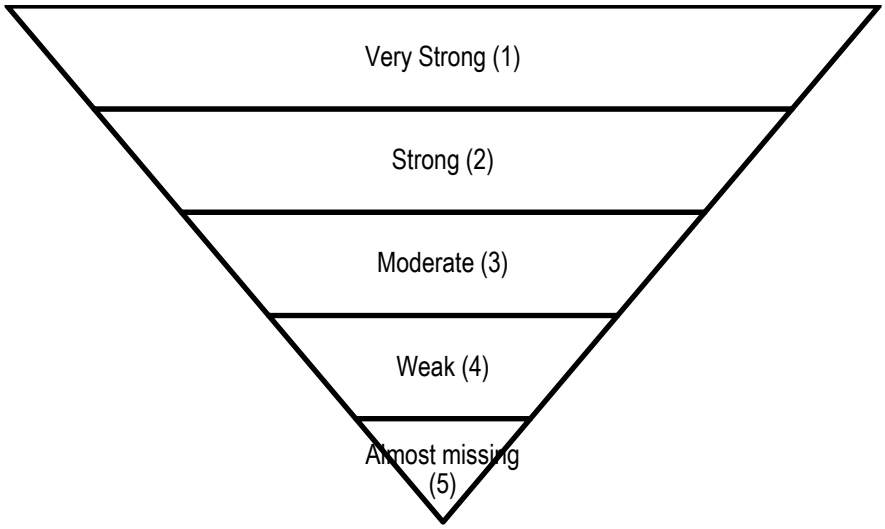
(vi) Past incidents/ trend

(vii) Organization's sensitivity towards Health, Safety & Environment

(viii) Fraud detection

(ix) Balance of centralized versus decentralized operations within the organization

Control Environment Rating Pyramid



5.32 Internal auditor need to assess and consider the level of effectiveness of control environment activities and the risk of deficiencies in the control environment, while defining the audit universe and RBIAP.

The control environment rating can be assessed and interpreted using the below mentioned methodology.

Control Environment Rating	Description	Illustrative Parameters for Assessing
1	Very Strong	• Existence of strong preventive or detective control with mechanism for continuous monitoring and update the same • Strong legal compliance framework • Well established ERP system and IT security measures • Well defined and implemented policy and procedures • Consistent organisation growth with rare surprises • Balance of centralized versus decentralized operations within the organization
2	Strong	• Defined preventive or detective control • Strong legal compliance framework • Established ERP system and IT security measures • Well defined policy and procedures and minor deviations • Consistent organisation growth with unlikely losses • Balance of centralized versus decentralized operations within the organization
3	Moderate	• Defined preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations • Established ERP system and IT security measures • Defined policy and procedures but insufficient control on implementation and compliance to same.

Control Environment Rating	Description	Illustrative Parameters for Assessing
		• Consistent organisation growth with possible losses
4	Weak	• Preventive or detective controls not identified or defined • Missing legal compliance framework with alternative measure to monitor legal compliance • Moderate IT environment with missing automated controls. • Policy and procedures not formally defined and there may be possible deviations • Consistent organisation growth with frequent losses • Inadequate board monitoring and governance structure
5	Almost Missing	• Missing preventive or detective controls • Missing legal compliance framework with no alternative measure to monitor legal compliance. • Insufficient IT environment with missing automated controls. • Policy and procedures not defined • Inconsistent organisation growth with major losses • Inadequate board monitoring and governance structure • Inadequate decentralisation of decision making

Update Summarized Risk Register

5.33 The next step is to update the summarized risk register. The summarized risk register needs to be updated with the following information:

(i) Factor Affecting Control Environment

(ii) Control Environment Rating

At this stage, the detailed risk register is replaced with the summarized risk register to contain the following information:

(i) Auditable Entity

(ii) Sub-process

(iii) Initial Risk Rating for each sub process (i.e., the consolidated risk rating arrived in previous step)

(iv) Rationale for initial risk rating

(v) Control environment rating

(vi) Rationale for control environment rating

Illustrative Updated Risk Register

Sr. no.	Auditable Entity	Sub Process	Initial Risk Rating	Rationale for initial risk rating	Control environment rating	Rationale for control environment rating
1	Procure to Pay	Procurement Planning	3.25	High risk of financial loss and procurement at high prices	4	Weak IT system and Manual controls. Policies and procedures not defined and ineffective monitoring by management.
		Vendor Selection				
		Ordering				
		Receiving				
		Quality check				
		Invoicing				
		Accounts payables				
		Payment processing				

Derive Residual Risk Rating

5.34 As referred earlier, preliminary assessment of the risk provides the understanding and evaluation of inherent risk. The inherent risk needs to be factored with the mitigating controls and the control environment around the underlying processes that could reduce the level of residual risk.

There are two elements of a risk:

- Impact Rating or Preliminary Risk Assessment Rating.
- Likelihood Rating (also called probability) or Control Environment Rating.

Consequence and likelihood can be multiplied together to give a single measure of the significance of a risk, or a residual risk. For example, take a risk that purchases prices are not competitive. Assuming it has high impact on the organization's cost of purchase, the impactrating could be major (scores 4) but the likelihood could be 3 due to moderate control environment. Table below describes the illustrative examples of calculating the residual risk scores.

Illustrative Risk	Preliminary Risk Rating (A)	Control Environment Rating (B)	Residual Risk Score (C)
Inadequate objectives and strategy	5	1	5
Inappropriate stocking of goods	5	1	5
Ineffective assessment of competition	5	3	15
Ineffective Pricing	5	2	10
Inadequate store layout	4	4	16
Incorrect Invoicing	4	1	4
Stock Outs	5	1	5

Thus, this can be concluded that :

Residual Risk Rating Score = Preliminary Risk Assessment x Control Environment Rating

Update Summarized Risk Register

5.35 The next step is to update the summarized risk register. The summarized risk register need to be updated with the residual Risk Rating.

At this stage, the summarized risk register would contain the following information:

(i) Auditable entity

(ii) Sub process

(iii) Initial risk rating for each sub process

(iv) Rationale for initial risk rating

(v) Control environment rating

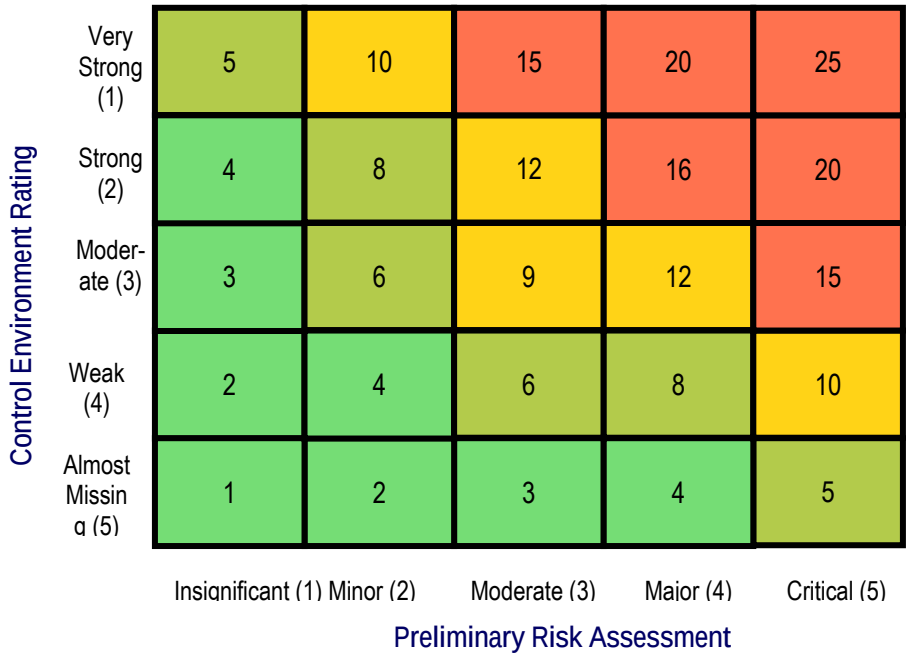
(vi) Rationale for control environment rating

(vii) Residual risk rating score

Illustrative Updated Risk Register

Sr. no.	Auditable Entity	Sub Process	Initial Risk Rating A	Rationale for initial risk rating	Control environment rating B	Rationale for control environment rating	Residual Risk Rating Score C = A X B
1	Procure to Pay	Procurement Planning	3.25	High risk of financial loss and procurement at high prices	4	Weak IT system and Manual controls. Policies and procedures not defined and ineffective monitoring by management.	13
		Vendor Selection					
		Ordering					
		Receiving					
		Quality check					
		Invoicing					
		Accounts payables					
		Payment processing					

The Matrix below describes the residual risk rating score for all combinations of the Preliminary Risk Assessment and Control Environment Rating.



Develop Internal Audit Plan

5.36 Business environment is very dynamic, typically three to five years internal audit plan is developed, considering the nature of business, business environment, stability of the business processes, changes in the objective of the management and expectations from the internal audit.

With certain adjustments based on management and audit committee input or regulatory requirements, low- risk areas would be audited every three years, moderate-risk areas audited every other year, and high-risk areas audited every year. The three-year audit plan should be revisited each year during the update phase of the risk assessment process and adjustments should be made based on new or changed risk factors. This methodology allows the internal auditor flexibility in a changing risk environment. Further consideration should be given to the following aspect while deriving the annual internal audit plan.

- Availability of audit resources over the 3 year period;

- Feasibility of conducting an audit;
- Conduct of other reviews providing oversight;
- Mandated audit projects;
- Management requests;
- Audit and Evaluation Committee direction.

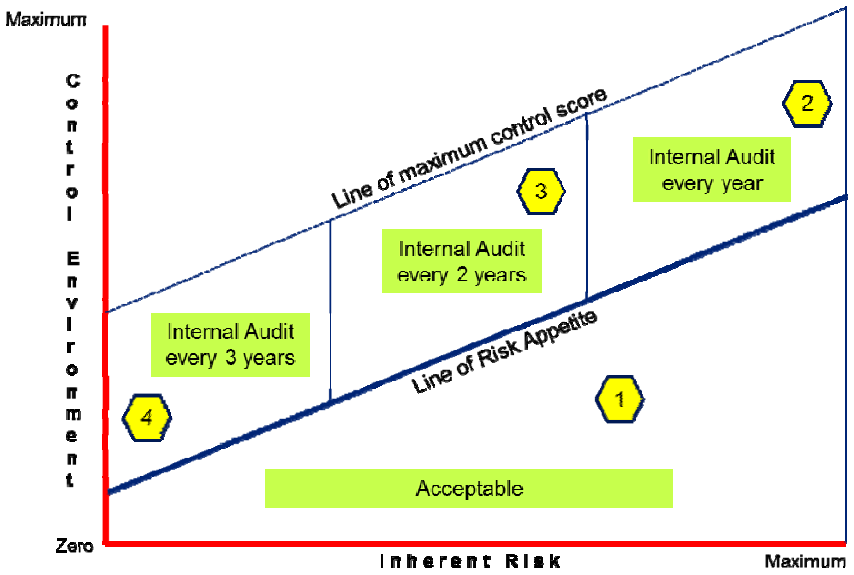
5.37 New priorities are determined based on these considerations; audits are defined for the top priorities. The outcome is a short-list of audit projects and activities to be conducted during the coming three-year planning horizon. An analysis of the proposed audit coverage of the organization is conducted in order to ensure an appropriately balanced audit plan. The project team considered the number of corporate risks covered by the plan, the number of priorities covered, and how the allocation of audit resources aligns with the organization's expenditures.

Acceptable Range of Risks

5.38 At this stage it is important to understand and define the organisation's 'risk appetite'. One method of deciding which risks to accept is to place them on a grid of Risk and Control Environment rating. This enables the board/ audit committee to define the action it requires internal audit function to take for each likelihood/ consequence combination. The boundary between the acceptable risks and those which require managing is known as the 'risk appetite'. If inherent risks cannot be managed below this line by 'treatment' then they will have to be terminated, transferred or tolerated.

Selection of Risks

5.39 At this point, the risk and audit universe shows risks, their scores and the audits linked to them. There will be a range of scores and, in drawing up the audit plan, a policy will have to be established about which risks to cover and how often. It is unlikely that the board, or audit committee, will require assurance on the management of every risk above the risk appetite, every year. They may require assurance on the risks with a high likelihood of significant/ critical losses every year but other risks above the risk appetite every two or three years. Note the audit action to be taken and the next audit year in the appropriate columns. The diagram below shows a possible method of assessing the type of work and frequency. The thick line represents the risk appetite (the equation of the line is control risk = inherent risk – risk appetite).



Frequency of Audit and its Selection

5.40 The various auditable entities can be plotted on a matrix which would fall in any of the Zone 1 to 4 as mentioned in the above graph. The appropriate audit plan for the various auditable entities in these zones can be derived as per below explanation:

Zone 1: These are the areas below the risk appetite of the organisation. Considering the fact that they are well within the tolerance (Risk Appetite) range of the organisation, these does not require immediate internal audit attention. For these areas control score is minimal and the inherent risk is maximum. These areas require management attention to carry out the consultancy work and develop the control environment.

