Technical Guide on Internal Audit of IT Software Industry (2024 Edition)

The Institute of Chartered Accountants of India

(Set up by an Act of Parliament)

New Delhi

Technical Guide on Internal Audit of IT Software Industry

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

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

First Edition	:	February, 2014
Second Edition	:	January, 2024
Committee/Department	:	Board of Internal Audit and Management Accounting
E-mail	:	biama@icai.in
Website	:	www.icai.org/ www.internalaudit.icai.org
Price	:	₹ 165/-
ISBN	:	978-81-8441-681-7
Published by	:	The Publication & CDS Directorate on behalf of The Institute of Chartered Accountants of India ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi – 110 002 (India)
Printed by	:	Sahitya Bhawan Publications, Hospital Road, Agra – 282 003 January | 2024 | P3540 (Revised)

Foreword

Globalization and Liberalisation in India had been one of the key game changers for economic development of the Country and boost for many industries including the software industry. The economic liberalisation of 1991 had paved the way to give impetus to the growth of this sector in India. Over a period, technology has grown by leaps and bounds and so there has been an overhaul of modus-operandi and regulation of the industry as a whole. There also has been evolution of new concepts in the industry which require greater internal control mechanism therefore calling for a robust system of audit so that the inefficiencies can not only be identified but also addressed in a timely manner.

Over the years, the Board of Internal Audit and Management Accounting (BIAMA) of ICAI has been issuing various Technical Guides on Internal Audit for the benefit of the members engaged in various industries. I am happy to note that the BIAMA has revised the Technical Guide on Internal Audit of IT Software Industry. This revised Technical Guide provides a comprehensive guidance in simple and easy to understand language on various issues involved in internal audit of IT Software Industry to assist internal auditors in discharge of their professional responsibilities.

My compliments to CA. Rajendra Kumar P, Chairman, CA. Charanjot Singh Nanda, Vice-Chairman and other members of the Board of Internal Audit and Management Accounting for their sincere efforts in bringing out 'Technical Guide on Internal Audit of IT Software Industry (2024 Edition)' for the benefit of the members.

I am sure that the members and other interested readers would find this Technical Guide useful.

2nd January, 2024
Delhi

CA. Aniket Sunil Talati
President, ICAI

Preface

Indian IT Software industry is leading industry and has been progressively contributing to the growth of economy by handling major portion of exports and creation of employment opportunities. Young and skilled talent pool with strong entrepreneurial mindset, excellent physical and digital infrastructure, vibrant domestic market, and strong Government support are base for development of this industry.

This unique sector faces complexity of processes which give rise to a spectrum of strategic, economic, operational, compliance, disaster, political, human capital and reputational risks. Internal auditors can play an important role in governance, risk and compliance aspects, which are essential to ensure that the IT Software industry remains on the growth path.

The Board of Internal Audit and Management Accounting has issued Technical Guide on Internal Audit of Software Industry in 2014. Considering the evolution of IT Software Industry due to adoption of Cloud services, DevOps Practices, Rise of Artificial Intelligence and Machine Language and Increased focus on Cyber security, Implementation of Dat Privacy Regulations and Impact of Covid 19 Pandemic, the Board is issuing Revised Edition of Technical Guide on Internal Audit of IT Software Industry to equip the internal auditors with deeper understanding of this unique and complex industry.

This Guide covers evolution, history, special features, business processes, major challenges faced by the entities in IT Software Industry. This Guide also explains legal framework applicable to IT Software Industry in detail. This Guide provides Guidance to members on major areas of external and internal risks faced by this Industry. This Guide explains the detailed procedures to be undertaken by the internal auditor in respect of contracts, fixed assets, government grants, loans and borrowings, foreign currency transactions, related party transactions, information security and privacy of data, patents and copyrights, etc.

This Guide also includes glossary of the terms and abbreviations used in the IT Software Industry, Annexure listing out major compliances applicable to software industry under various governing laws and regulations.

We are immensely grateful to CA. Savio Vincent Mendonca, Special Invitee, Board of Internal Audit and Management Accounting, ICAI and CA. Vikram Pandya for sharing their experience and knowledge in review and revising Technical Guide. We also thanked to CA. M. Guruprasad, CA. Kaushik Raghunandan and CA Samarth K Hegde to review and revise Checklist on Compliance given as Annexure in this publication.

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

We also wish to express our sincere appreciation for CA. Arti Bansal, Secretary, Board of Internal Audit and Management Accounting, ICAI, Mr. Harish Dua, advisor, and her team for their efforts in giving final shape to the publication.

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

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

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

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

26th December, 2023
New Delhi

Foreword to the First Edition

Over the last decade, the information technology sector has played a crucial role in placing India on the global map. The sector has crossed significant milestones in terms of revenue growth, employment generation and value creation, in addition to becoming the global brand ambassador for India. Trends in service delivery like, cloud computing, platform BPO, etc., are remodeling the industry and driving tremendous changes which involve high degree of research and scientific sophistication, and specialist analytical methodology. The software industry faces multiple risks like, strategic risk, economic risk, operational risk, compliance risk, disaster risk, political risk, human capital risk, reputational risk, etc.

In this challenging environment, chartered accountants armed with sound domain knowledge, good analytical skills and in depth process understanding play an important role. As internal auditors, they can assist organizations operating in software industry in ensuring that objectives are achieved, risks are managed appropriately, organizational resources are used responsibly and governance systems are strengthened. I am happy that the Internal Audit Standards Board of the Institute of Chartered Accountants of India (ICAI) has brought out this "*Technical Guide on Internal Audit of IT Software Industry*" which is aimed to equip the internal auditors with deeper understanding of this unique and complex industry. I congratulate CA. S.B. Zaware, Chairman, Internal Audit Standards Board and other members of the Board on issuance of this Technical Guide.

It is my sincere hope that this publication would further strengthen the skills of our members as internal auditors of software industry.

February 6, 2014
New Delhi

CA. Subodh K. Agrawal
President, ICAI

Preface to the First Edition

As one of the key growth drivers of engines of the economy, the Indian software industry has been contributing notably to the economic growth and providing direct and indirect employment to a large number of people. The phenomenal success of this industry can be attributed to availability of strong qualified human resources, favourable government policies, burgeoning demand conditions and competitive environment. Emerging technologies such as, social media, mobility, analytics and cloud computing, etc., are driving the growth in this segment and helping it to escalate to the next level. Challenges faced by the industry are poor infra structure, high competition, small domestic market, defusing industry environment, brain drain, etc.

Keeping this in view, the Internal Audit Standards Board of the Institute has issued this "***Technical Guide on Internal Audit of IT Software Industry***" which deals with operational areas of entities operating in this industry, with emphasis on compliance as mandated as per various regulations as applicable to software industry. It provides detailed guidance on business processes controls, risk management, legal and regulatory compliance, etc., related to software industry. This Guide specifically does not covers entities working in Information Technology Enabled Services (ITeS), Knowledge Process Outsourcing and Business Process Outsourcing. This Guide provides a brief about the IT Software companies covering evolution of IT industry, growth trajectory, initiatives taken by the government, major challenges faced, industry segmentation, project lifecycle, revenue model, etc. Salient features of legal framework and regulations governing Software Industry have been discussed in the Guide. The guide also throws light on major areas of external and internal risks being faced by the software industry. Major areas of internal audit significance like, contracts, fixed assets, government grants, loans and borrowings, foreign currency transactions, related party transactions, information security and privacy of data, patents and copyrights, etc., have also been explained. The Guide also contains an Annexure listing out major compliances applicable to software industry under various governing laws and regulations.

At this juncture, I am grateful to CA. Arun Kumar Natha and study group members Shri Ganesh S. Kumar, Shri Sawnya Acharya and Shri Shon Sunny George for sharing their experience and knowledge with us and preparing the draft of the publications and CA. Anil Patwardhan for reviewing the draft Technical Guide.

I also wish to thank to CA. Subodh Kumar Agrawal, President and CA. K. Raghu, Vice President 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. Babu Abraham Kallivayalil, Vice-Chairman, IASB, CA. Rajkumar S. Adukia, CA. Jay Ajit Chhaira, CA. Tarun Jamnadas Ghia, CA. Pankaj Inderchand Jain, CA. Nihar Niranjan Jambusaria, CA. Dhinal Ashvinbhai Shah, CA. S. Santhanakrishnan, CA. J. Venkateswarlu, CA. Abhijit Bandyopadhyay, CA. Anuj Goyal, CA. Naveen N.D. Gupta, Shri Gautam Guha and Shri Manoj Kumar. I also wish to place on record my gratitude for the co-opted members on the Board viz., CA. Ashok Patil Pundlik, CA. Chandrakant Raghunath Karode, CA. Rakesh Dhody, CA. Saurabh Mukund Chitale and CA. Sanjeeb Kumar Agarwal and special Invitee, CA. Sanjay Arora for their invaluable guidance as also their dedication and support to the various initiatives of the Board. I would also like to place on record appreciation to CA. Jyoti Singh, Secretary, Internal Audit Standards Board and her team of officers for their efforts in giving the Guide it's final shape.