Zone 2: Areas where inherent risk is near maximum and the control score is also very strong, the residual risk score remain high. These areas need to be audited every year as the control is considered to be very effective as well as the risk is high.

Zone 3: Areas where inherent risk is moderate and the control score is also moderate, the residual risk score remain medium. These areas could be audited every two years.

Zone 4: Areas where inherent risk is minor and the control score is also missing, the residual risk score is low. These areas need to be audited every three year as the possible impact on the organisation is low.

Planning and Developing Internal Audit Plan

5.41 At this stage, the risk and audit universe shows risks, their scores and the audits linked to them. Internal audit function needs to plot the auditable entities in the following zones based on the residual risk ratings and the immediate objective of the management and audit committee.

(i) High Risk: This is said to be the unacceptable zone, where the residual risk score is more than 12. These are the areas with high inherent risk and low control environment. These areas need to be audited every year until the residual risk are reduced and brought in the manageable zone.

(ii) Medium Risk: This is said to be the manageable zone, where the residual risk score is more than 8 and less than or equal to 12. These are the areas with minor to critical risk and varying control environment. These areas need to be audited once in every two year until the residual risk are reduced to advisable zone.

(iii) Low Risk: This is said to be the advisable zone, where the residual risk score is more than 4 and less than or equal to 8. These are the areas with insignificant to Major risk and strong to almost missing control environment. These areas need to be audited once in every three year until the residual risk are reduced acceptable zone.

(iv) Insignificant Risk: This is said to be the acceptable zone, where the residual risk score is less than or equal to 4. These are the areas with low risk and strong control environment. These areas need not be audited unless Board/ Management/ Audit Committee directs considering the recent changes or business objectives. This is the zone which contains the areas within the risk appetite of the organisation.

Update Risk Register and Audit Universe

5.42 The risk register containing all identified and assessed risk need to be updated with following:

(i) Factors Affecting Control Environment

(ii) Control Environment Rating

(iii) Risk Category

(iv) Risk Rating

Update Summarized Risk Register

5.43 The next step is to update the summarized risk register. The summarized risk register need to be updated with the frequency of internal audit.

At this stage, the summarized risk register would contain the following information:

(i) Auditable entity

(ii) Sub-Process

(iii) Initial Risk Rating for each sub process

(iv) Rationale for initial risk rating

(v) Control environment rating

(vi) Rationale for control environment rating

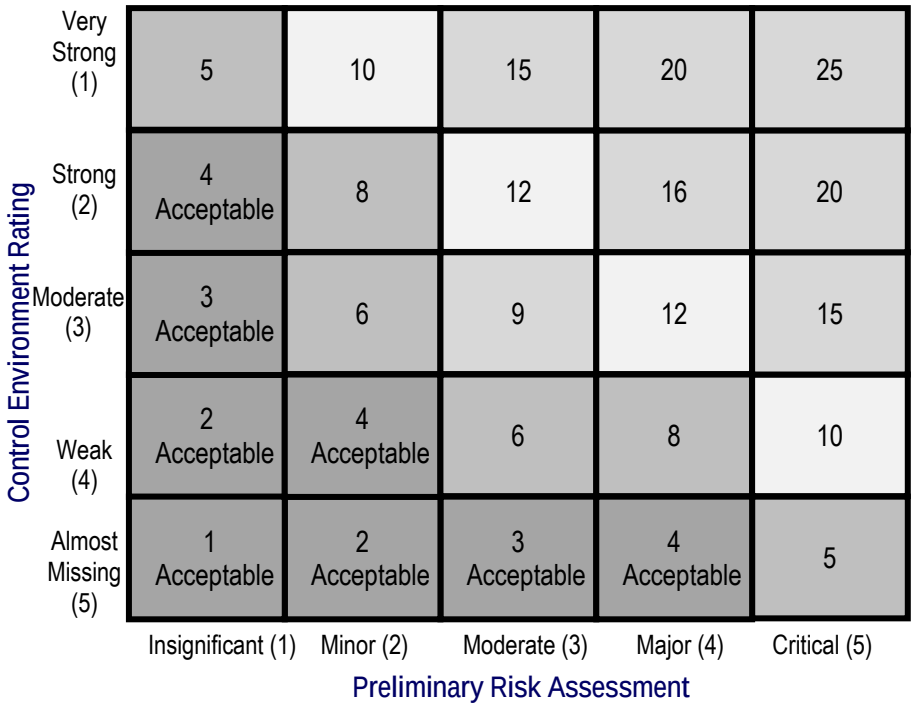
(vii) Residual Risk Rating Score

(viii) Frequency of Audit

Illustrative Updated Risk Register

Sr. no	Auditable Entity	Sub Process	Initial Risk Rating A	Rationale for initial risk rating	Control environment rating B	Rationale for control environment rating	Residual Risk Rating Score C = A X B	Frequency of Audit
1	Procure to Pay	Procurement Planning	3.25	High risk of financial loss and procurement at high prices	4	Weak IT system and Manual controls. Policies and procedures not defined and ineffective monitoring by management.	13	Once in a year
		Vendor Selection						
		Ordering						
		Receiving						
		Quality check						
		Invoicing						
		Accounts payables						
		Payment processing						

The Matrix below describes the residual risk rating score for all combinations of the Preliminary Risk Assessment and Control Environment Rating and the corresponding audit frequency.



Matrix of Residual Risk Scores and Audit Frequency

Implement and Update RBIAP

5.44 Once the three year risk based internal audit plan is developed, the same needs to be implemented in the organisation for ensuring effective conduct of the internal audit activities. For effective implementation of the RBIAP, the following stages are involved.

(i) Prepare audit scope

(ii) Allocate resources, engagement scheduling and execution

(iii) Re-assess risk and control environment

(iv) Update RBIAP

Prepare Internal Audit Scope

5.45 As per the SIA 1, "Planning an Internal Audit" issued by The Institute of Chartered Accountant of India:

> "15. The next stage in planning an internal audit is establishing the scope of the engagement. The scope of the engagement should be sufficient in coverage so as to meet the objectives of the engagement. The internal auditor should consider the information gathered during the preliminary review stage to determine the scope of his audit procedures. The nature and extent of the internal auditor's procedures would also be affected by the terms of the engagement. In case the internal auditor is of the view that circumstances exist which would restrict the auditor from carrying out the procedures, including any alternative procedures, considered necessary by him, he should discuss the matter with the client to reach a conclusion whether or not to continue the engagement. The scope of his engagement should documented comprehensively to avoid misunderstanding on the areas covered for audit. The internal auditors are often confronted with a situation where client denies access to certain information or has a negative list of areas where internal audit is not desired. There are also situations where while the client requires internal audit procedures to be carried but findings are not to form part of the reportbut to be reported separately.
>
> 16. Further, in case of information technology based environment, the scope of engagement would include the extent to which internal auditor are permitted to access the system and reports which can be viewed and those which can be exported. Further, system based audit tools that an internal auditor can use to draw and analyze the data should be clearly understood in the scope of his engagement."

5.46 The annual internal audit plan need to be approved by the board/ audit committee and should be developed on the basis of the three year RBIAP and the following additional factors:

- Changes in the business environment
- Changes in the organisation structure

- Changes in the business processes
- Changes in the regulatory environment
- Time of last audit engagement
- Availability of the skilled resources
- Management's feedback and expectation from internal audit
- Changes in employee and government relations
- Recent change in accounting system
- Recent change in key personnel

5.47 The audit scope for the year need to be developed considering the above mentioned factors. The scope, thus, prepared would be finalized for an year and approved by the board/ audit committee. The audit scope comprises of the following:

- Auditable entities
- Locations to be covered
- Tentative schedule of the audit
- Key objective of the audit
- Factors which define the limits of the audit including processes specifically excluded
- Any special considerations, such as management requests, provided they are acceptable
- Personnel carrying out the audit, including any special responsibilities

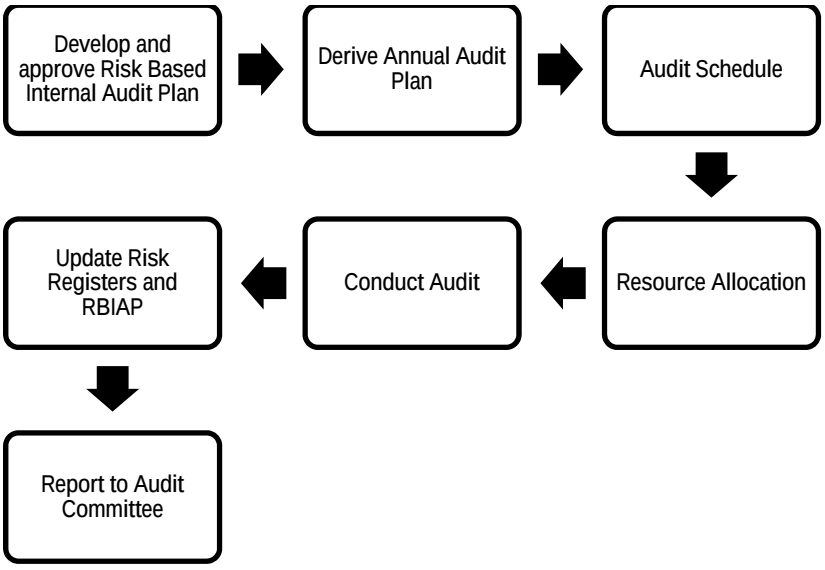
Allocate Resources, Engagement Scheduling and Execution

5.48 We can decide on the staff resources required to deliver the internal audit plan by deciding on the number of days each level of auditor is required for each audit, adding these up, and comparing them with the total days available. Note that audits will vary in length, even those which are high risk could be done very quickly. It may only take logging into organisation's intranet to confirm that it has a strategy, and this is being communicated. The resource requirements should be regularly updated to ensure the plan can be completed, especially, if audits are added and staff leave.

Next step is to perform the detailed engagement scheduling based in the

allocated resources, availability of the auditee, target date to finalise the report and criticality and extent of audit required. The schedule need to be agreed with the auditee before execution. The schedule need to be realistic to ensure adequate coverage of the work plan, assessment of all the identified risks and testing of all the controls. This is followed by the execution of the internal audit as per the defined approach and methodology of the internal audit function of the organisation and the relevant auditing standards.

Steps for Audit Scheduling, Resource Allocation and Execution



Re-assess Risk and Control Environment and Update RBIAP

5.49 SIA 1 "Planning as Internal Audit" defines audit universe as "Audit universe comprises the activities, operations, units, etc., to be subjected to audit during the planning period. The audit universe is designed to reflect the overall business objectives and therefore includes components from the strategic plan of the entity. Thus, the audit universe is affected by the risk management process of the client. The audit universe and the related audit plan should also reflect changes in the management's course of action, corporate objectives, etc."

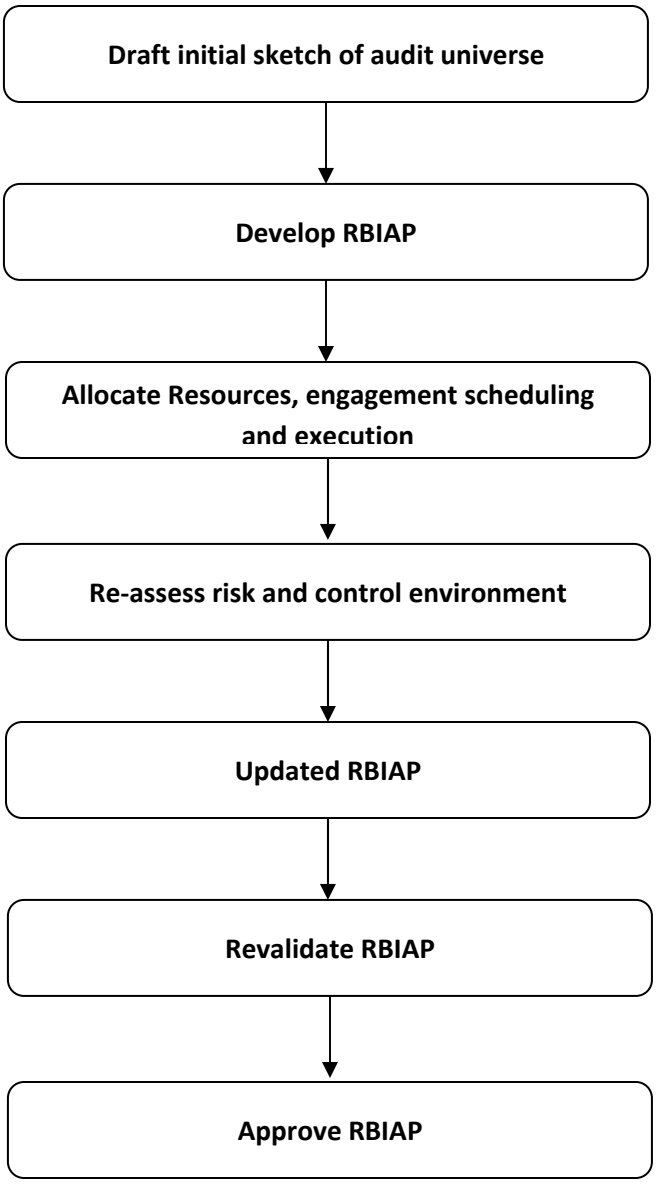
Planning involves developing an overall plan for the expected scope and conduct of audit and developing an audit programme showing the nature, timing and extent of audit procedures. Planning is a continuous exercise. A plan once prepared should be continuously reviewed by the internal auditor to identify any modifications required to bring the same in line with the changes, if any, in the audit environment. However, any major modification to the internal audit plan should be done in consultation with those charged with governance. Further, the internal auditor should also document the changes to the internal audit plan.

Therefore, the preparation of the risk based internal audit plan is based on the defined methodology to be followed and the various steps as described earlier. It is vital to note that the entire exercise of the risk identification, prioritization and development of audit plan is not scientific and some level of judgement and past experience is involved while preparing the risk based internal audit plan. The risk registers prepared should be reviewed periodically and updated while performing the actual internal audit.

5.50 As discussed earlier, risk identification is the process to identify all possible risk in the auditable entities identified at the time of preparation of the audit universe. This includes evaluation of 'what can go wrong' in the particular process attached with the identified auditable entity which can have any adverse impact on the organization. The adverse impact could be in the form of possible financial loss, operational inefficiency and ineffectiveness, statutory non-compliance, incorrect reporting etc. The quality and effectiveness of the risk assessment depends on the comprehensiveness and completeness of the risk identification exercise. The risk identification can be more comprehensive and complete by the exercise of continuous exercise of re-validating the risk along with the audit execution.

The risk based internal audit plan should be evaluated every year by repeating the steps involved in development of risk based internal audit plan to identify if there are some auditable entities for which residual risk score has increased or decreased and that is required to be audited more often, or the same be brought down to the manageable/ acceptable zone to reduce the frequency of internal audit.

Steps for Developing the Audit Universe



Chapter 6
Case Study

Situation

Company is involved in upstream and midstream business of oil and gas with wide spread business across the country having a Corporate Office, Plant Operations and Depots. Internal audit function of the Company comprises of a small team who needs to complete the internal audit for the Company as per the annual charter approved by the Audit Committee of the Company. The IA function is headed by an Internal Audit Head who is reporting to the Audit Committee. Audit Committee directs the IA head to prepare the Risk Based Internal Audit Plan (RBIAP) of the Company for a period of 3 years.

Solution

IA head forms a team of 4 members comprising of Accounting and Technical professionals. The team which has follows the following steps to prepare the RBIAP:

(a) Define objective, criteria and risk appetite

(b) Understanding the business environment and processes

(c) Prepare audit universe

(d) Risk identification

(e) Risk prioritization and rating

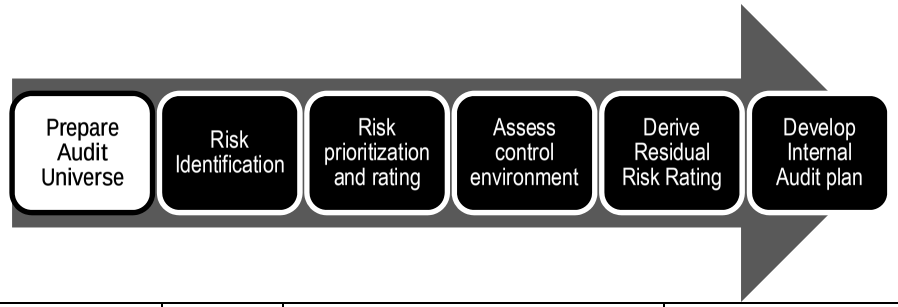
(f) Assess control environment

(g) Derive residual risk rating

(h) Develop internal audit plan

Steps (a) and (b) equips the team with the relevant knowledge and information required for the purpose of developing the RBIAP (Refer Chapter 5 for steps). The illustrative deliverables of the steps (c) to (h) are summarized below:

Step 1: Prepare Audit Universe



D. Sr. no.	Department	P. Sr. No.	Process	Business Locations		
				Corporate Office	Plant	Depot
1	Contracts	1.1	Tendering and RFQ	✔		
1	Contracts	1.2	Contracting and Ordering	✔	✔	
2	Plant Operations	2.1	Production and Distribution		✔	
2	Plant Operations	2.2	Operation and Maintenance		✔	
2	Plant Operations	2.3	Safety and Environment		✔	
3	Drilling	3.1	Drilling		✔	

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations		
				Corporate Office	Plant	Depot
4	Information Technology	4.1	IT Security	✓	✓	
4	Information Technology	4.2	ERP and other applications	✓		
5	Geology & Reservoir	5.1	Geology & Reservoir		✓	
6	Research and Development	6.1	Research and Development		✓	
7	Material Management	7.1	MM - Planning & Receiving		✓	
7	Material Management	7.2	MM - Depot		✓	✓
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓
8	Well Logging	8.1	Well Logging		✓	
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓		
9	Finance and Accounts	9.2	Treasury	✓		
9	Finance and Accounts	9.3	Financial Reporting	✓	✓	
9	Finance and Accounts	9.4	Asset Management		✓	
9	Finance and Accounts	9.5	Payables		✓	
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓	
9	Finance and Accounts	9.7	JV Operations	✓		

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations		
				Corporate Office	Plant	Depot
9	Finance and Accounts	9.8	Taxation		✓	
10	Human Resource	10.1	Recruitment		✓	
10	Human Resource	10.2	Learning and Development		✓	
10	Human Resource	10.3	Separations		✓	
10	Human Resource	10.4	Payroll Process		✓	
11	Projects	11.1	Planning and Investment	✓		
11	Projects	11.2	Execution and handover		✓	
12	Business Development	12.1	Business Development	✓		
13	Exploration & Development	13.1	Exploration & Development		✓	
14	Maintenance	14.1	Pipeline Maintenance		✓	
14	Maintenance	14.2	Equipment Maintenance		✓	

Step 2: Risk Identification

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
1	Contracts	1.1	Tendering and RFQ	✔			Procurement beyond the defined budgetary limits.	Financial
1	Contracts	1.1	Tendering and RFQ	✔			Inadequate vendor selection due to non-compliance to procurement policies and procedures (incl. tendering)	Financial
1	Contracts	1.1	Tendering and RFQ	✔			Increased cost of procurement due to ineffective negotiation/	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							comparison of commercial bid submitted	
1	Contracts	1.1	Tendering and RFQ	✔			Unfavourable RFQ terms and conditions.	Financial
1	Contracts	1.1	Tendering and RFQ	✔			Risk of favoritism to vendor.	Financial
1	Contracts	1.1	Tendering and RFQ	✔			Inappropriate technical evaluation procedures.	Financial
1	Contracts	1.1	Tendering and RFQ	✔			Inadequate procedures for procurement in case of proprietary items.	Financial
1	Contracts	1.1	Tendering and RFQ	✔			Fictitious vendors in the system	Financial
1	Contracts	1.2	Contracting and Ordering	✔			Contract terms and conditions not favourable to the Company	Financial
1	Contracts	1.2	Contracting and Ordering	✔			Delay in contracting or ordering	Operational
1	Contracts	1.2	Contracting	✔			Risk of issue of	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
			and Ordering				unauthorised order.	
1	Contracts	1.2	Contracting and Ordering	✓			Inadequate contract compliance procedures.	Operational
1	Contracts	1.2	Contracting and Ordering	✓			Work started before completion of contracting procedures.	Operational
2	Plant Operations	2.1	Production and Distribution		✓		Regular updation and review of the actual production against the planned production not done.	Financial
2	Plant Operations	2.1	Production and Distribution		✓		Production levels may not have been monitored regularly on a Central Tank Farm (CTF), GGS and well-wise basis for the level of oil production	Financial
2	Plant Operations	2.1	Production and		✓		Production targets are not being communicated	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
			Distribution				and monitored by the Group Gathering Stations (GGS).	
2	Plant Operations	2.1	Production and Distribution		✔		Crude Oil pilferages / leakages while transportation	Financial
2	Plant Operations	2.1	Production and Distribution		✔		Incorrect certification of bills	Financial
2	Plant Operations	2.1	Production and Distribution		✔		Inadequate testing of material used leading to well issues later affecting production	Financial
2	Plant Operations	2.1	Production and Distribution		✔		Non-utilization of the assets	Financial
2	Plant Operations	2.1	Production and Distribution		✔		Inadequate fire safety arrangement at site	Health, Safety & Environment
2	Plant	2.1	Production and		✔		Wrong financial reporting due to inadequate	Incorrect Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
	Operations		Distribution				controls on production recording	Reporting
2	Plant Operations	2.1	Production and Distribution		✓		Inadequate QA / QC during process Production	Financial Loss
2	Plant Operations	2.1	Production and Distribution		✓		Production loss due to inadequate breakdown analysis and compliance	Financial Loss
2	Plant Operations	2.2	Operation and Maintenance		✓		Scheduled maintenance and work over operations for various wells not planned in advance.	Operational
2	Plant Operations	2.2	Operation and Maintenance		✓		Track of total amount of water pumped into each well is not being tracked causing over pumping of water.	Operational
2	Plant Operations	2.2	Operation and Maintenance		✓		Appropriate records are not being maintained in respect of the collection of oil and gas from the	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							wells	
2	Plant Operations	2.2	Operation and Maintenance		✔		Flow meters at CTF are not properly calibrated and the calibration is not being periodically checked. Pumping records of the extent of oil pumped to the customer are not properly kept and maintained.	Operational
2	Plant Operations	2.2	Operation and Maintenance		✔		Production failure/ loss due to inadequate preventive maintenance schedule or lack of compliance of schedule.	Financial Loss
2	Plant Operations	2.2	Operation and Maintenance		✔		Delays in maintenance	Financial Loss
2	Plant Operations	2.3	Safety and Environment		✔		Regular visits of the oil well are not conducted	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							and all oil well installations are not being inspected	
2	Plant Operations	2.3	Safety and Environment		✓		HSE non-compliances by contractors	Statutory Non compliance
3	Drilling	3.1	Drilling		✓		The cost benefit analysis for drilling not done resulting into excess cost of operations.	Financial
3	Drilling	3.1	Drilling		✓		Risk of accidents due to inadequate training and mis-handling.	Health, Safety and Environment
3	Drilling	3.1	Drilling		✓		Inadequate HSE compliance at the drilling sites.	Health, Safety and Environment
3	Drilling	3.1	Drilling		✓		Damage to the equipment due to inadequate security at the drilling site.	Financial
3	Drilling	3.1	Drilling		✓		Sub-optimal utilization of rigs and other drilling	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							equipment.	
3	Drilling	3.1	Drilling		✔		Delays in operation due to inadequate co-ordination and delays in equipment availability.	Operational
3	Drilling	3.1	Drilling		✔		Mis-alignment of the drilling plan with the overall work program	Financial
3	Drilling	3.1	Drilling		✔		Wrong financial reporting due to inappropriate inputs for cost allocation process, well cost reconciliation process	Reporting
3	Drilling	3.1	Drilling		✔		Lack of planning and monitoring of cost and effort involved in drilling of wells (recording and monitoring against KPIs / Targets)	Financial
3	Drilling	3.1	Drilling		✔		Ineffective/ Inefficient functioning of the process	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							due to non-compliance to policies and procedures defined	
4	Information Technology	4.1	IT Security	✓	✓		Unauthorized system access due to weak logical access control rights, password controls, etc.	Operational
4	Information Technology	4.1	IT Security	✓	✓		Inadequate environment controls.	Operational
4	Information Technology	4.1	IT Security	✓	✓		Inadequate access controls to data centre.	Operational
4	Information Technology	4.1	IT Security	✓	✓		Unauthorised access to data centre.	Operational
4	Information Technology	4.1	IT Security	✓	✓		Penal consequences due to usage on unlicensed softwares.	Financial Loss
4	Information Technology	4.1	IT Security	✓	✓		Disaster recovery policy and procedures to identify critical business applications/ data not	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							defined	
4	Information Technology	4.1	IT Security	✔	✔		Increased vulnerability of the network to intrusions - external or internal.	Financial Loss
4	Information Technology	4.1	IT Security	✔	✔		Leakage/ loss of sensitive information/ corrupted and insecure data	Financial Loss
4	Information Technology	4.2	ERP and other applications	✔			Corrupt/ loss of data due to inadequate configuration and logical controls within SAP	Incorrect Financial Reporting
4	Information Technology	4.2	ERP and other applications	✔			Unauthorized transactions due to inadequate segregation of duties	Financial Loss
4	Information Technology	4.2	ERP and other applications	✔			Inaccurate master data due to inadequate controls on master data maintenance and changes	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
4	Information Technology	4.2	ERP and other applications	✔			Absence of an audit trail in case of unauthorized access / users.	Financial Loss
4	Information Technology	4.2	ERP and other applications	✔			Inadequate system logic controls to prevent unauthorized/ incorrect transaction processing through SAP.	Financial Loss
4	Information Technology	4.2	ERP and other applications	✔			Inadequate user management	Financial Loss
4	Information Technology	4.2	ERP and other applications	✔			Access and ID of the separated employees not removed.	Financial Loss
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Existing work being done within the department is not backed up by a physical plan.	Operational
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Proper procedure do not exists or are not followed while deciding the type of	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							survey (2D, 3D or 4D survey).	
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Cost report not prepared	Financial
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Surveys done are not properly recorded.	Operational
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Adequate physical security does not exist of the recorded data	Health, Safety and Environment
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Unavailability of adequate technical data used for proposing exploratory locations	Operational
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Inability to optimize/ actualize expected returns from exploration blocks	Financial Loss
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Delays in monitoring the reserves	Financial Loss
5	Geology &	5.1	Geology &		✔		Inaccurate estimation of	Incorrect