I am confident that this publication would prove to be immensely useful for the members.

February 7, 2014
Pune

CA. Shiwaji Bhikaji Zaware
Chairman
Internal Audit Standards Board

Abbreviations

AMC	Annual Maintenance Contract
CAGR	Compounded Annual Growth Rate
CCTV	Closed Circuit Television
CMM	Capability Maturity Model
DGFT	Directorate General of Foreign Trade
DTA	Domestic Tariff Area
DTAA	Double Taxation Avoidance Agreement
ESI	Employees State Insurance
FCNR	Foreign Currency Non-Resident Account
FEMA	Foreign Exchange Management Act
FIRC	Foreign Inward Remittance Certificate
HRD	Human Resources Department
IPR	Intellectual Property Rights
ISO	International Standards Organisation
ISP	Internet Service Provider
ITeS	Information Technology Enabled Services
MSA	Master Service Agreements
NASSCOM	National Association of Software and Services Companies
NSDL	National Securities Depository Limited
NSR	National Skills Registry
PF	Provident Fund
RBI	Reserve Bank of India
RFP	Request for Proposal
RFQ	Request for Quote
SBU	Strategic Business Units

SEZ	Special Economic Zone
SIA	Standards on Internal Audit
SME	Small and Medium Enterprises
SMS	Short Message Service
STPI	Software Technology Parks of India
T & M	Time & Material Billing
TDS	Tax Deducted at Source
TRPS	Trade Related Aspects of Intellectual Property Rights
VAR	Value Added Reseller
WCT	WIPO Copyright Treaty
WPPT	WIPO Performances and Phonograms Treaty
WTO	World Trade Organisation

Glossary

Annual Maintenance Contract (AMC)	Legal agreement entered between two companies wherein the latter agrees to render the maintenance service annually to the former at an exchange of a fixed amount.
Closed Circuit Television (CCTV)	Use of video cameras to transmit signal to a specific place, on a limited set of monitors.
Cloud Computing	Cloud computing is a expression used to describe a variety of different computing concepts that involve a large number of computers that are connected through a real-time communication network (typically, the Internet).
Cloud Storage	Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties.
Directorate General of Foreign Trade (DGFT)	The agency of the Ministry of Commerce and Industry of the Government of India responsible for administering laws regarding foreign trade and foreign investment in India.
Domestic Tariff Area (DTA)	An area within India that is outside Special Economic Zone and other specified areas.
Double Taxation Avoidance Agreement (DTAA)	A tax treaty formally concluded and ratified agreement between two independent nations (bilateral treaty) or more than two nations (multi-lateral treaty) on matters concerning taxation, normally, in written form.
Employees State Insurance (ESI)	A self-financing social security and health insurance scheme for Indian workers.
Foreign Currency Non-Repatriable Account Deposits (FCNR)	A Fixed Deposit Foreign Currency account and not a savings account. Deposits in this account can be made in any of the major currencies like, US Dollar, UK Pound, Canadian Dollar, Deutsche Mark, Japanese Yen and Euro.

Foreign Exchange Management Act (FEMA)	An Act that consolidates and amends the law relating to foreign exchange with the objective of facilitating external trade and payments and for promoting the orderly development and maintenance of foreign exchange market in India.
Foreign Inward Remittance Certificate (FIRC)	A document that provides proof of inward remittance to India.
Firewall	Software or hardware-based network security system that controls the incoming and outgoing network traffic by analysing the data packets and determining whether they should be allowed through or not, based on a rule set.
Global Delivery Model	A methodology used by IT companies by using a model of executing technology project using a team that is distributed globally.
Intellectual Property Rights (IPR)	Rights given to persons over the creations of their minds.
Information Technology (IT) Companies	Companies dealing in information technology are referred to as IT Companies.
Information Technology Enabled Services (ITeS)	Sector of IT Industry which aims at providing various services through the use of IT.
National Association of Software and Services Companies (NASSCOM)	Premier organisation that represents and sets the tone for public policy for the Indian software industry.
Off-shoring	Relocation by a company of a business process from one country to another.
Employee Provident Fund Organization (EPFO)	Employee Provident Fund Organisation is a statutory body of the Government of India under the Ministry of Labor and Employment. It administers a compulsory contributory Provident Fund Scheme, Pension Scheme and an Insurance Scheme.

Reserve Bank of India (RBI)	The apex bank of India. The RBI uses monetary policy to create financial stability in India and is charged with regulating the country's currency and credit systems.
Special Economic Zone (SEZ)	Geographical region that is designed to export goods and provide employment.
Small and Medium Enterprises (SME)	Enterprises where the investment does not exceed specified limits.
Software Ecosystem	A Software ecosystem consists of sets of software solutions that enable, support and automate the activities in a social or business ecosystem.
Statement of Work (SOW)	A formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client.
Software Technology Parks of India (STPI)	An export-oriented scheme for the development and export of computer software, including export of professional services.
Tax Deducted at Source (TDS)	Collecting income tax from source of income in India, governed under the Indian Income Tax Act, 1961.
Value Added Resellers (VAR)	Business process that adds features or services to existing product and later resells it.
Y2K	YEAR 2000 was a problem for both digital and non-digital documentation and data storage solutions that resulted in from the practice of abbreviating 4-digit year to 2-digit.

Contents

Chapter 1
Introduction

Objective and Scope of Technical Guide

1.1 This Technical Guide is intended to assist Internal Auditors in carrying out Internal Audit of entities operating in the Software (Information Technology) Industry. The technical guide deals with operational areas of entities operating in this Industry with emphasis on compliance as mandated as per various regulations as applicable to the specific entity.

1.2 The Indian Information Technology/ Software industry is a global powerhouse today, and its impact on India has been incomparable. It has contributed immensely in positioning the country as a preferred investment destination amongst global investors and creating hug job opportunities in India, as well as in the USA, Europe and other parts of the world. In the last decade, the industry has grown many folds in revenue terms, and relative share to India's GDP is around 7.5 percent in FY2022-23. India is the topmost off-shoring destination for IT companies across the world. Having proven its capabilities in delivering both on-shore and off-shore services to global clients, emerging technologies now offer an entire new gamut of opportunities for top IT firms in India. Indian IT/Software industry offers cost-effectiveness, great quality, high reliability, speedy deliveries and, above all, the use of state-of-the-art technologies globally. (Source: Ministry of Electronics and Information Technology)

1.3 The Indian IT/ ITeS industry has a leading position globally and has been progressively contributing to the growth of exports and creation of employment opportunities. India's IT-BPM industry (excluding e-commerce) is expected to grew by 7.9% to reach at USD 245 billion, including exports of 194 USD Billion in FY2022-23 (E). The IT/ITeS has also created large employment opportunities and is estimated to employ 5.4 million professionals, an addition of 2,90,000 people over FY 2021-2022 (E). Women employees account for 36% share in total industry employee base. (Source: Ministry of Electronics and Information Technology)

1.4 Indian IT/ ITeS sector is growing substantially with its:

- Expansion into varied verticals

- Well differentiated service offerings
- Increasing geographic penetration

The phenomenal success of Indian IT- ITeS industry can be attributed to availability of strong qualified human resources, favourable government policies, burgeoning demand conditions, healthy growth of related industries and competitive environment prevalent in the industry and the focus on innovation by the IT Industry. The interplay of these forces has led to putting the industry on the global map.

1.5 The Software industry is a giant industry embracing large range of segments. To elaborate further, this sector can be categorised into:

(a) Software solutions

(b) IT Services

Scope

1.6 The Technical Guide does not covers following:

(a) IT enabled Services (ITeS) – In this Technical Guide the services relating to Information Technology enabled services (ITeS) have been excluded.

(b) Knowledge Process Outsourcing (KPO) and Business Process Outsourcing (BPO) – Internal audit processes relating to KPO and BPO have also been excluded. The readers may refer to Technical Guide on Internal Audit of BPO Industry as issued by the ICAI for detailed guidance in this area.