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
	Reservoir		Reservoir				reserves	Financial Reporting
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Incorrect interpretation due to no quality review process of validating the interpretation workflow / cycle followed	Financial Loss
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Delay in seismic data processing due to ineffective scheduling	Financial Loss
6	Research and Development	6.1	Research and Development		✓		Inadequate calibration of R&D tools and equipments causing incorrect results.	Financial Loss
6	Research and Development	6.1	Research and Development		✓		High cost of operation due to obsolete technology.	Financial Loss
6	Research and Development	6.1	Research and Development		✓		Delay in procurement of lab equipments causing delay in completion of R&D activities	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
7	Material Management	7.1	MM - Planning & Receiving		✔		Risk of receiving more than the ordered quantity	Financial
7	Material Management	7.1	MM - Planning & Receiving		✔		Risk of accepting the inferior quality of material	Financial
7	Material Management	7.1	MM - Planning & Receiving		✔		Proper quality assurance testing of all raw materials is not done when it is received.	Financial
7	Material Management	7.2	MM - Depot		✔	✔	Unauthorized disposal of scrap	Financial Loss
7	Material Management	7.2	MM - Depot		✔	✔	Inadequate segregation of duties between personnel responsible for ordering, receiving and issue of material	Financial Loss
7	Material Management	7.2	MM - Depot		✔	✔	Inventory loss due to weak storage/ stacking and segregation guidelines.	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
7	Material Management	7.2	MM - Depot		✓	✓	Financial loss due to inadequate security procedures at the warehouse	Financial Loss
7	Material Management	7.2	MM - Depot		✓	✓	Loss of life/ resources due to non-compliance to regulatory laws and regulations	Health, Safety & Environment
7	Material Management	7.2	MM - Depot		✓	✓	Delay in renewal or expiry of various licenses	Statutory Non compliance
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	Unauthorized and inappropriate indenting	Financial Loss
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	Inadequate monitoring of slow/ non-moving inventory	Financial Loss
7	Material Management	7.3	MM - Inventory Handling		✓	✓	Damage to spares and material due to inadequate storage.	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
			and Storage					
7	Material Management	7.3	MM - Inventory Handling and Storage		✔	✔	Critical spares not identified and maintained	Financial Loss
7	Material Management	7.3	MM - Inventory Handling and Storage		✔	✔	Unauthorised issue of material	Financial Loss
8	Well Logging	8.1	Well Logging		✔		Absence of monitoring of the time taken to interpret the data given to the interpretation team and review the records maintained in this respect to ascertain major delays.	Operational
8	Well Logging	8.1	Well Logging		✔		Inadequate records maintained to document discussions and conclusions of interpretation team.	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
8	Well Logging	8.1	Well Logging		✓		Database/ information not maintained about unsuccessful wells and the same is used during subsequent decisions.	Operational
8	Well Logging	8.1	Well Logging	✓	✓		Existing work being done within the Department is not backed up by a plan.	Operational
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			Delays in preparation and communication of annual plans.	Operational
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			Inappropriate basis and inputs for planning	Operational
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			Management Information System inadequately aligned with strategic objectives	Incorrect Financial Reporting
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			Delays in financial reporting and closing	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
9	Finance and Accounts	9.2	Treasury	✔			Adverse fluctuation in foreign exchange rates	Financial Loss
9	Finance and Accounts	9.2	Treasury	✔			Inadequate working capital management	Financial Loss
9	Finance and Accounts	9.2	Treasury	✔			Inadequate monitoring of cash and bank balances	Financial Loss
9	Finance and Accounts	9.3	Financial Reporting	✔	✔		Inadequate financial reporting systems	Incorrect Financial Reporting
9	Finance and Accounts	9.3	Financial Reporting	✔	✔		Mis-representation in financial statements and reports	Incorrect Financial Reporting
9	Finance and Accounts	9.4	Asset Management		✔		Incorrect capitalization of assets	Incorrect Financial Reporting
9	Finance and Accounts	9.4	Asset Management		✔		Physical verification of assets not done	Incorrect Financial Reporting
9	Finance and Accounts	9.4	Asset Management		✔		Depreciation & Depletion charges have not been	Incorrect Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							accurately calculated and recorded in the appropriate period.	Reporting
9	Finance and Accounts	9.5	Payables		✓		Risk of delay in invoice processing	Financial
9	Finance and Accounts	9.5	Payables		✓		Duplicate vendor codes	Financial
9	Finance and Accounts	9.5	Payables		✓		Risk of delay in payment processing	Financial
9	Finance and Accounts	9.5	Payables		✓		Royalty not paid as specified in Production Sharing Contract.	Financial
9	Finance and Accounts	9.5	Payables		✓		Risk of excess payment	Financial
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		The accounting policies for accounting of sales especially take or pay, underlifts/ overlifts, contractual liabilities etc. not in compliance with	Reporting

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							the Accounting Standards.	
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Delay in invoicing.	Financial
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Incorrect and unauthorised invoicing.	Financial
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Quantitative reconciliation not done to identify excessive losses.	Financial
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Royalty not paid as specified Production Sharing Contract.	Financial
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Inaccurate calculations of the wellhead value.	Financial
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Investment multiple not calculated in the manner as provided in the	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
							Production Sharing Contract.	
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		Inadequate monitoring of receivable and follow up for collections.	Financial
9	Finance and Accounts	9.7	JV Operations	✓			Inaccurate working of cost allocated by operating partners for JV Non Operated	Incorrect Financial Reporting
9	Finance and Accounts	9.7	JV Operations	✓			Non raising/ delayed recovery of cash call from JV partner.	Financial Loss
9	Finance and Accounts	9.7	JV Operations	✓			Wrong allocations to JV due to inadequate process of costing and identification of allocable costs.	Financial Loss
9	Finance and Accounts	9.7	JV Operations	✓			Inadequate control over expenses in case of non operating blocks	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
9	Finance and Accounts	9.8	Taxation		✔		Risk of regulatory penalties due to non compliance with TDS, Service Tax and other relevant acts	Risk of Regulatory Non-Compliance
9	Finance and Accounts	9.8	Taxation		✔		Tax payments and tax returns are not made or filed within permissible time limits	Statutory Non compliance
9	Finance and Accounts	9.8	Taxation		✔		Inadequate monitoring mechanism for pending demands or assessment cases, etc.	Financial Loss
10	Human Resource	10.1	Recruitment		✔		Delay in hiring impacting operation delays	Operational
10	Human Resource	10.1	Recruitment		✔		Hiring inappropriate personnel	Operational
10	Human Resource	10.1	Recruitment		✔		Incomplete documentation in employee records/ files	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
10	Human Resource	10.1	Recruitment		✓		Inadequate background and reference checks	Operational
10	Human Resource	10.2	Learning and Development		✓		Inadequate planning of training requirements	Operational
10	Human Resource	10.2	Learning and Development		✓		Training needs not identified	Operational
10	Human Resource	10.2	Learning and Development		✓		Training programs not conducted in timely manner	Operational
10	Human Resource	10.2	Learning and Development		✓		Feedback procedures not established	Operational
10	Human Resource	10.3	Separations		✓		Delay in Full and Final	Financial
10	Human Resource	10.3	Separations		✓		Inadequate clearance procedures	Financial
10	Human Resource	10.3	Separations		✓		Inadequate waivers	Financial
10	Human Resource	10.3	Separations		✓		Old loan and advances not settled before releiving.	Financial

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
10	Human Resource	10.3	Separations		✓		Exit formalities not completed in timely manner.	Operational
10	Human Resource	10.4	Payroll Process		✓		Incorrect processing of salary	Financial Loss
10	Human Resource	10.4	Payroll Process		✓		Incorrect processing and settlement of various employee claims	Financial Loss
10	Human Resource	10.4	Payroll Process		✓		Incorrect attendance monitoring and accounting of leaves.	Financial Loss
10	Human Resource	10.4	Payroll Process		✓		Incorrect provisioning and accounting of retirement funds management by the company.	Financial Loss
10	Human Resource	10.4	Payroll Process		✓		Delay in disbursement/ transfer of salary.	Financial Loss
11	Projects	11.1	Planning and Investment	✓			Inadequate planning and budgeting of Projects	Financial Loss

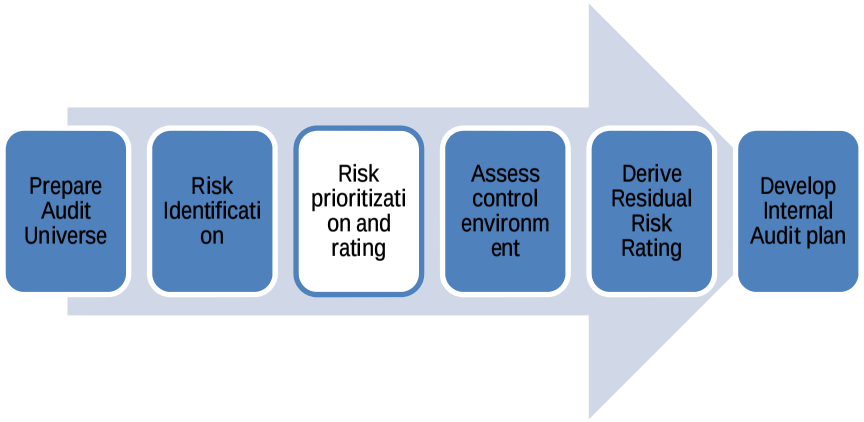
D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
11	Projects	11.1	Planning and Investment	✓			Appropriate feasibility studies not conducted	Financial
11	Projects	11.1	Planning and Investment	✓			Required clearances not obtaining on timely basis	Compliance
11	Projects	11.1	Planning and Investment	✓			Inadequate assessment of Return on Investments	Financial
11	Projects	11.2	Execution and handover		✓		Time and Cost overruns in the projects due to weak project monitoring and/ or execution.	Financial Loss
11	Projects	11.2	Execution and handover		✓		Operational delays due to delay in obtaining/ renewal of statutory clearances	Financial Loss
11	Projects	11.2	Execution and handover		✓		Non compliance to various statutory provisions and requirements.	Statutory Non compliance

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
11	Projects	11.2	Execution and handover		✓		Delay in procurement/ ordering.	Financial Loss
11	Projects	11.2	Execution and handover		✓		Commissioning without adequate quality checks and testing procedures	Financial Loss
11	Projects	11.2	Execution and handover		✓		Lack of monitoring of HSE compliance by contractors / internal staff during execution	Health, Safety & Environment
12	Business Development	12.1	Business Development	✓			Inadequate post acquisition techno-commercial review for overseas acquisitions	Financial Loss
12	Business Development	12.1	Business Development	✓			Delays in floating of Tenders	Financial Loss
12	Business Development	12.1	Business Development	✓			Financial health check up analysis not performed for acquired assets	Financial Loss

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
13	Exploration & development	13.1	Exploration & development		✓		Inability to optimize/ actualize expected returns from exploration blocks	Financial Loss
13	Exploration & development	13.1	Exploration & development		✓		Non fulfillment to minimum work program specially with respect to timeliness	Financial Loss
14	Maintenance	14.1	Pipeline Maintenance		✓		All Flow lines are not being regularly tested and inspected for any blockage	Operational
14	Maintenance	14.1	Pipeline Maintenance		✓		Delays in providing maintenance services impacting operational efficiency.	Financial Loss
14	Maintenance	14.1	Pipeline Maintenance		✓		Inadequate planning of maintenance activities	Operational
14	Maintenance	14.1	Pipeline Maintenance		✓		Preventive maintenance not carried on timely basis.	Operational

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category
				Corporate Office	Plant	Depot		
14	Maintenance	14.1	Pipeline Maintenance		✔		Inadequate training to manpower	Financial Loss
14	Maintenance	14.1	Pipeline Maintenance		✔		Safety risk of working in running pipelines	Health, Safety & Environment
14	Maintenance	14.2	Equipment Maintenance		✔		Delays in providing maintenance services impacting operational efficiency.	Financial Loss
14	Maintenance	14.2	Equipment Maintenance		✔		Inadequate planning of maintenance activities	Operational
14	Maintenance	14.2	Equipment Maintenance		✔		Preventive maintenance not carried on timely basis.	Operational
14	Maintenance	14.2	Equipment Maintenance		✔		Inadequate training to manpower	Financial Loss
14	Maintenance	14.2	Equipment Maintenance				Safety risk of working in running pipelines	Health, Safety & Environment
14	Maintenance	14.2	Equipment Maintenance				Frequent breakdowns due to non-performance of root cause analysis	Financial Loss

Step 3: Risk Prioritization and Rating



(a) Assign Risk Score to each of the risk identified under risk identification

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
1	Contracts	1.1	Tendering and RFQ	✔			Procurement beyond the defined budgetary limits.	Financial	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
1	Contracts	1.1	Tendering and RFQ	✓			Inadequate vendor selection due to non-compliance to procurement policies and procedures (incl. tendering)	Financial	5
1	Contracts	1.1	Tendering and RFQ	✓			Increased cost of procurement due to ineffective negotiation/ comparison of commercial bid submitted	Financial	4
1	Contracts	1.1	Tendering and RFQ	✓			Unfavourable RFQ terms and conditions.	Financial	5
1	Contracts	1.1	Tendering and RFQ	✓			Risk of favoritism to vendor.	Financial	5
1	Contracts	1.1	Tendering and RFQ	✓			Inappropriate technical evaluation procedures.	Financial	4
1	Contracts	1.1	Tendering and RFQ	✓			Inadequate procedures for procurement in case of proprietary items.	Financial	2

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
1	Contracts	1.1	Tendering and RFQ	✓			Fictitious vendors in the system	Financial	3
1	Contracts	1.2	Contracting and Ordering	✓			Contract terms and conditions not favourable to the Company	Financial	4
1	Contracts	1.2	Contracting and Ordering	✓			Delay in contracting or ordering	Operational	3
1	Contracts	1.2	Contracting and Ordering	✓			Risk of issue of unauthorised order.	Financial	5
1	Contracts	1.2	Contracting and Ordering	✓			Inadequate contract compliance procedures.	Operational	4
1	Contracts	1.2	Contracting and Ordering	✓			Work started before completion of contracting procedures.	Operational	3
2	Plant Operations	2.1	Production and Distribution		✓		Regular updation and review of the actual production against the planned production not done.	Financial	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
2	Plant Operations	2.1	Production and Distribution		✓		Production levels may not have been monitored regularly on a Central Tank Farm (CTF), GGS and well-wise basis for the level of oil production	Financial	3
2	Plant Operations	2.1	Production and Distribution		✓		Production targets are not being communicated and monitored by the Group Gathering Stations (GGS).	Financial	3
2	Plant Operations	2.1	Production and Distribution		✓		Crude Oil pilferages / leakages while transportation	Financial	4
2	Plant Operations	2.1	Production and Distribution		✓		Incorrect certification of bills	Financial	4
2	Plant Operations	2.1	Production and		✓		Inadequate testing of material used leading to	Financial	5

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
			Distribution				well issues later affecting production		
2	Plant Operations	2.1	Production and Distribution		✓		Non-utilization of the assets	Financial	4
2	Plant Operations	2.1	Production and Distribution		✓		Inadequate fire safety arrangement at site	Health, Safety & Environment	5
2	Plant Operations	2.1	Production and Distribution		✓		Wrong financial reporting due to inadequate controls on production recording	Incorrect Financial Reporting	4
2	Plant Operations	2.1	Production and Distribution		✓		Inadequate QA / QC process during Production	Financial Loss	4
2	Plant Operations	2.1	Production and Distribution		✓		Production loss due to inadequate breakdown analysis and compliance	Financial Loss	4
2	Plant Operations	2.2	Operation and Maintenance		✓		Scheduled maintenance and work	Operational	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							over operations for various wells not planned in advance.		
2	Plant Operations	2.2	Operation and Maintenance		✓		Track of total amount of water pumped into each well is not being tracked causing over pumping of water.	Operational	3
2	Plant Operations	2.2	Operation and Maintenance		✓		Appropriate records are not being maintained in respect of the collection of oil and gas from the wells	Operational	3
2	Plant Operations	2.2	Operation and Maintenance		✓		Flow meters at CTF are not properly calibrated and the calibration is not being periodically checked. Pumping records of the extent of oil pumped to the customer are not	Operational	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							properly kept and maintained.		
2	Plant Operations	2.2	Operation and Maintenance		✓		Production failure/ loss due to inadequate preventive maintenance schedule or lack of compliance of schedule.	Financial Loss	5
2	Plant Operations	2.2	Operation and Maintenance		✓		Delays in maintenance	Financial Loss	4
2	Plant Operations	2.3	Safety and Environment		✓		Regular visits of the oil well are not conducted and all oil well installations are not being inspected	Operational	4
2	Plant Operations	2.3	Safety and Environment		✓		HSE non compliances by contractors	Statutory Non compliance	5
3	Drilling	3.1	Drilling		✓		The cost benefit analysis for drilling not done resulting into	Financial	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							excess cost of operations.		
3	Drilling	3.1	Drilling		✔		Risk of accidents due to inadequate training and mis-handling.	Health, Safety and Environment	5
3	Drilling	3.1	Drilling		✔		Inadequate HSE compliance at the drilling sites.	Health, Safety and Environment	5
3	Drilling	3.1	Drilling		✔		Damage to the equipment due to inadequate security at the drilling site.	Financial	4
3	Drilling	3.1	Drilling		✔		Sub-optimal utilization of rigs and other drilling equipment.	Financial	4
3	Drilling	3.1	Drilling		✔		Delays in operation due to inadequate co-ordination and delays in equipment availability.	Operational	3
3	Drilling	3.1	Drilling		✔		Mis-alignment of the	Financial	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							drilling plan with the overall work program		
3	Drilling	3.1	Drilling		✓		Wrong financial reporting due to inappropriate inputs for cost allocation process, well cost reconciliation process	Reporting	4
3	Drilling	3.1	Drilling		✓		Lack of planning and monitoring of cost & effort involved in drilling of wells (recording and monitoring against KPIs/ Targets)	Financial	3
3	Drilling	3.1	Drilling		✓		Ineffective/ Inefficient functioning of the process due to non-compliance to policies and procedures defined	Financial	3
4	Information Technology	4.1	IT Security	✓	✓		Unauthorized system access due to weak	Operational	5

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							logical access control rights, password controls, etc.		
4	Information Technology	4.1	IT Security	✔	✔		Inadequate environment controls.	Operational	4
4	Information Technology	4.1	IT Security	✔	✔		Inadequate access controls to data centre.	Operational	4
4	Information Technology	4.1	IT Security	✔	✔		Unauthorised access to data centre.	Operational	4
4	Information Technology	4.1	IT Security	✔	✔		Penal consequences due to usage on unlicensed softwares.	Financial Loss	5
4	Information Technology	4.1	IT Security	✔	✔		Disaster recovery policy and procedures to identify critical business applications/ data not defined	Financial Loss	3
4	Information Technology	4.1	IT Security	✔	✔		Increased vulnerability of the network to intrusions - External or Internal.	Financial Loss	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
4	Information Technology	4.1	IT Security	✓	✓		Leakage / loss of sensitive information/ corrupted and insecure data	Financial Loss	4
4	Information Technology	4.2	ERP and other applications	✓			Corrupt/ loss of data due to inadequate configuration and logical controls within SAP	Incorrect Financial Reporting	3
4	Information Technology	4.2	ERP and other applications	✓			Unauthorized transactions due to inadequate segregation of duties	Financial Loss	3
4	Information Technology	4.2	ERP and other applications	✓			Inaccurate master data due to inadequate controls on master data maintenance and changes	Financial Loss	4
4	Information Technology	4.2	ERP and other applications	✓			Absence of an audit trail in case of unauthorized access / users.	Financial Loss	2

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
4	Information Technology	4.2	ERP and other applications	✔			Inadequate system logic controls to prevent unauthorized/ incorrect transaction processing through SAP.	Financial Loss	4
4	Information Technology	4.2	ERP and other applications	✔			Inadequate user management	Financial Loss	4
4	Information Technology	4.2	ERP and other applications	✔			Access and ID of the separated employees not removed.	Financial Loss	4
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Existing work being done within the department is not backed up by a physical plan.	Operational	3
5	Geology & Reservoir	5.1	Geology & Reservoir		✔		Proper procedure do not exists or are not followed while deciding the type of survey (2D, 3D or 4D survey).	Operational	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Cost report not prepared	Financial	3
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Surveys done are not properly recorded.	Operational	3
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Adequate physical security does not exist of the recorded data	Health, Safety and Environment	4
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Unavailability of adequate technical data used for proposing exploratory locations	Operational	4
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Inability to optimize/ actualize expected returns from exploration blocks	Financial Loss	4
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Delays in monitoring the reserves	Financial Loss	3
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Inaccurate estimation of reserves	Incorrect Financial Reporting	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Incorrect interpretation due to no quality review process of validating the interpretation workflow / cycle followed	Financial Loss	5
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		Delay in seismic data processing due to ineffective scheduling	Financial Loss	3
6	Research and Development	6.1	Research and Development		✓		Inadequate calibration of R&D tools and equipments causing incorrect results.	Financial Loss	2
6	Research and Development	6.1	Research and Development		✓		High cost of operation due to obsolete technology.	Financial Loss	3
6	Research and Development	6.1	Research and Development		✓		Delay in procurement of lab equipments causing delay in completion of R&D activities	Financial Loss	2

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
7	Material Management	7.1	MM - Planning & Receiving		✓	✓	Risk of receiving more than the ordered quantity	Financial	3
7	Material Management	7.1	MM - Planning & Receiving		✓	✓	Risk of accepting the inferior quality of material	Financial	3
7	Material Management	7.1	MM - Planning & Receiving		✓	✓	Proper quality assurance testing of all raw materials is not done when it is received.	Financial	4
7	Material Management	7.2	MM - Depot		✓	✓	Unauthorized disposal of scrap	Financial Loss	2
7	Material Management	7.2	MM - Depot		✓	✓	Inadequate segregation of duties between personnel responsible for ordering, receiving and issue of material	Financial Loss	2
7	Material Management	7.2	MM - Depot		✓	✓	Inventory loss due to weak storage/ stacking	Financial Loss	2