Chapter 2
About IT Software Industry

Eco-System

2.1 The software industry is one of the most promising industries in India. Software companies make widespread use of partner business models like resell. Some software companies create and manage partner ecosystems around them. Each software ecosystem is created for a purpose and often one finds network effects in a software ecosystem.

Software Economics and Ecosystems

Today, there are only a few sources in the literature on the form of co-operation between software companies and on the objectives, structure and forms of co-operation in so-called software ecosystems (e.g., referral). For software companies, this is a crucial problem, since the decision to join or to create a software ecosystem or to partner is not easy. All issues around business models, software ecosystem leverage, and software partnerships are roughly summarized in the term 'Software Economics'.

Software Economics refers to the study on how software companies make decisions about resource allocation, partnership formation, and business model selection, considering factors like cost, value, risk, and market dynamics.

Interactions in the Ecosystem

2.2 A software vendor sells software to its customers. The companies in the ecosystem interact with the software vendor or its customers or partners in the following ways:

- Sell products or services to the software vendor's customers. These products or services might be related to or integrated with the software vendor's products or services.
- Sell the software vendor's products, e.g., as Value Added Resellers (VAR).
- Sell services to the software vendor, to the customers, or to the software vendor's partners.
- Purchase or license the software vendor's products.

- Sell or license software to the software vendor (suppliers).
- Align on standards with the software vendor to create bigger markets based on standardized products or services.

Evolution of IT Industry

2.3 The evolution of IT industry can be studied in following phases which have been discussed in the paragraphs given below:

Phase I: Prior to 1980

2.4 The Software industry was literally non-existent in India until 1960. Software used in the computers till that time, were in-built with the systems. Government protected the hardware industry through high tariff barriers and licensing. However, in the west, the need for software development was gradually being felt as the software in-built in the system was not sufficient to perform all the operations. The government of India therefore, realised the potential for earning foreign exchange.

In 1972, the government formulated the Software Export Scheme. This scheme made the provision of hardware imports in exchange of software exports. Tata Consultancy Services Limited (TCS) became the first firm to agree to this condition. The year 1974 marked the beginning of software exports from India.

Phase II: 1980-1990

2.5 Despite the government initiatives, the software exports were not picking up because of two reasons mainly:

- The exports of software were heavily dependent on the imports of hardware, which was costly as well as the procedure for obtaining the same was very cumbersome.
- Secondly, there was a lack of infrastructural facilities for software development.

To counter these, the government formulated a new computer policy in 1984, which simplified import procedure and also reduced the import duty on hardware for software developers. In an attempt to make software industry independent of hardware industry, the government in 1986 formulated Software policy which further liberalised the IT industry. According to this policy, the hardware imports were de-licensed and were also made duty free

for the exporters. This along with the worldwide crash in the hardware prices reduced the entry barriers substantially.

In 1990, government established Software Technology Park of India. This scheme was formulated to increase the export of software and services.

Phase III: 1990-2000

2.6 This decade made several significant changes in the economy, including trade liberalisation, opening up of Indian economy to foreign investment, devaluation of rupee, and relaxation of entry barriers. These changes attracted many foreign entities to our nation. These MNC's in India, introduced 'Offshore Model' for software services, according to which the companies used to service their clients from India itself. This model further graduated itself to 'Global Delivery Model', It is the combination of Onsite and Offshore Model. In this Model Offshore Development Centre is located in various locations across the globe.

During this period due to the entry of many players in Indian market, the competition got intensified. Therefore, the players started investing in research and development to distinguish their services from others.

Phase IV: 2000 - 2007

2.7 The Global problems like, Y2K, the dotcom crash and recession in the US economy, proved to be a boon to Indian IT Industry. The Y2K problem demanded the existing software to be compatible to the year 2000. Due to the shortage of US based programmers during this period, many mid – sized firms were forced to utilise the services of Indian Firms. This had placed the Indian IT industry on the global Map.

Post 2002-03, the industry had registered a robust growth rate because of increase in the number of clients, large sized contracts and a strong global delivery model.

Phase V: 2007 - 2015

2.8 Economies faced a downward trend during the 2007-10 due to recession in the United States of America and the snowball effect to the European and the Asian countries. This situation got even more aggravated with the uncertainties in the global political and economic environment. This affected economy at large with rising unemployment rates, political instabilities, general uncertainty and large-scale cost reduction initiatives by both private and public sector organizations. This has resulted in huge budget cuts on IT investment by large corporations. It leads to stiffer

competition for software companies to grab their market share to sustain their growth rates.

Since 2010, the recession impact smoothened and there have been signs of recovery. However, the markets and the corporates are cautious in their approach especially on any long-term strategic investment decisions. This stage evolved into a lot of phenomenal changes in the industry. The key changes post 2010 phase are:

- Early capital budgeting was performed by the companies in order to avoid last minute funds shortage.
- The software industry approach changed towards outcomes-based solutions for their clients. The prime motive of the big players of the industry was to blend their services and products specific to customer requirements and serve their needs efficiently in an Operating Expenditure (Opex) based model rather than the traditional Capital Expenditure (Capex) based model.
- Companies came out with different strategies to adopt with client and to gain customer base. Some of these are gain sharing, investment sharing, etc.
- The most prominent change that emerged after the phase of 2010 was Cloud Computing. Mass storage of data on cloud has not been very commonly used pre-2010. This trend saw a huge change. 90% of today's data of an enterprise or individual users are stored on cloud, with or without our knowledge.
- Mobile had just been a device for calling, SMS and some entertainment like music, videos. Nowadays, the industry is not the same though. Usage of mobiles has come to such a large extent that the same is used for enterprise mobility, decision-making, social media, banking, analytics, etc.

Phase VI: Post 2015

Increased Adoption of Cloud Services

2.9 Post-2015, the adoption of cloud services significantly increased. Businesses started shifting their operations to the cloud to take advantage of the scalability, accessibility, and cost-effectiveness it offers.

Rise of AI and Machine Learning

This period witnessed a surge in the use of Artificial Intelligence and Machine Learning in software development. These technologies allowed for more sophisticated software capable of automation, prediction, and complex data analysis.

Adoption of DevOps Practices

The post-2015 phase saw many companies adopting DevOps practices. This approach brought together software development and IT operations to shorten the systems development life cycle and provide continuous delivery with high software quality.

Increased Focus on Cybersecurity

With the increase in digital operations and data storage, the focus on cybersecurity grew. Software companies started investing more in secure coding practices and security measures to protect data and systems.

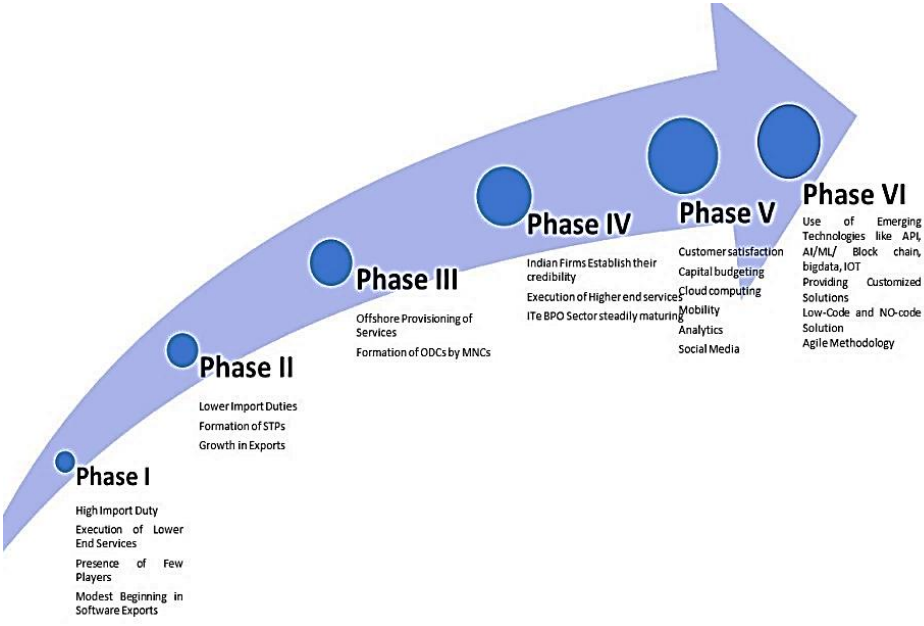
Adaptation to Data Privacy Regulations

The introduction of data privacy regulations like GDPR and CCPA had a significant impact on the software industry. Companies had to adjust their software and practices to comply with these regulations. In India recently Personal Data Protection Act 2023 got passed. it has been explained in detail in another chapter of this Guide only.