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							and segregation guidelines.		
7	Material Management	7.2	MM - Depot		✔	✔	Financial loss due to inadequate security procedures at the warehouse	Financial Loss	2
7	Material Management	7.2	MM - Depot		✔	✔	Loss of life/ resources due to non-compliance to regulatory laws and regulations	Health, Safety & Environment	4
7	Material Management	7.2	MM - Depot		✔	✔	Delay in renewal or expiry of various licenses	Statutory Non compliance	5
7	Material Management	7.3	MM - Inventory Handling and Storage		✔	✔	Unauthorized and inappropriate indenting	Financial Loss	1
7	Material Management	7.3	MM - Inventory Handling and Storage		✔	✔	Inadequate monitoring of slow/ non moving inventory	Financial Loss	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	Damage to spares and material due to inadequate storage.	Financial Loss	4
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	Critical spares not identified and maintained	Financial Loss	4
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	Unauthorised issue of material	Financial Loss	3
8	Well Logging	8.1	Well Logging		✓		Absence of monitoring of the time taken to interpret the data given to the interpretation team and review the records maintained in this respect to ascertain major delays.	Operational	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
8	Well Logging	8.1	Well Logging		✔		Inadequate records maintained to document discussions and conclusions of interpretation team.	Operational	3
8	Well Logging	8.1	Well Logging		✔		Database/ information not maintained about unsuccessful wells and the same is used during subsequent decisions.	Operational	3
8	Well Logging	8.1	Well Logging		✔		Existing work being done within the Department is not backed up by a plan.	Operational	3
9	Finance and Accounts	9.1	Financial Planning and Analysis	✔			Delays in preparation and communication of annual plans.	Operational	3
9	Finance and Accounts	9.1	Financial Planning and Analysis	✔			Inappropriate basis and inputs for planning	Operational	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			Management System Information inadequately aligned with strategic objectives	Incorrect Financial Reporting	3
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			Delays in financial reporting and closing	Operational	4
9	Finance and Accounts	9.2	Treasury	✓			Adverse fluctuation in foreign exchange rates	Financial Loss	4
9	Finance and Accounts	9.2	Treasury	✓			Inadequate working capital management	Financial Loss	5
9	Finance and Accounts	9.2	Treasury	✓			Inadequate monitoring of cash and bank balances	Financial Loss	3
9	Finance and Accounts	9.3	Financial Reporting	✓	✓		Inadequate financial reporting systems	Incorrect Financial Reporting	4
9	Finance and Accounts	9.3	Financial Reporting		✓		Mis-representation in financial statements and reports	Incorrect Financial Reporting	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
9	Finance and Accounts	9.4	Asset Management		✓		Incorrect capitalization of assets	Incorrect Financial Reporting	4
9	Finance and Accounts	9.4	Asset Management		✓		Physical verification of assets not done	Incorrect Financial Reporting	4
9	Finance and Accounts	9.4	Asset Management		✓		Depreciation & Depletion charges have not been accurately calculated and recorded in the appropriate period.	Incorrect Financial Reporting	4
9	Finance and Accounts	9.5	Payables		✓		Risk of delay in invoice processing	Financial	3
9	Finance and Accounts	9.5	Payables		✓		Duplicate vendor codes	Financial	4
9	Finance and Accounts	9.5	Payables		✓		Risk of delay in payment processing	Financial	3
9	Finance and Accounts	9.5	Payables		✓		Royalty not paid as specified in Production Sharing Contract.	Financial	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
9	Finance and Accounts	9.5	Payables		✓		Risk of excess payment	Financial	4
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		The accounting policies for accounting of sales especially take or pay, underlifts/ overlifts, contractual liabilities etc. not in compliance with the Accounting Standards.	Reporting	3
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		Delay in invoicing.	Financial	3
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		Incorrect and unauthorised invoicing.	Financial	4
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		Quantitative reconciliation not done to identify excessive losses.	Financial	4
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		Royalty not paid as specified Production Sharing Contract.	Financial	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Inaccurate calculations of the wellhead value.	Financial	4
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Investment multiple not calculated in the manner as provided in the Production Sharing Contract.	Financial	4
9	Finance and Accounts	9.6	Invoicing and Receivables	✔	✔		Inadequate monitoring of receivable and follow up for collections.	Financial	3
9	Finance and Accounts	9.7	JV Operations	✔			Inaccurate working of cost allocated by operating partners for JV Non Operated	Incorrect Financial Reporting	4
9	Finance and Accounts	9.7	JV Operations	✔			Non raising/ delayed recovery of cash call from JV partner.	Financial Loss	4
9	Finance and Accounts	9.7	JV Operations	✔			Wrong allocations to JV due to inadequate process of costing and	Financial Loss	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							identification of allocable costs.		
9	Finance and Accounts	9.7	JV Operations	✓			Inadequate control over expenses in case of non operating blocks	Financial Loss	4
9	Finance and Accounts	9.8	Taxation		✓		Risk of regulatory penalties due to non compliance with TDS, Service Tax and other relevant acts	Risk of Regulatory Non-Compliance	4
9	Finance and Accounts	9.8	Taxation		✓		Tax payments and tax returns are not made / filed within permissible time limits	Statutory Non compliance	4
9	Finance and Accounts	9.8	Taxation		✓		Inadequate monitoring mechanism for pending demands / assessment cases, etc.	Financial Loss	4
10	Human Resource	10.1	Recruitment		✓		Delay in hiring impacting operation delays	Operational	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
10	Human Resource	10.1	Recruitment		✔		Hiring inappropriate personnel	Operational	4
10	Human Resource	10.1	Recruitment		✔		Incomplete documentation in employee records/ files	Operational	2
10	Human Resource	10.1	Recruitment		✔		Inadequate background and reference checks	Operational	3
10	Human Resource	10.2	Learning and Development		✔		Inadequate planning of training requirements	Operational	4
10	Human Resource	10.2	Learning and Development		✔		Training needs not identified	Operational	4
10	Human Resource	10.2	Learning and Development		✔		Training programs not conducted in timely manner	Operational	4
10	Human Resource	10.2	Learning and Development		✔		Feedback procedures not established	Operational	3
10	Human Resource	10.3	Separations		✔		Delay in Full and Final	Financial	3
10	Human Resource	10.3	Separations		✔		Inadequate clearance procedures	Financial	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
10	Human Resource	10.3	Separations		✓		Inadequate waivers	Financial	3
10	Human Resource	10.3	Separations		✓		Old loan and advances not settled before relieving.	Financial	3
10	Human Resource	10.3	Separations		✓		Exit formalities not completed timely manner.	Operational	3
10	Human Resource	10.4	Payroll Process		✓		Incorrect processing of salary	Financial Loss	4
10	Human Resource	10.4	Payroll Process		✓		Incorrect processing and settlement of various employee claims	Financial Loss	4
10	Human Resource	10.4	Payroll Process		✓		Incorrect attendance monitoring and accounting of leaves.	Financial Loss	3
10	Human Resource	10.4	Payroll Process		✓		Incorrect provisioning and accounting of retirement funds	Financial Loss	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							management by the company.		
10	Human Resource	10.4	Payroll Process		✔		Delay in disbursement/ transfer of salary.	Financial Loss	3
11	Projects	11.1	Planning and Investment	✔			Inadequate planning and budgeting of Projects	Financial Loss	4
11	Projects	11.1	Planning and Investment	✔			Appropriate feasibility studies not conducted	Financial	5
11	Projects	11.1	Planning and Investment	✔			Required clearances not obtaining on timely basis	Compliance	5
11	Projects	11.1	Planning and Investment	✔			Inadequate assessment of Return on Investments	Financial	4
11	Projects	11.2	Execution and handover		✔		Time and Cost overruns in the projects due to weak project monitoring and/ or execution.	Financial Loss	4
11	Projects	11.2	Execution and handover		✔		Operational delays due to delay in obtaining/	Financial Loss	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							renewal of statutory clearances		
11	Projects	11.2	Execution and handover		✓		Non compliance to various statutory provisions and requirements.	Statutory Non compliance	5
11	Projects	11.2	Execution and handover		✓		Delay in procurement/ ordering.	Financial Loss	3
11	Projects	11.2	Execution and handover		✓		Commissioning without adequate quality checks and testing procedures	Financial Loss	4
11	Projects	11.2	Execution and handover		✓		Lack of monitoring of HSE compliance by contractors / internal staff during execution	Health, Safety & Environment	5
12	Business Development	12.1	Business Development	✓			Inadequate post acquisition techno-commercial review for overseas acquisitions	Financial Loss	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
12	Business Development	12.1	Business Development	✔			Delays in floating of Tenders	Financial Loss	2
12	Business Development	12.1	Business Development	✔			Financial health check up analysis not performed for acquired assets	Financial Loss	3
13	Exploration & development	13.1	Exploration & development		✔		Inability to optimize/ actualize expected returns from exploration blocks	Financial Loss	4
13	Exploration & development	13.1	Exploration & development		✔		Non fulfillment to minimum work program specially with respect to timeliness	Financial Loss	3
14	Maintenance	14.1	Pipeline Maintenance		✔		All Flow lines are not being regularly tested and inspected for any blockage	Operational	4
14	Maintenance	14.1	Pipeline Maintenance		✔		Delays in providing maintenance services	Financial Loss	4

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
							impacting operational efficiency.		
14	Maintenance	14.1	Pipeline Maintenance		✓		Inadequate planning of maintenance activities	Operational	3
14	Maintenance	14.1	Pipeline Maintenance		✓		Preventive maintenance not carried on timely basis.	Operational	4
14	Maintenance	14.1	Pipeline Maintenance		✓		Inadequate training to manpower	Financial Loss	3
14	Maintenance	14.1	Pipeline Maintenance		✓		Safety risk of working in running pipelines	Health, Safety & Environment	4
14	Maintenance	14.2	Equipment Maintenance		✓		Delays in providing maintenance services impacting operational efficiency.	Financial Loss	4
14	Maintenance	14.2	Equipment Maintenance		✓		Inadequate planning of maintenance activities	Operational	4
14	Maintenance	14.2	Equipment		✓		Preventive	Operational	3

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Risk Description	Risk Category	Risk Score
				Corporate Office	Plant	Depot			
			Maintenance				maintenance not carried on timely basis.		
14	Maintenance	14.2	Equipment Maintenance		✓		Inadequate training to manpower	Financial Loss	4
14	Maintenance	14.2	Equipment Maintenance		✓		Safety risk of working in running pipelines	Health, Safety & Environment	3
14	Maintenance	14.2	Equipment Maintenance		✓		Frequent breakdowns due to non performance of root cause analysis	Financial Loss	4

Prepare the summarized Risk Register using the arithmetic mean of the Risk Scores assigned to the risk identified under previous step. Also, assign the rationale for providing the risk ratings for each of the audit area

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
1	Contracts	1.1	Tendering and RFQ	✔			4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability
1	Contracts	1.2	Contracting and Ordering	✔			3.80	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability
2	Plant Operations	2.1	Production and Distribution		✔		3.91	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
								• Significant threat to Health, Safety & Environment • Major impact on organizational profitability
2	Plant Operations	2.2	Operation and Maintenance		✓		3.83	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Impact of Major Financial Loss • Significant threat to Health, Safety & Environment
2	Plant Operations	2.3	Safety and Environment		✓		4.50	• Risk of high reputational impact to organization • Non-compliance with major financial penalties and prosecutions. • Impact of High Financial Loss

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
								• Significant threat to Health, Safety & Environment • High impact on organizational profitability
3	Drilling	3.1	Drilling		✓		3.80	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability
4	Information Technology	4.1	IT Security	✓	✓		4.13	• Process risks with critical risk on the organization. • Impact of High Financial Loss • Repeated fraud/ misappropriation with major financial or reputational consequences • Missing IT and ERP systems
4	Information Technology	4.2	ERP and other applications	✓			3.43	• Process risks with major risk on the organization. • Repeated fraud/ misappropriation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
								• Deficient IT and ERP systems
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		3.64	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Major impact on organizational profitability
6	Research and Development	6.1	Research and Development		✓		2.33	• Process risks with tolerable risk on the organization. • Tolerable impact on organizational profitability
7	Material Management	7.1	MM - Planning & Receiving		✓		3.33	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
7	Material Management	7.2	MM - Depot		✓	✓	2.83	• Process risks with tolerable risk on the organization. • Possible threat to Health, Safety & Environment • Possible fraud/ misappropriation • Tolerable impact on organizational profitability
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	3.20	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability
8	Well Logging	8.1	Well Logging		✓		3.00	• Process risks with tolerable risk on the organization. • Tolerable impact on organizational profitability

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			3.50	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Major impact on organizational profitability
9	Finance and Accounts	9.2	Treasury	✓			4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability
9	Finance and Accounts	9.3	Financial Reporting	✓	✓		3.50	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Repeated fraud/ misappropriation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
9	Finance and Accounts	9.4	Asset Management		✓		4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability
9	Finance and Accounts	9.5	Payables		✓		3.40	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Repeated fraud/ misappropriation
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		3.50	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
								organizational profitability
9	Finance and Accounts	9.7	JV Operations	✓			4.00	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability
9	Finance and Accounts	9.8	Taxation		✓		4.00	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Major impact on organizational profitability

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
10	Human Resource	10.1	Recruitment		✓		3.00	• Process risks with tolerable risk on the organization. • Non-compliance with major financial penalties. • Possible fraud/ misappropriation • Tolerable impact on organizational profitability
10	Human Resource	10.2	Learning and Development		✓		3.75	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Significant threat to Health, Safety & Environment
10	Human Resource	10.3	Separations		✓		3.00	• Process risks with tolerable risk on the organization. • Possible fraud/ misappropriation • Tolerable impact on organizational profitability

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
10	Human Resource	10.4	Payroll Process		✔		3.40	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Repeated fraud/ misappropriation
11	Projects	11.1	Planning and Investment	✔			4.50	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization • Non-compliance with major financial penalties and prosecutions. • Impact of High Financial Loss • High impact on organizational profitability
11	Projects	11.2	Execution and handover		✔		4.17	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization • Non-compliance with major

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
								financial penalties and prosecutions. • Impact of High Financial Loss • Significant threat to Health, Safety & Environment • Repeated fraud/ misappropriation with major financial or reputational consequences • High impact on organizational profitability
12	Business Development	12.1	Business Development	✓			2.67	• Impact of significant Financial Loss • Tolerable impact on organizational profitability
13	Exploration & development	13.1	Exploration & development		✓		3.50	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating
				Corporate Office	Plant	Depot		
								• Significant threat to Health, Safety & Environment • Major impact on organizational profitability
14	Maintenance	14.1	Pipeline Maintenance		✓		3.67	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability
14	Maintenance	14.2	Equipment Maintenance		✓		3.67	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability

Step 4: Assess control environment

Assign the control environment rating for each of the identified audit area and provide rational for assigning the control environment ratings.

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
1	Contracts	1.1	Tendering and RFQ	✔			4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriati	4.00	• Preventive or detective controls not identified or defined • Moderate IT

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								on • Major impact on organizational profitability		environment with missing automated controls. • Policy and Procedures not formally defined and there may be possible deviations
1	Contracts	1.2	Contracting and Ordering	✓			3.80	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls.

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								profitability		• Policy and Procedures not formally defined and there may be possible deviations
2	Plant Operations	2.1	Production and Distribution		✓		3.91	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss • Significant threat to Health, Safety	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Defined Policy and Procedures but insufficient

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								& Environment • Major impact on organizational profitability		control on implementation and compliance to same. • Consistent organisation growth with possible losses
2	Plant Operations	2.2	Operation and Maintenance		✓		3.83	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Defined Policy

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								penalties or prosecutions. • Impact of Major Financial Loss • Significant threat to Health, Safety & Environment		and Procedures but insufficient control on implementation and compliance to same. • Consistent Organisation growth with possible losses
2	Plant Operations	2.3	Safety and Environment		✓		4.50	• Risk of high reputational impact to organization • Non-compliance with major financial penalties and prosecutions.	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								• Impact of High Financial Loss • Significant threat to Health, Safety & Environment • High impact on organizational profitability		deviations. • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent Organisation growth with possible losses
3	Drilling	3.1	Drilling		✓		3.80	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact	4.00	• Policy and Procedures not formally defined and there may be possible deviations • Consistent organisation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								on organizational profitability		growth with frequent losses • Inadequate board monitoring and governance structure
4	Information Technology	4.1	IT Security	✓	✓		4.13	• Process risks with critical risk on the organization. • Impact of High Financial Loss • Repeated fraud/ misappropriation with major financial or reputational consequences	2.00	• Defined Preventive or detective control • Established ERP system and IT security measures • Well defined Policy and Procedures and minor deviations

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								• Missing IT and ERP systems		
4	Information Technology	4.2	ERP and other applications	✓			3.43	• Process risks with major risk on the organization. • Repeated fraud/ misappropriation • Deficient IT and ERP systems	2.00	• Defined Preventive or detective control • Established ERP system and IT security measures • Well defined Policy and Procedures and minor deviations
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		3.64	• Process risks with major risk on the organization. • Impact of Major Financial	2.00	• Defined Preventive or detective control • Well defined Policy and Procedures and

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								• Loss • Major impact on organizational profitability		minor deviations • Consistent organisation growth with unlikely losses.
6	Research and Development	6.1	Research and Development		✓		2.33	• Process risks with tolerable risk on the organization. • Tolerable impact on organizational profitability	1.00	• Existence of strong Preventive or detective control with mechanism for continuous monitoring and update the same. • Well established ERP system and IT security measures • Well defined and implemented

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
										Policy and Procedures • Consistent organisation growth with rare surprises
7	Material Management	7.1	MM - Planning & Receiving		✓		3.33	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing automated controls. • Policy and Procedures not defined • Inconsistent organisation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								organizational profitability		growth with major losses • Inadequate decentralisation of decision making
7	Material Management	7.2	MM - Depot		✓	✓	2.83	• Process risks with tolerable risk on the organization. • Possible threat to Health, Safety & Environment • Possible fraud/ misappropriation • Tolerable	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing automated controls. • Policy and Procedures not defined • Inconsistent organisation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								impact on organizational profitability		growth with major losses • Inadequate decentralisation of decision making
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	3.20	• Process risks with major risk on the organization. • Impact of major Financial loss • Repeated fraud/ misappropriation • Major impact on organizational	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing automated controls. • Policy and Procedures not defined • Inconsistent Organisation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								profitability		growth with major losses • Inadequate decentralisation of decision making
8	Well Logging	8.1	Well Logging		✓		3.00	• Process risks with tolerable risk on the organization. • Tolerable impact on organizational profitability	1.00	• Existence of strong preventive or detective control with mechanism for continuous monitoring and update the same. • Well established ERP system and IT security measures • Well defined and

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
										implemented policy and procedures • Consistent organisation growth with rare surprises
9	Finance and Accounts	9.1	Financial Planning and Analysis				3.50	• Process risks with major risk on the organization. • Impact of major financial loss • Major impact on organizational profitability	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Established ERP system and IT

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
										security measures • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent Organisation growth with possible losses
9	Finance and Accounts	9.2	Treasury	✓			4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriation	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Established ERP

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								• Major impact on organizational profitability		system and IT security measures • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent organisation growth with possible losses
9	Finance and Accounts	9.3	Financial Reporting	✓	✓		3.50	• Process risks with major risk on the organization. • Risk of reputational	4.00	• Preventive or detective controls not identified or defined • Missing legal

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								impact to organization • Non-compliance with major financial penalties or prosecutions. • Repeated fraud/ misappropriation		compliance framework with alternative measure to monitor legal compliance. • Moderate IT environment with missing automated controls. • Policy and procedures not formally defined and there may be possible deviations.
9	Finance and Accounts	9.4	Asset Management		✓		4.00	• Impact of major financial loss	4.00	• Preventive or detective controls not

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								• Repeated fraud/ misappropriation • Major impact on organizational profitability		identified or defined • Moderate IT environment with missing automated controls. • Policy and procedures not formally defined and there may be possible deviations • Consistent organisation growth with frequent losses.
9	Finance and Accounts	9.5	Payables		✓		3.40	• Process risks with major risk on the	4.00	• Preventive or detective controls not

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								organization. • Risk of reputational impact to organization • Repeated fraud/ misappropriation		identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined and there may be possible deviations
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		3.50	• Process risks with major risk on the organization. • Risk of reputational impact to	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Established ERP

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								organization • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability		system and IT security measures • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent organisation growth with possible losses
9	Finance and Accounts	9.7	JV Operations	✓			4.00	• Process risks with major risk on the organization. • Risk of reputational	4.00	• Preventive or detective controls not identified or defined • Moderate IT

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								impact to organization • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability		environment with missing automated controls. • Policy and Procedures not formally defined and there may be possible deviations • Consistent Organisation growth with frequent losses • Inadequate board monitoring and governance structure
9	Finance and	9.8	Taxation		✓		4.00	• Process risks	4.00	• Preventive or

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
	Accounts							with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Major impact on organizational profitability		detective controls not identified or defined • Missing Legal compliance framework with alternative measure to monitor legal compliance. • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined and there may

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
										be possible deviations
10	Human Resource	10.1	Recruitment		✓		3.00	• Process risks with tolerable risk on the organization. • Non-compliance with major financial penalties. • Possible fraud/ misappropriation • Tolerable impact on organizational profitability	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined and there may be possible deviations • Consistent organisation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
										growth with frequent losses • Inadequate board monitoring and governance structure
10	Human Resource	10.2	Learning and Development		✓		3.75	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Significant threat to Health, Safety & Environment	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
										and there may be possible deviations • Consistent organisation growth with frequent losses • Inadequate board monitoring and governance structure
10	Human Resource	10.3	Separations		✓		3.00	• Process risks with tolerable risk on the organization. • Possible fraud/ misappropriation • Tolerable	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								impact on organizational profitability		automated controls. • Policy and Procedures not formally defined and there may be possible deviations • Consistent organisation growth with frequent losses • Inadequate board monitoring and governance structure
10	Human Resource	10.4	Payroll Process		✓		3.40	• Process risks with major risk on the	5.00	• Missing preventive or detective

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								organization. • Risk of reputational impact to organization • Repeated fraud/ misappropriation		controls • Insufficient IT environment with missing automated controls. • Policy and Procedures not defined.
11	Projects	11.1	Planning and Investment	✓			4.50	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization • Non-compliance with major	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Defined Policy and Procedures but insufficient control on implementation

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								financial penalties and prosecutions. • Impact of High Financial Loss • High impact on organizational profitability		and compliance to same. • Consistent organisation growth with possible losses
11	Projects	11.2	Execution and handover		✓		4.17	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization • Non-compliance with major financial	4.00	• Preventive or detective controls not identified or defined • Policy and Procedures not formally defined and there may be possible deviations • Consistent

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								penalties and prosecutions. • Impact of High Financial Loss • Significant threat to Health, Safety & Environment • Repeated fraud/ misappropriation with major financial or reputational consequences • High impact on organizational profitability		organisation growth with frequent losses • Inadequate board monitoring and governance structure.
12	Business Development	12.1	Business Development	✓			2.67	• Impact of significant	2.00	• Defined Preventive or

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								Financial Loss • Tolerable impact on organizational profitability		detective control • Well defined Policy and Procedures and minor deviations • Consistent organisation growth with unlikely losses.
13	Exploration & development	13.1	Exploration & development		✓		3.50	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations.

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								• Significant threat to Health, Safety & Environment • Major impact on organizational profitability		• Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent organisation growth with possible losses
14	Maintenance	14.1	Pipeline Maintenance		✓		3.67	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				
								organizational profitability		minor deviations. • Defined Policy and Procedures but insufficient control on implementation and compliance to same.
14	Maintenance	14.2	Equipment Maintenance		✓		3.67	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations.

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating
				Corporate Office	Plant	Depot				• Defined Policy and Procedures but insufficient control on implementation and compliance to same.

Step 5: Derive Residual Risk Rating

Derive Residual Risk Ratings for each of the identified audit area by using the product of Initial Risk Ratings and Control Environment Ratings.

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
1	Contracts	1.1	Tendering and RFQ	✔			4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriati	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								on • Major impact on organizational profitability		with missing automated controls. • Policy and Procedures not formally defined and there may be possible deviations	
1	Contracts	1.2	Contracting and Ordering	✓			3.80	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls.	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								profitability		• Policy and procedures not formally defined and there may be possible deviations	
2	Plant Operations	2.1	Production and Distribution		✓		3.91	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss • Significant threat to	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations.	12.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Health, Safety & Environment • Major impact on organizational profitability		• Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent organisation growth with possible losses	
2	Plant Operations	2.2	Operation and Maintenance		✓		3.83	• Process risks with major risk on the organization. • Risk of	3.00	• Defined Preventive or detective control but unlikely	12.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Impact of Major Financial Loss • Significant threat to Health, Safety & Environment		monitoring and update exercise. • Legal compliance framework with minor deviations. • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent organisation	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										growth with possible losses	
2	Plant Operations	2.3	Safety and Environment		✓		4.50	• Risk of high reputational impact to organization • Non-compliance with major financial penalties and prosecutions. • Impact of High Financial Loss • Significant threat to Health, Safety & Environment	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Defined Policy and Procedures but	14.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• High impact on organizational profitability		insufficient control on implementation and compliance to same. • Consistent Organisation growth with possible losses	
3	Drilling	3.1	Drilling		✓		3.80	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment	4.00	• Policy and Procedures not formally defined and there may be possible deviations • Consistent	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Major impact on organizational profitability		Organisation growth with frequent losses • Inadequate board monitoring and governance structure	
4	Information Technology	4.1	IT Security	✓	✓		4.13	• Process risks with critical risk on the organization. • Impact of High Financial Loss • Repeated fraud/ misappropriati	2.00	• Defined Preventive or detective control • Established ERP system and IT security measures	9.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• on with major financial or reputational consequences • Missing IT and ERP systems		• Well defined Policy and Procedures and minor deviations	
4	Information Technology	4.2	ERP and other applications	✓			3.43	• Process risks with major risk on the organization. • Repeated fraud/ misappropriation • Deficient IT and ERP systems	2.00	• Defined Preventive or detective control • Established ERP system and IT security measures • Well defined Policy and Procedures and minor	7.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		3.64	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Major impact on organizational profitability	2.00	• Defined Preventive or detective control • Well defined Policy and Procedures and minor deviations • Consistent organisation growth with unlikely losses.	8.00
6	Research and Development	6.1	Research and Development		✓		2.33	• Process risks with tolerable risk on the organization. • Tolerable	1.00	• Existence of strong Preventive or detective control with	3.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								impact on organizational profitability		mechanism for continuous monitoring and update the same. • Well established ERP system and IT security measures • Well defined and implemente d Policy and Procedures • Consistent organisation growth with	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										rare surprises	
7	Material Management	7.1	MM - Planning & Receiving		✓		3.33	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing automated controls. • Policy and Procedures not defined • Inconsistent organisation growth with major losses	17.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										• Inadequate decentralisation of decision making	
7	Material Management	7.2	MM - Depot		✓	✓	2.83	• Process risks with tolerable risk on the organization. • Possible threat to Health, Safety & Environment • Possible fraud/ misappropriation • Tolerable impact on	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing automated controls. • Policy and Procedures not defined • Inconsistent organisation	15.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								organizational profitability		growth with major losses • Inadequate decentralisation of decision making	
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	3.20	• Process risks with major risk on the organization. • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing automated controls. • Policy and Procedures	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								on organizational profitability		• not defined • Inconsistent organisation growth with major losses • Inadequate decentralisation of decision making	
8	Well Logging	8.1	Well Logging		✓		3.00	• Process risks with tolerable risk on the organization. • Tolerable impact on organizational profitability	1.00	• Existence of strong Preventive or detective control with mechanism for continuous monitoring	3.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
9	Finance and Accounts	9.1	Financial Planning	✓			3.50	• Process risks with major risk	3.00	• Defined Preventive and update the same. • Well established ERP system and IT security measures • Well defined and implemented Policy and Procedures • Consistent organisation growth with rare surprises	11.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
			and Analysis					on the organization. • Impact of Major Financial Loss • Major impact on organizational profitability		or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Established ERP system and IT security measures • Defined Policy and Procedures but	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										insufficient control on implementation and compliance to same. • Consistent organisation growth with possible losses	
9	Finance and Accounts	9.2	Treasury	✓			4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Established	12.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								organizational profitability			
9	Finance and	9.3	Financial	✓	✓		3.50	• Process risks	4.00	• ERP system and IT security measures • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent organisation growth with possible losses • Preventive	14.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
	Accounts		Reporting					with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Repeated fraud/ misappropriation		or detective controls not identified or defined • Missing Legal compliance framework with alternative measure to monitor legal compliance. • Moderate IT environment with missing automated controls. • Policy and	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										Procedures not formally defined and they may be possible deviations.	
9	Finance and Accounts	9.4	Asset Management		✓		4.00	• Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined and	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										they may be possible deviations • Consistent organisation growth with frequent losses.	
9	Finance and Accounts	9.5	Payables		✓		3.40	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Repeated fraud/ misappropriation	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures	14.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										not formally defined and they may be possible deviations	
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		3.50	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Impact of Major Financial Loss • Repeated fraud/ misappropriation	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Established ERP system and IT security measures • Defined Policy and	11.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Major impact on organizational profitability			
9	Finance and Accounts	9.7	JV Operations	✓			4.00	• Process risks with major risk on the organization. • Risk of reputational impact to	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								organization • Impact of Major Financial Loss • Repeated fraud/ misappropriation • Major impact on organizational profitability		with missing automated controls. • Policy and Procedures not formally defined and they may be possible deviations • Consistent organisation growth with frequent losses • Inadequate board monitoring and governance	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										structure	
9	Finance and Accounts	9.8	Taxation		✓		4.00	• Process risks with major risk on the organization. • Risk of reputational impact to organization • Non-compliance with major financial penalties or prosecutions. • Major impact on organizational profitability	4.00	• Preventive or detective controls not identified or defined • Missing Legal compliance framework with alternative measure to monitor legal compliance. • Moderate IT environment with missing automated	16.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										controls. • Policy and Procedures not formally defined and there may be possible deviations	
10	Human Resource	10.1	Recruitment		✓		3.00	• Process risks with tolerable risk on the organization. • Non-compliance with major financial penalties. • Possible fraud/ misappropriati	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures	12.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Tolerable impact on organizational profitability on		• Consistent organisation growth with frequent losses • Inadequate board monitoring and governance structure	
10	Human Resource	10.2	Learning and Development		✓		3.75	• Process risks with major risk on the organization.	4.00	• Preventive or detective controls not identified or	15.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Risk of reputational impact to organization • Significant threat to Health, Safety & Environment		defined • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined and there may be possible deviations • Consistent organisation growth with frequent losses • Inadequate board	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										monitoring and governance structure	
10	Human Resource	10.3	Separations		✓		3.00	• Process risks with tolerable risk on the organization. • Possible fraud/ misappropriation • Tolerable impact on organizational profitability	4.00	• Preventive or detective controls not identified or defined • Moderate IT environment with missing automated controls. • Policy and Procedures not formally defined and there may be possible	12.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										deviations • Consistent organisation growth with frequent losses • Inadequate board monitoring and governance structure	
10	Human Resource	10.4	Payroll Process		✓		3.40	• Process risks with major risk on the organization. • Risk of reputational impact to organization	5.00	• Missing preventive or detective controls • Insufficient IT environment with missing	17.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Repeated fraud/ misappropriation		automated controls. • Policy and Procedures not defined.	
11	Projects	11.1	Planning and Investment	✓			4.50	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization • Non-compliance with major financial penalties and prosecutions. • Impact of High	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Defined Policy and Procedures but insufficient control on implementat	14.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								• Financial Loss • High impact on organizational profitability		ion and compliance to same. • Consistent organisation growth with possible losses	
11	Projects	11.2	Execution and handover		✓		4.17	• Process risks with critical risk on the organization. • Risk of high reputational impact to organization • Non-compliance with major financial	4.00	• Preventive or detective controls not identified or defined • Policy and Procedures not formally defined and there may be possible deviations	17.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								penalties and prosecutions. • Impact of High Financial Loss • Significant threat to Health, Safety & Environment • Repeated fraud/ misappropriation with major financial or reputational consequences • High impact on organizational profitability		• Consistent Organisation growth with frequent losses • Inadequate board monitoring and governance structure.	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
12	Business Development	12.1	Business Development	✓			2.67	• Impact of significant Financial Loss • Tolerable impact on organizational profitability	2.00	• Defined Preventive or detective control • Well defined Policy and Procedures and minor deviations • Consistent Organisation growth with unlikely losses.	6.00
13	Exploration & development	13.1	Exploration & development		✓		3.50	• Process risks with major risk on the organization. • Risk of reputational	3.00	• Defined Preventive or detective control but unlikely monitoring	11.00