Pandemic Impact

The COVID-19 pandemic in 2020 led to a rapid shift towards remote work, thereby increasing the demand for collaboration tools, virtual meeting software, and digital transformation initiatives.

Growth Trajectory



Initiatives Taken by the Government

2.10 Although the story of the Indian software industry is a story of private initiative, the government played a supporting role with public funding of a large, well-trained pool of engineers and management personnel who could forge the Indian IT industry into a world class treasure in a short time. Early government support came from a few visionary civil servants who championed the cause and helped the industry find its way through a labyrinth of regulations, making exemptions wherever possible. Later, policies that encouraged local firms and direct foreign investments were introduced.

2.11 Government targeted software exports once the market identified the industry's potential and created the necessary institutions. As early as 1972, the Department of Electronics introduced a policy to permit duty-free imports of computer systems, if importers would promise to export software and services worth twice the value of the imported computers within a specified time. This policy helped a number of leading companies in their inception stage. In the 1980s the Department gave software developers a further boost by initiating software export friendly policies. It formed a software export promotion council and liberalized import rules for materials needed for the

industry. Software was explicitly targeted as a key sector for export promotion. In the late 1990s, the government created four major taskforces comprising chief executives of leading software companies to study the sector and recommend actions, and then acted on most of the recommendations. At that time the Department of Electronics became the Ministry of Communication and Information Technology. This was followed by the IT Act to address a large number of issues. In addition to these federal interventions, many states promoted local software industry by improving infrastructure, IT education, and provision of more facilitating environments.

With the beginning of economic reforms in the early 1990s, efforts were made to attract foreign as well as domestic investment. Foreign companies were permitted to establish fully owned subsidiaries in the electronics export processing zones. Within the Ministry of Finance there was greater recognition of India's comparative advantage in the sector, as it abolished entry barriers for foreign companies, made available fast, low-cost data connection facilities, and reduced and rationalized duties, taxes, and tariffs.

The Reserve Bank of India adopted several measures to support the IT industry. These included: simplification of the filing of Software Export Declaration Form (SOFTEX); acquisition of overseas parent company shares by employees of the Indian company; companies whose software sales were over 80 percent could grant stock options to non-resident and permanent resident employees; foreign exchange could be freely remitted for buying services; and companies which executed contracts in "computer software" abroad could use income up to 70 percent of contract value to meet contract-related expenses abroad.

The Reserve Bank of India's support, including measures such as stock options for employees and the facilitation of foreign exchange for buying services, further bolstered the IT industry. These initiatives ensured a conducive environment for IT companies to operate and grow, contributing to the industry's success.

Tax holidays were given on company profits, although the government is progressively phasing out these deductions. Tax breaks from corporate income and tax on profits was available to units in any free trade zone, any software technology park, or any special economic zone to the extent of 100 percent of the profits derived from the business. These deductions were not available from Financial Year 2009–2010 onwards.

Indian direct investment in joint venture (JV)/ wholly owned subsidiaries (WOS) abroad was simplified and a fast-track window is available for large investments. IT software and services companies in India can acquire

companies overseas through American Depositary Receipt/ Global Depository Receipt stock swaps without prior approval for up to $100 million or ten times the export earnings of the previous year.

2.12 While the government has enacted significant reforms in the area of intellectual property rights (IPRs) and has joined the World Trade Organization and Trade-Related Aspects of IPRs, the reforms have so far not led to a surge in patents in the Indian software industry, nor have IPRs been perceived as effective in protecting innovations in the Indian software industry.

Several policy reforms in the telecom sector helped accelerate the domestic and export industry. In 1998, a national telecom policy was announced to clarify the role of the regulator, transition from license fee to a revenue sharing model and open domestic long distance to private operators. The ISP gateway monopoly ended in 2000 and permitted private companies to set up international gateways. In 2002, international long distance was liberalized two years ahead of WTO commitments and competition increased in cellular markets. As a result, India's tele density, the number of phones per 100 people, increased to five and cellular penetration overtook the land line penetration.

Recognizing the growing need for manpower in the software industry, the Ministry of Human Resources Development took the following actions:

- Helped create and expand computer science departments in existing engineering colleges.
- Eased policies in order to enable private sectors to open educational institutions without public funding. A large number of engineering colleges were opened in the private sector.
- Introduced quality control systems for engineering colleges and other IT training institutions, such as the All-India Council for Technical Education and an accreditation system run by professional bodies such as the Computer Society of India to monitor private training institutions.
- Encouraged the private sector to open training institutions. At its peak nearly one million Indians were being trained in a year with the IT training industry earning over nearly 10 billion rupees in 1998 with no government subsidy.

The Ministry of Electronics and Information Technology is coordinating strategic activities, promoting skill development programmes, enhancing

infrastructure capabilities and supporting R&D for India's leadership position in IT and IT-enabled Services.

Next Generation Incubation Scheme or "NGIS" is a futuristic & comprehensive incubation scheme entrusted by MeitY to STPI for implementation. NGIS has a vision to drive the rise of India as a Software Product Nation so as to make India a global player in development, production and supply of Innovative, Efficient and Secure Software Products (including embedded software). NGIS is focusing on 12 locations across India viz. Agartala, Bhilai, Bhopal, Bhubaneswar, Dehradun, Guwahati, Jaipur, Lucknow, Prayagraj, Mohali, Patna & Vijayawada. The Scheme targets to support 300 tech- startups/Entrepreneurs in the field of IT/ITeS/ESDM. (Source: Ministry of Electronics and Information Technology)

Further, Government has undertaken the following Other Projects & Initiatives in the IT sector:

- Sign Language Accessibility
- National Single Sign-On (NSSO)
- Aadhaar Data Vault
- e-Sign (e-Hastakshar)
- API Setu
- CSC 2.0-A way Forward
- Digitize India Platform (DIP)
- National Information Infrastructure (NII) EFC Note & Memo - Comments requested by 23rd Feb 2015 at akbalani@deity.gov.in [PDF]15.38 MB
- PayGov India – National Payment Service platform
- Centre for e-governance
- E-Governance Conformity Assessment Centre
- Open Technology Centre
- India Development Gateway
- World Bank assisted projects
- e-Pramaan
- New Awareness and Communication Scheme
- e-Gov AppStore

- Accessibility (Knowledge & Resource Centre for Accessibility in ICT (KAI))

(Source: Ministry of Electronics and Information Technology)

Software Technology Parks

Creation of NASSCOM in 1988 and later establishment of STPs in 1990 represented a fundamental approach to policy making for the software industry. An important institutional intervention was the establishment of STPs to provide infrastructure for private companies to export software. Established in 39 locations, including most major towns, they provided ready-to-plug IT and telecom infrastructure. STPs also allowed single-window clearance for all regulatory matters. The benefits and approvals for STPs are similar to those of Export Oriented Units. Incentives provided in the Export–Import Policy are also applicable to STP members.

Software Technology Parks of India (STPI) is a premier S&T organization under Ministry of Electronics and Information Technology (MeitY) engaged in promoting IT/ITES Industry, innovation, R&D, start-ups, product/IP creation in the field of emerging technologies like IoT, Blockchain, Artificial Intelligence (AI), Machine Learning (ML), Computer Vision, Robotics, Robotics Process Automation (RPA), Augmented & Virtual Reality, Animation & Visual effect, Data Science & Analytics for various domains like Gaming, FinTech, Agritech, MedTech, Autonomous Connected Electric & Shared(ACES) Mobility, ESDM, Cyber Security, Industry 4.0, Drone, Efficiency Augmentation, etc.

STPI is establishing CoEs/Technology incubators for building India's leadership in the above-mentioned technology areas across the country in a collaborative manner. Till date, STPI has launched 22 Centres of Entrepreneurship (CoEs).

STPI is aspiring to become the largest technology startup ecosystem in the country and has been endeavouring to transform the country into a software product nation as envisaged in National Policy on Software Products (NPSP) 2019. In order to achieve this, STPI has evolved a collaborative model wherein government, industry, academia, and other stakeholders are playing a vital role for providing end-to-end support to startups. Aligned with this vision for promoting R&D, innovation, product & IPR creation, STPI is providing state-of-the-art infrastructure, skilling, mentoring, market connect and other necessary support pan-India to startups.

STPI has also embarked on launching Next Generation Incubation Scheme (NGIS), a futuristic incubation scheme to offer comprehensive support & services and extend seed funding to startups from 12 STPI incubation facilities pan-India.