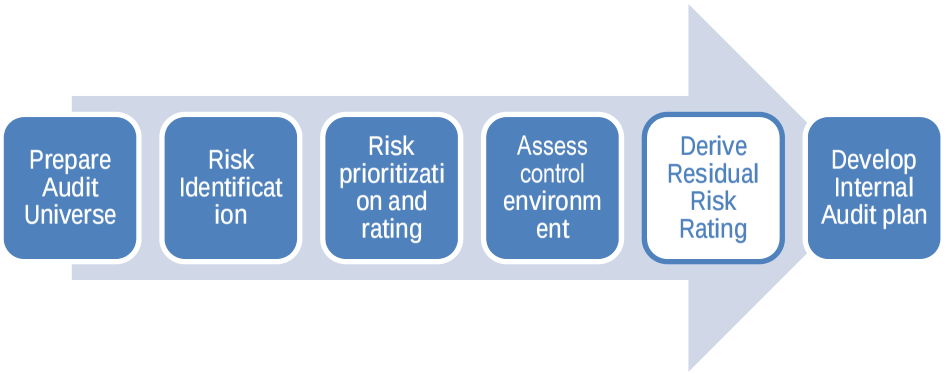
D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
								impact to organization • Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability		and update exercise. • Legal compliance framework with minor deviations. • Defined Policy and Procedures but insufficient control on implementation and compliance to same. • Consistent Organisation growth	

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										with possible losses	
14	Maintenance	14.1	Pipeline Maintenanc e		✓		3.67	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Defined Policy and Procedures but	11.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										insufficient control on implementation and compliance to same.	
14	Maintenance	14.2	Equipment Maintenance		✓		3.67	• Impact of Major Financial Loss • Significant threat to Health, Safety & Environment • Major impact on organizational profitability	3.00	• Defined Preventive or detective control but unlikely monitoring and update exercise. • Legal compliance framework with minor deviations. • Defined	11.00

D. Sr. No.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Rationale for Initial Risk Rating	Control Environ-ment Rating	Rationale for Control Environment Rating	Residual Risk Score (Rounded up)
				Corporate Office	Plant	Depot					
										Policy and Procedures but insufficient control on implementation and compliance to same.	

Step 6: Develop Internal Audit Plan



(a) Arrive at the frequency of the internal audit using the residual risk score calculated in the previous steps. The following definitions could be used for arriving at the frequency of audit in the time span of 3 years.

- High Risk – Audit areas having residual risk score of more than 12 which need to be audited every year.
- Medium Risk - Audit areas having residual risk score of more than or equal to 9 but less than or equal to 12 which need to be audited twice in three years.
- Low Risk - Audit areas having residual risk score of more than or equal to 5 but less than or equal to 8 which need to be audited once in three years.
- Acceptable - Audit areas having residual risk score of less than 5 which could to be audited based on management discretion.

(b) Prepare the annual audit plan by identifying the areas that need to be audit in year 1, year 2 and year 3.

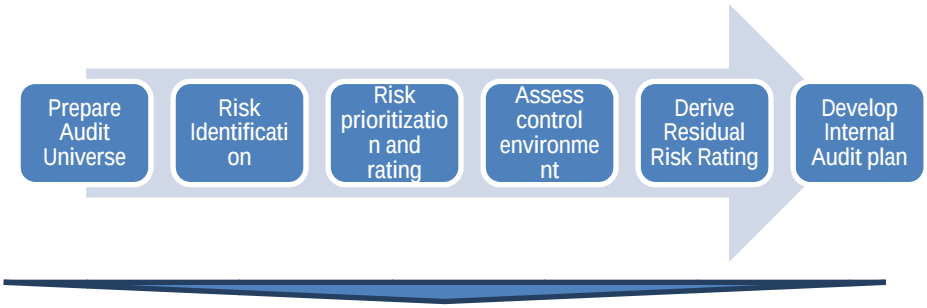
D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Control Environment Rating	Residual Risk Score	Frequency of Audit	Audit Plan Year - 1	Audit Plan Year - 2	Audit Plan Year - 3
				Corporate Office	Plant	Depot							
1	Contracts	1.1	Tendering and RFQ	✓			4.00	4.00	16.00	Every Year	✓	✓	✓
1	Contracts	1.2	Contracting and Ordering	✓	✓		3.80	4.00	16.00	Every Year	✓	✓	✓
2	Plant Operations	2.1	Production and Distribution		✓		3.91	3.00	12.00	Twice in 3 years	✓		
2	Plant Operations	2.2	Operation and Maintenance		✓		3.83	3.00	12.00	Twice in 3 years	✓		
2	Plant Operations	2.3	Safety and Environment		✓		4.50	3.00	14.00	Twice in 3 years	✓		
3	Drilling	3.1	Drilling		✓		3.80	4.00	16.00	Every Year	✓	✓	✓
4	Information Technology	4.1	IT Security	✓	✓		4.13	2.00	9.00	Twice in 3 years	✓	✓	
4	Information Technology	4.2	ERP and other applications	✓			3.43	2.00	7.00	Once in 3 years	✓		

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Control Environment Rating	Residual Risk Score	Frequency of Audit	Audit Plan Year - 1	Audit Plan Year - 2	Audit Plan Year - 3
				Corporate Office	Plant	Depot							
5	Geology & Reservoir	5.1	Geology & Reservoir		✓		3.64	2.00	8.00	Once in 3 years		✓	
6	Research and Development	6.1	Research and Development		✓		2.33	1.00	3.00	Acceptable	✓	✓	✓
7	Material Management	7.1	MM - Planning & Receiving		✓		3.33	5.00	17.00	Every Year	✓	✓	✓
7	Material Management	7.2	MM - Depot		✓	✓	2.83	5.00	15.00	Every Year	✓	✓	✓
7	Material Management	7.3	MM - Inventory Handling and Storage		✓	✓	3.20	5.00	16.00	Every Year	✓	✓	✓
8	Well Logging	8.1	Well Logging		✓		3.00	1.00	3.00	Acceptable	✓	✓	✓
9	Finance and Accounts	9.1	Financial Planning and Analysis	✓			3.50	3.00	11.00	Twice in 3 years	✓		✓
9	Finance and	9.2	Treasury	✓			4.00	3.00	12.00	Twice in 3	✓		✓

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Control Environment Rating	Residual Risk Score	Frequency of Audit	Audit Plan Year - 1	Audit Plan Year - 2	Audit Plan Year - 3
				Corporate Office	Plant	Depot							
	Accounts									years			
9	Finance and Accounts	9.3	Financial Reporting	✓	✓		3.50	4.00	14.00	Twice in 3 years	✓		✓
9	Finance and Accounts	9.4	Asset Management		✓		4.00	4.00	16.00	Every Year	✓	✓	✓
9	Finance and Accounts	9.5	Payables		✓		3.40	4.00	14.00	Twice in 3 years	✓		✓
9	Finance and Accounts	9.6	Invoicing and Receivables	✓	✓		3.50	3.00	11.00	Twice in 3 years	✓		✓
9	Finance and Accounts	9.7	JV Operations	✓	✓		4.00	4.00	16.00	Every Year	✓	✓	✓
9	Finance and Accounts	9.8	Taxation		✓		4.00	4.00	16.00	Every Year	✓	✓	✓
10	Human Resource	10.1	Recruitment		✓		3.00	4.00	12.00	Twice in 3 years		✓	✓
10	Human Resource	10.2	Learning and Development		✓		3.75	4.00	15.00	Every Year	✓	✓	✓

D. Sr. no.	Department	P. Sr. No.	Process	Business Locations			Initial Risk Rating	Control Environment Rating	Residual Risk Score	Frequency of Audit	Audit Plan Year - 1	Audit Plan Year - 2	Audit Plan Year - 3
				Corporate Office	Plant	Depot							
10	Human Resource	10.3	Separations		✓		3.00	4.00	12.00	Twice in 3 years		✓	✓
10	Human Resource	10.4	Payroll Process		✓		3.40	5.00	17.00	Every Year	✓	✓	✓
11	Projects	11.1	Planning and Investment	✓			4.50	3.00	14.00	Twice in 3 years	✓	✓	
11	Projects	11.2	Execution and handover		✓		4.17	4.00	17.00	Every Year	✓	✓	✓
12	Business Development	12.1	Business Development	✓			2.67	2.00	6.00	Once in 3 years			✓
13	Exploration & development	13.1	Exploration & development		✓		3.50	3.00	11.00	Twice in 3 years	✓	✓	
14	Maintenance	14.1	Pipeline Maintenance		✓		3.67	3.00	11.00	Twice in 3 years	✓	✓	
14	Maintenance	14.2	Equipment Maintenance		✓		3.67	3.00	11.00	Twice in 3 years	✓	✓	

Prepare Heat Map – Graphical presentation of the Risk Based Internal Audit Plan



Control Environment Rating			Residual Risk Score 1	2	3	4	5	Control Environment Rating
	Almost Missing	5			MM - Depot	MM - Planning & Receiving MM - Inventory Handling and Storage Human Resource - Payroll Process		5
	Weak	4			Human Resource - Recruitment Human Resource - Separations	Contracts - Tendering and RFQ Contracts - Contracting and Ordering Drilling Finance and Accounts - Asset Management Finance and Accounts - JV Operations Finance and Accounts - Taxation Human Resource - Learning and Development	Projects - Execution and handover	4
	Moderate	3			Finance and Accounts - Invoicing and Receivables	Plant Operations - Production and Distribution Plant Operations - Operation and Maintenance Plant Operations - Safety and Environment Financial Planning and Analysis Treasury Financial Reporting Finance and Accounts - Payables Exploration & development Maintenance - Pipeline Maintenance Maintenance - Equipment Maintenance	Projects - Planning and Investment	3
	Strong	2			Business Development	Information Technology - ERP and other applications Geology & Reservoir	Information Technology - IT Security	2
	Very Strong	1			Research and Development Well Logging			1
			1	2	3	4	5	
			Insignificant	Minor	Moderate	Major	Critical	
			Residual Risk Score					