Since its inception in 1991, STPI has been working towards equitable and inclusive IT-led growth pan-India which in turn has helped promoting Software exports, Science, Technology & Innovation (STI) and Software product development. With 11 jurisdictional directorates and 63 centres, STPI has expanded its presence pan-India to support IT/ITeS Industry. Working closely with all stakeholders, STPI has played a key role in transforming the country as the preferred IT destination, a fact that aptly proven by the stupendous growth in exports by STPI-registered units from Rs. 52 crores in 1992-93 to Rs. 6,28,330 crores in 2021-22, which is approx. 50% of the national software exports and 2.3% of India's GDP. The first historic event that triggered the high-octane growth of IT Industry in India was the establishment of three Software Technology Parks (STPs) at Bengaluru, Bhubaneswar and Pune in 1989. Consequently, in 1991 these three STPs were merged to create a single entity Software Technology Parks of India. (Source: Software Technology Parks of India (STPI))

Competition and Differentiators

Talent availability	Outsourcing	Pyramidal structure	Foreign Investment	Labour arbitrage

Indian software industry thrives significantly based on the clients from the US market. Although there are a number of clients across other continents, *viz*., Europe, Middle-East, Asia, Australia, US still has the lion share of market for the Indian software industry.

The key areas which would differentiate Indian Software industry from others are as under:

- The Indian comparative advantage is based on cost and availability of software talent. The ability to offer the services of a large number of software professionals at costs substantially lower than those in the U.S. U.S. firms do not outsource requirement analysis, specification, and high-level design, nor do they outsource larger scale system integration types of activities to India. However, the leading Indian software firms do have the ability to provide these high-end services.

- The option of outsourcing has been of great value to U.S. firms. Virtually, all the U.S. managers noted that outsourcing to Indian firms allowed them to use in-house staff for more valuable and creative activities, such as the development of new business applications with a greater potential for influencing the firm. They greatly value the flexibility inherent in outsourcing – the firm does not take on a long-term obligation when it is uncertain about the future, both about the evolution of information technology and about its own specific uses of the technology.
- Indian software firms do not pose serious competitive challenge to U.S. software firms. Indeed, for the most part, they complement the U.S. industry, with the possible exception of those U.S. firms that provide staff augmentation and software services.
- The Indian software industry has a pyramidal structure with large corporates ruling the sector. India's software products sales are likely to hit $30 billion mark by 2025, as domestic companies expand their footprints globally and many new players are getting into the products space, as per the report from NASSCOM. The report says, the software products market is estimated to clock $13.3 billion in annual revenue for the FY22 ended March 31, after logging a CAGR of over 10 per cent in the previous three financial years.
- Multinational Companies (MNCs) are setting up their branches in India to conduct sophisticated software development activities and as a captive source of R&D, utilising India's abundant manpower.

Major Challenges Faced by the Industry

The Indian software services industry has been spectacularly successful, growing at over 50% annually for several years. However, the nature of markets and technology is changing. Other changes include rising salaries in India, fast growing higher end markets, talent shortage worldwide, and need for faster implementation of projects. However, for Indian companies a key change could be the growth of market segments that are not so price sensitive, and price-based competition from China, Mexico, Philippines and other countries. Challenges arising from sustained high growth, operating as a low-cost service provider, challenge of overseas development, managing multiple agencies in a single project, cultural challenges of operating in overseas markets and entry barriers to higher end value added work.

2.13 The major challenges faced by the IT Industry in India are as under:

- **Less Expensive Labour**

  Though initially India provided less expensive and highly skilled manpower; currently it has run out of that 'skilled' manpower and whatever manpower is available is either not 'skilled enough' or very expensive.

- **Poor Infrastructure**

  Infrastructure in India has not been able to keep pace with the sustained development needs in the software industry. For example, the rental in the housing markets has increased nearly four fold in the last 5 years, however the incomes for these software professionals have not increased in the same proportion.

- **High Competition**

  The ASEAN and Eastern European countries provide as much cost benefit as Indians do and they currently are as competitive as Indians are in cost.

- **Brain Drain**

  Project management expertise is scarce. This problem is exacerbated by a large number of experienced professionals who emigrate to the U.S.

- **Defusing Industry Environment**

  The Indian software industry specializes in the export of low-end software development services, competing primarily on cost and availability of software talent. The industry is diffusing geographically. Although Bangalore is still home to many of the leading firms, the industry is not confined to Bangalore and is diffusing to regions other than Bangalore and Mumbai, with a substantial presence in Hyderabad, Chennai, and Delhi, and a growing presence in Calcutta and Pune.

- **Current Relevance**

  - Remote Work: With the advent of the COVID-19 pandemic, remote work has become a common practice in the software industry. This has implications for both labor cost and infrastructure. While remote work allows access to global talent, it also brings challenges in terms of team coordination, communication, and maintaining company culture.

- Emerging Technologies: Rapid advancements in technologies like Artificial Intelligence, Machine Learning, and Blockchain are reshaping the software industry. Staying relevant requires continuous learning and adaptation to these new technologies.
- Cybersecurity: With the increasing digitization of businesses, cybersecurity has become a significant concern. It's crucial for software companies to invest in secure coding practices and protect their systems from cyber threats.
- Data Privacy Regulations: Regulations like the Personal Data Protection Bill 2023, General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the US have increased the importance of data privacy and security in the software industry.

- **Lack of R&D**

- Focus on Services: The Indian IT industry has traditionally been focused on providing services rather than investing in research and development. This has resulted in a lack of innovative products originating from India.
- Short-term Goals: Companies often prioritize short-term revenue generation over long-term R&D investments. This approach can limit the growth and innovation potential of the industry.
- Talent Gap: There is a need for skilled professionals who can carry out advanced research in software development. The education system needs to be equipped to provide the necessary training and promote research-oriented thinking.

Factors Contributing to Industry Growth

2.14 Factors that contribute to industry growth are as follows:

VUCA World

The disruptions brought on by the COVID-19 pandemic continued through CY2022. The new variant, BF.7, impacted most Asian economies including Japan and China. With the ongoing disruption of the supply chain (especially with respect to semiconductors), both governments and enterprises are re-thinking their supply chain strategy. The surprising invasion of Ukraine by Russia in early CY2022 impacted food and energy security worldwide, leading to higher inflation. CY2022 also saw ongoing concerns around

recession as the global economies saw slower growth. However, the growth of emerging economies has been more resilient, with India leading the economic revival at a rate much higher than the rest of the world. Overall, India's tech industry is estimated to touch $245 billion in the 2022-23 financial year, with an incremental revenue addition of $19 billion during the same period.

Technology: The Focal Point for Businesses

Among businesses, the Technology industry was the silver lining as enterprises reshaped and accelerated their digital transformation agenda, and as a result, sourcing, and talent strategies for CY2023. Increasingly, enterprises, including traditional enterprises, are leaning on technology for scaling automation while humanising UX, streamlining supply chain, enhancing cyber resilience, and delivering their sustainability goals towards becoming purpose-driven businesses.

Global Technology Trends 2022 onwards

In CY2022, the total global technology spends stood at $4.39 Trillion, a slight decline of -0.2% over CY2021, driven by lower consumer spending on devices. Enterprise software and IT services crossed the $2 Trillion mark, a growth of 4.5% year-on-year in CY2022.

(Source: NASSCOM)

Quality Accreditations

Quality accreditations continue to be an important aspect for companies operating in the software industry. These accreditations ensure not only client satisfaction but also product and service quality. They provide a structured system to handle potential process hindrances and maintain ethical and effective certification practices.

Among the quality accreditations, ISO 9001 remains a globally recognized standard. This quality management system is designed to help organizations meet the needs of customers and other stakeholders while adhering to statutory and regulatory requirements related to the product or service.

However, a quality accreditation is not a one-time certificate. It requires renewal through a quality assurance audit at regular intervals, usually every three years. In addition to ISO 9001, other popular quality accreditations used by software companies include ISO 27001 (Information Security Management), ISO 14001 (Environmental Management), and ISO 20000 (IT Service Management).

Another important accreditation is the Capability Maturity Model Integration (CMMI) issued by the Software Engineering Institute. This certification focuses on process improvement and the highest grade, Level 5, represents an organization that has achieved an optimized process state.

In recent years, given the increasing significance of data protection and privacy, certifications such as ISO 27701 (Privacy Information Management) have gained prominence. This standard helps organizations establish a Privacy Information Management System (PIMS).

Furthermore, the Reserve Bank of India (RBI) has issued guidelines for the adoption of digital payment technologies, requiring software companies in the FinTech space to adhere to specific standards of data security and customer privacy.

For companies engaged in AI and Machine Learning developments, adherence to AI ethics guidelines, such as those proposed by NASSCOM, is becoming increasingly important. These guidelines emphasize aspects such as transparency, fairness, security, and privacy in AI applications.

The Government of India has also been actively promoting the adoption of Indian Standards (IS) in the software industry, in alignment with the Make in India initiative. These standards cover a broad spectrum of areas including software quality, cybersecurity, and interoperability.

Operating Model

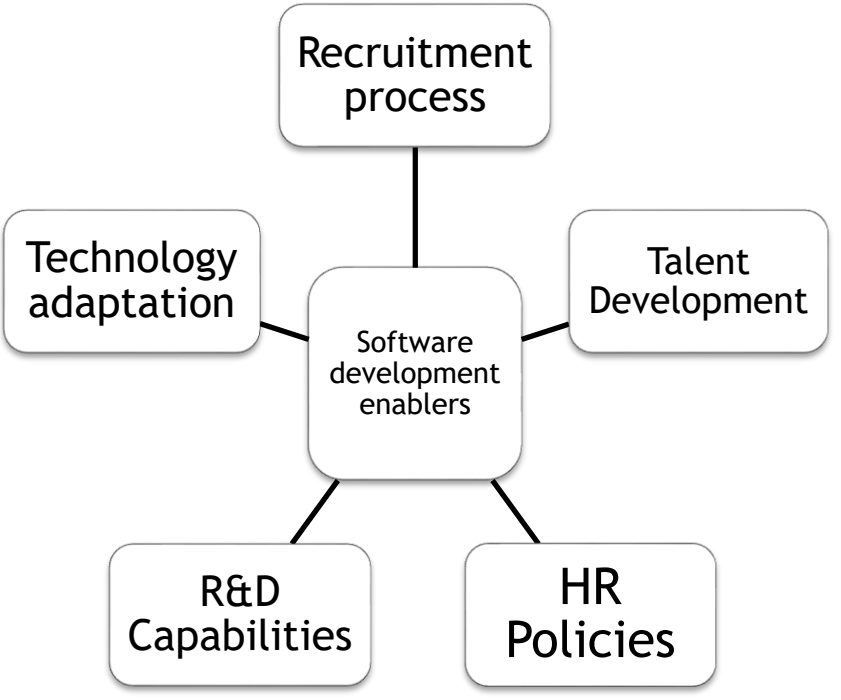
2.15 The IT industry has unique operating model due to the macro-economic factors influencing the industry. The global environment and the various industries in which the customers are operating play an important role in the way the IT companies are structured to provide meaningful services. In the Indian market context, these IT companies are focused on providing the services to the global companies at a lower cost with most innovative solutions in a global delivery model. While the origin of the business model began with providing service at a lower cost, it has gradually evolved in to providing more value to the clients through the intellectual capital accumulated over the past several decades. Let us understand the various elements of their operating model.

Business Model

2.16 Global customers especially look for support from India IT players in terms of providing high quality people who could help in their technological requirements. This could be around maintaining their existing technologies,

creating new technologies to support their business processes, new platforms, global infrastructure, helpdesk and so on. The primary resources for IT industry are the human resources and technology. These two drive a significant influence on providing value to the customers. Hence, the IT companies operate around where the human resources are available and the environment where new technologies can be generated.

Strength and competitiveness of the IT companies lays in their ability to attract high quality talent who can develop state-of-the-art technologies. This requires high standards of recruitment process, talent development, HR policies, research and development capabilities of the service provider. A professional sales force required at the customer locations that should be building solutions to their requirements. This would also require a number of onsite employees with delivery experience to demonstrate the delivery capabilities.



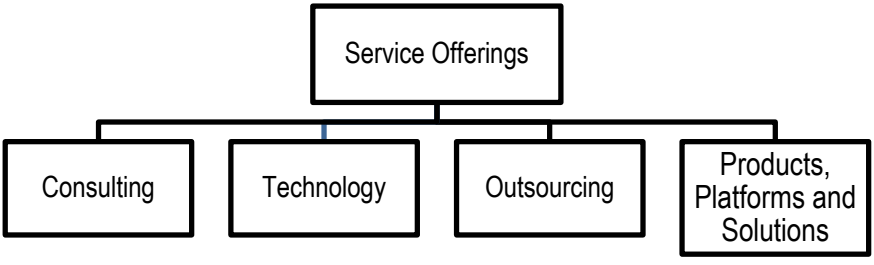
Depending on the customer requirements, they usually invite service provider by sending out Request for Proposal (RFP) or Request for Quotation (RFQ). This RFP will have all the necessary requirements of the customer that they expect from the service provider. The service provider will have to respond to the RFP by filling in the necessary details and the proposed solution

including the pricing. Depending on the solution and the other parameters, the customer evaluates the entire service provider and then finally selects the service provider to award the contract.

The type of contract varies from one-time projects with limited timeframe to long-term Master Service Agreements (MSAs) which covers a suite of services offered by the service provider. This depends on the strategy of the customer and their confidence in working with the service provider as a strategic partner. The contract contains a number of legal requirements which will be binding on both the parties obligated to a number of commitments.

Service Offerings

2.17 The services offerings of IT companies include the below 4 categories with specific areas:



(i) Consulting

- (a) Business Consulting
- (b) Technology Consulting
- (c) Process Consulting

(ii) Technology

- (a) Business Application services, across SAP, Oracle, IBM, TIBCO, Microsoft Dynamics, Salesfore.com, etc.
- (b) Business IT Services
  - (i) Application Outsourcing Services
  - (ii) Application Services
  - (iii) Independent Validation and Testing Services
  - (iv) Infrastructure Management Services

(v) Infrastructure Outsourcing Services

(c) Engineering services

(iii) Outsourcing

(a) Business Process Outsourcing (BPO)

(iv) Products, Platforms and Solutions

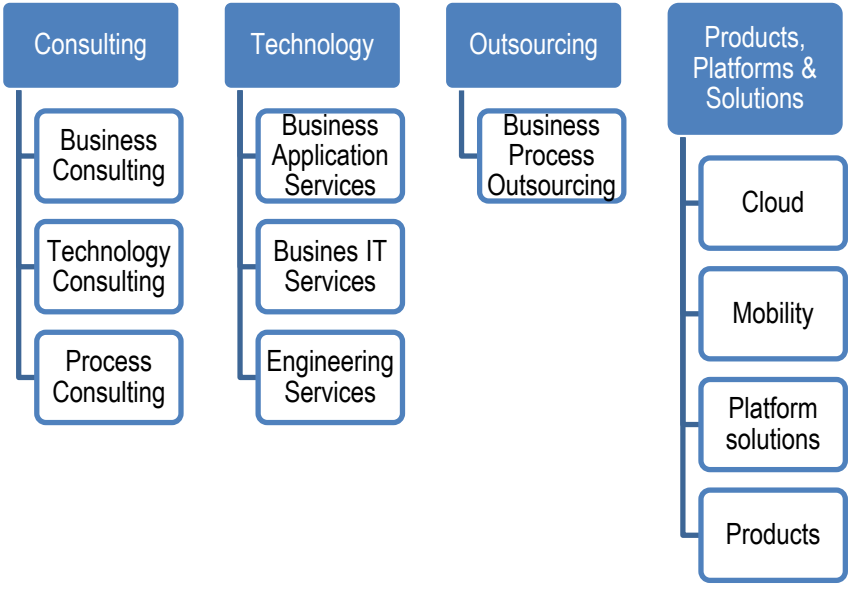
(a) Cloud

(b) Mobility

(c) Sustainability

(d) Platform solutions

(e) Products



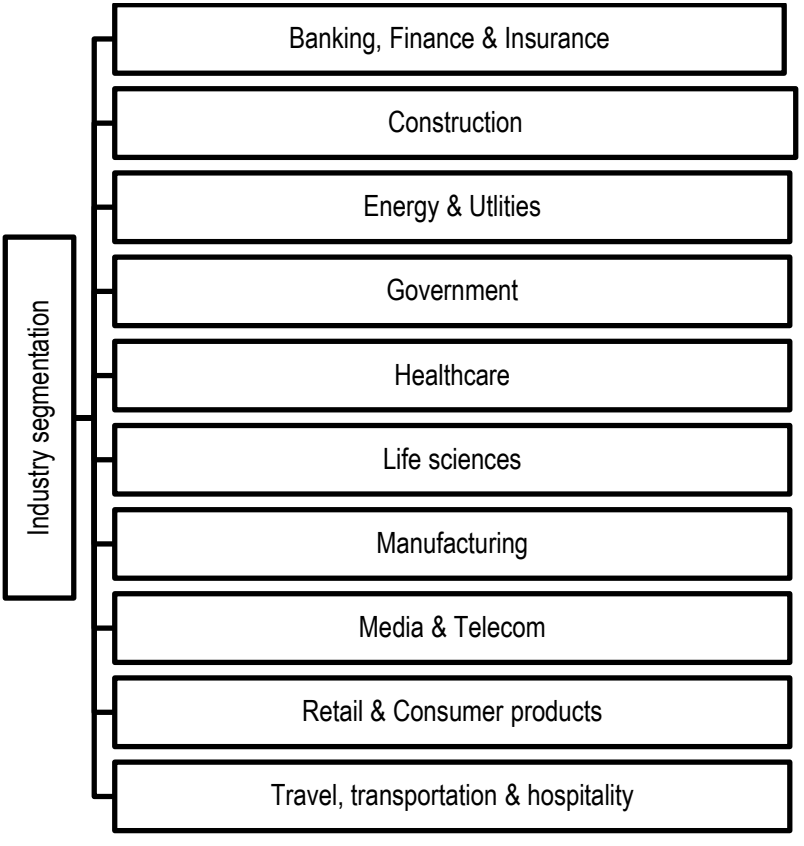
Customer Industry Orientation

2.18 While there are number of service offered by the IT companies, the significant value-add is provided by tailoring these services based on the industry in which their customers operate. This is to make their services relevant to their customer and also to ensure that their workforce is groomed to build expertise that matches their customer business environment. This is

one of the most important leverage for the customer to approach IT service providers as they get access to multi-varied experienced talent which otherwise would not be possible in-house. Therefore, the Industry segmentation organized by the IT companies is in the following Industry verticals as discussed below.

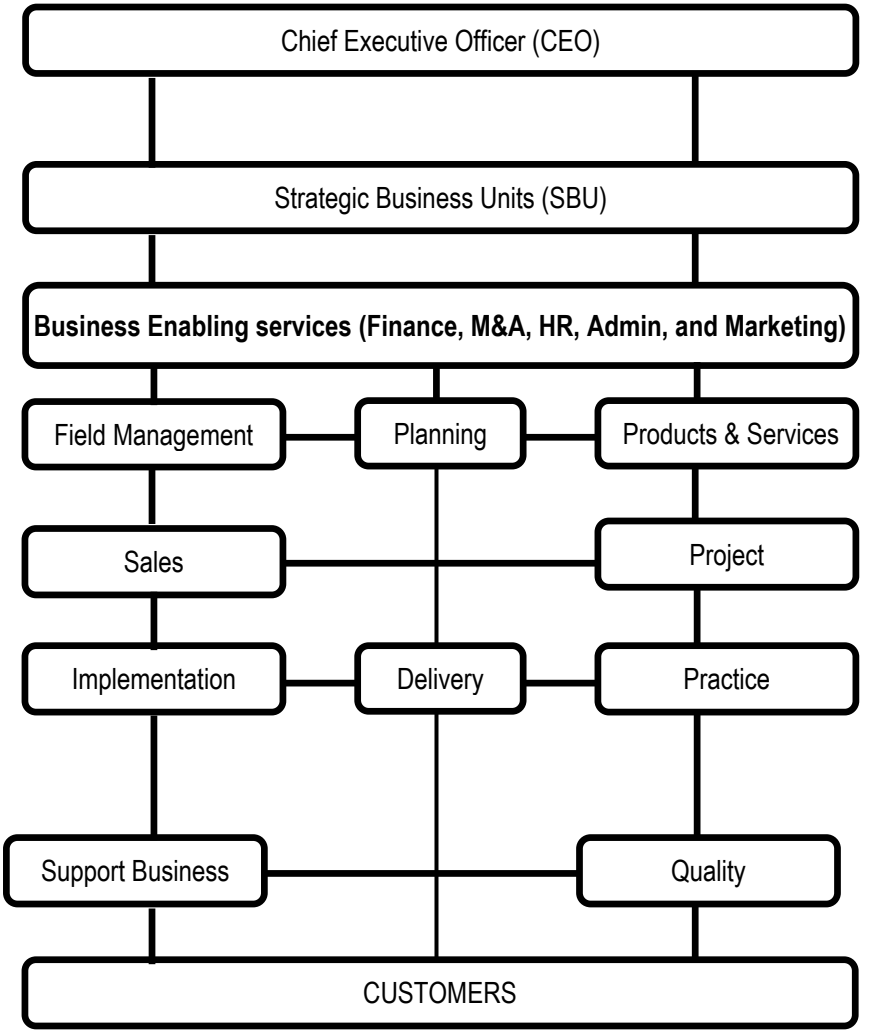
Industry Segmentation

2.19 Industry segmentation refers to the major industries in which Software Industry plays a vital role. The software companies in the industry render services and products to the following industries that fall as part of majority of revenue:



Typical Organization Structure

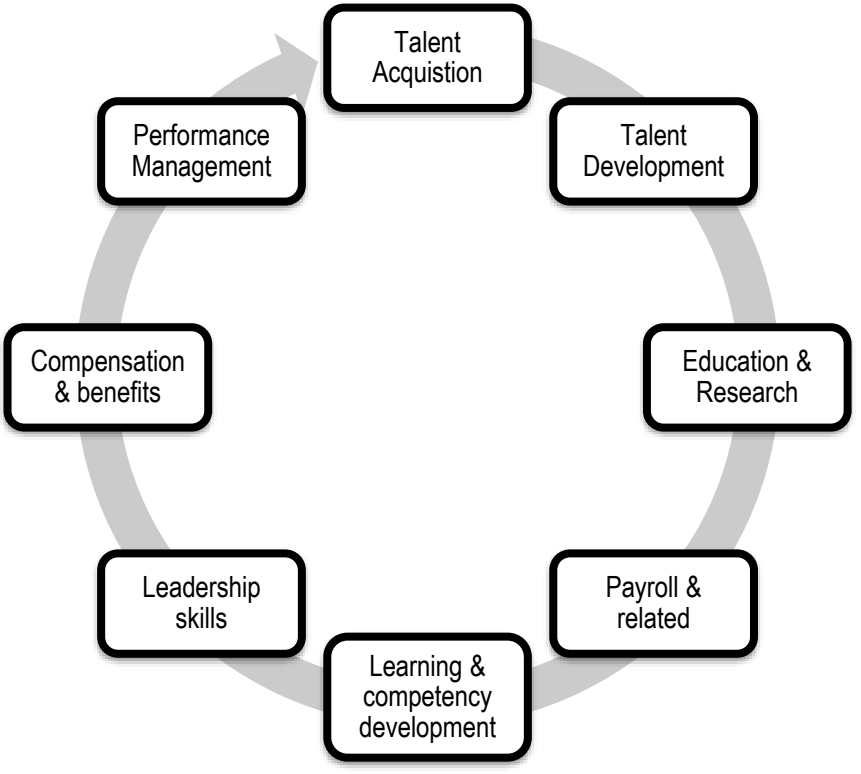
2.20 The typical organizational structure of a software company is depicted below. This is illustrative to visualize the organization structure normally followed explaining the inter-connectivity of variety of functions within the organization.



Human Resources Development

2.21 Human Resources Development (HRD) plays a backbone for an IT company, as the dependence on people is significantly high. Therefore, every IT company takes a number of efforts to ensure world class HR

practices in their businesses. The broad activities / departments within HRD include:



All these functions work in tandem to ensure they hire, retain, and groom best of the breed people within the organization. There are a number of accreditations and certifications provided by organizations for the best in the industry. Such accreditations demonstrate the organization practices around people as this becomes the basis on which customers rely on the services provided by the IT companies. There is a huge competition among the IT companies to differentiate themselves based on the HR practices in order to attract talent as well as to provide confidence to their customers for sustainable service offering.

Revenue Model

2.22 Revenues generated by IT companies vary depending on the nature of service and the arrangement with the customer. The typical billing models are:

Billing Models					
Time & Material based - (T&M)	Milestone based	License-based	Annual Maintenance Contracts - (AMC)	Outcome based	Transaction based

Time & Material (T&M) billing involves billing which could be on hourly rates, daily rates, weekly rates, fortnightly rates, monthly rates or bimonthly rates or quarterly rates, etc. In T&M, billing is done on the basis of the time spent by the people involved in the project. This is being tracked by the time sheets maintained by the employees and approved by the project managers. It is also known as Full Time Equivalent (FTE) method of billing.

Milestone billings is charged on the basis of achievement of a Milestone which could be Feasibility Study/ Business Analysis/ Development/ Implementation/ Go Live. The completion of the phase has to be signed by both the parties. Milestone contracts are also called Fixed Price Contracts.

Product License sales could be for examples like, SAP, JDE, Tally MS office, etc. wherein the customer is charged for the number of users using the product of the service provider. This model is usually adopted wherein the product is developed by a service provider and it is installed at the customer location. Typically, this product will require use by multitude of people and, therefore, the customer pays based on the number of users. A typical example would be a banking software, airline software, operating system, etc.

Annual Maintenance Contracts (AMC's) could be installation of Patches and Upgrades. AMCs may also involve change management of the software.

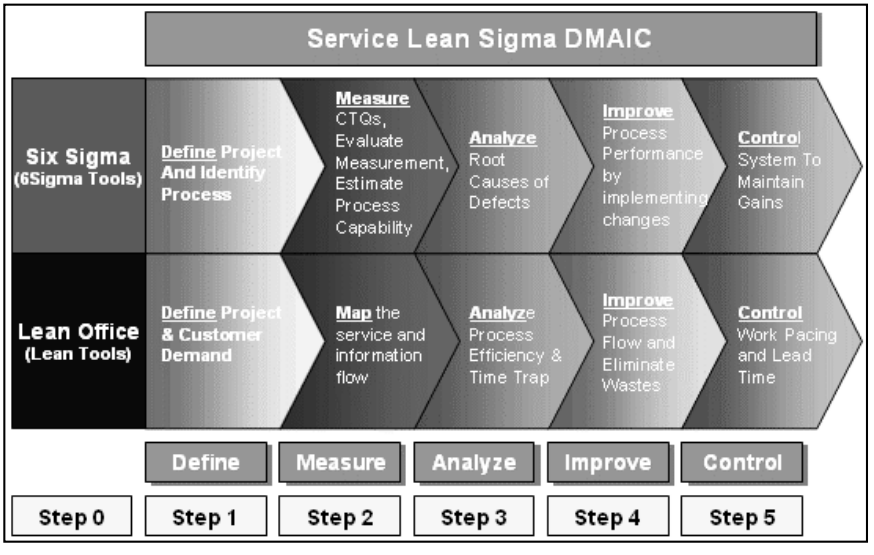
Outcome based pricing, wherein the service provider charges based on the outcomes realized by the customer. This is typically used in Products, Platforms and Solutions service offerings. This is becoming more popular model as the customers want to pay for outcomes than the efforts of the software company.

Transaction/ volume based pricing, wherein the customer pays based on the volumes or transactions delivered by the service provider, irrespective of the number of people or effort put in by them.

Project Lifecycle

2.23 The project spans in an IT industry typically spans anywhere from months to several years depending upon the nature of projects. The lifecycle of project would typically follow six sigma DMAIC steps of:

1. **D**efine
2. **M**easure
3. **A**nalyse
4. **I**mprove
5. **C**ontrol



Project Management plays a very significant role in the IT companies as this becomes key enabler to fulfil the customer requirements. Therefore, a number of training and coaching programs are conducted for the people to be fully equipped in managing projects. This is especially essential in a milestone-based billing projects. This also helps in projects where there will be multiple stakeholders involved across both service provider and the customer organizations. Agile methodology focuses on iterative and

incremental development, where requirements and solutions evolve through the collaborative effort of cross-functional teams. Scrum is a popular framework for implementing Agile development.

Service Delivery Commitment and Compliance

2.24 The service provider typically commits a minimum service level when it comes to the services offered. This is to provide assurance for the customer as well as to ensure continuity of business operations of the customer. There are many measurement criteria's being used to measure the minimum service levels which are converted into service commitment and built into the contract. The service provider is expected to fulfil this service commitment, failing which, they will be liable to penalties or even consequences of termination of contract. Therefore, in a typical IT project, the delivery commitment paramount becomes guiding factor to be ensured by the service provider. All the key people in the project are expected to be fully familiar with such commitments and ensure that they provide the necessary contribution to ensure it is met.

Governance Model

2.25 As there are number of stakeholders involved across both customer and the service provider across multiple locations, it is indeed essential to have a proper governance model which ensures the communication across levels happens as per agreed frequency. There will be multi-layered governance structure established with specific focus on various topics involved in the engagement between customer and the service provider.

	Governing body	Agenda	Members of Customer	Members of Service Provider	Frequency
1	Strategic: Steering committee	1.Engagement plan 2. Contractual 3.Performance 4 Future plans	Key stakeholders viz. CIO, relationship manager	Business Unit Head, Engagement manager	Quarterly
2	Operational: Project portfolio review committee	1. Portfolio review 2. Milestone updates	Project Management officer, Business stakeholders	Engagement manager, Delivery Leaders	Monthly

		3. Key issues / challenges 4. New opportunities / improvements			
3.	Tactical: Project review board	1. Individual project review 2. Issues / challenges 3. Agreements on performance	Project leader Project team members	Engagement leader Project Leader Project team	Weekly
4	Contract board	1. Contract review 2. MSA review 3. Legal 4. Performance compliance	Legal representative, Relationship manager	Engagement Manager, Legal representative	Monthly

Sustainability

2.26 As the IT service company is high-dense with people and infrastructure requirements, there is a significant need to ensure they follow sustainable practices which takes care of environment and society at large. There are number of stakeholders involved when it comes to the operational functions of the IT company. It is the responsibility of the IT company to ensure that their needs are addressed and met on a sustainable manner. Some of the key stakeholders are:

1. Investors
2. Customers
3. Vendors / Suppliers
4. Employees
5. Society
6. Regulators
7. Environment, Health and Safety
8. Governments / local legislators

The IT Company is accountable to ensure that all such stakeholders' interests are addressed in the operations of the organization. This is typically reported as part of the **Sustainability Report**, popularly known as **Business Responsibility Report**

The previous trend of losing or backward sustained development in the industry has been replaced. Currently, we can see a number of top corporate bodies serving under the Software industry contributed a lot towards Corporate Social Responsibility (CSR) and society as a whole.

Chapter 3
Special Features of Software Industry

3.1 There are certain special features which are applicable to IT Industry; it might not be applicable to other industries. Some of those features are discussed below in the following paragraphs:

Working from Home

3.2 It is an option increasingly being offered by companies to their employees to better manage their work-life balance by providing them flexibility to work from home. Work from Home (WFH) is now an accepted norm in many companies, especially in the IT sector. As the IT companies work for their clients across the globe in different time zones, their employees are expected to interact with their clients and associates in different locations. A critical point taken into account by a number of companies is that most working people complain of not having enough time to spend with their families. The WFH option offers them the opportunity to gain that much-needed work-life balance and motivates them to put in their best effort at work in return. While employees are happy, employers feel that in these times of high attrition rates, such an option helps in retention. Along with a good pay package and growth opportunity, employees these days are increasingly looking at the work culture of a place before deciding on a job.

Time Sheet Management for Work from Home

3.3 The work from home option is not feasible for all sectors. Only those in which there is minimum personal interaction required, like in some departments of the IT sector, does it work. And in even those, one has to work closely with a supervisor, on a set of deliverables. In such a situation it becomes very important to maintain a time sheet.

The method used to maintain the time sheet should monitor and generate timesheets for each employee which includes a start and end time for each task. A detailed breakdown of tasks as well as the cost incurred for each task should be available. They should report to a supervisor who will monitor the work done by the employees and will approve the time sheet for further processing.

Geographic Spread of Software Industry

3.4 Recent years have seen the increasing geographic distribution of software development. The software industry now tends to relocate its production units in decentralized zones in which a skilled workforce is more readily available, thus taking advantage of political and economic factors. The main objective of this is to optimize resources in order to develop higher quality products at a lower cost. The distance between the different teams can vary from a few meters (when the teams work in adjacent buildings) to different continents. The situation in which the teams are distributed beyond the limits of a nation is called Global Software Development (GSD). This kind of scenario is interesting for several reasons, mainly because it enables organizations to abstract themselves from geographical distance, whilst having qualified human resources and minimizing cost, thus increasing the market area by producing software for remote clients and obtaining a longer workday by taking advantage of time differences. In this context, "offshoring'' refers to the transfer of an organizational function to another country, usually one in which human resources are cheaper. "Onshoring" is the opposite of offshoring. It is the relocation of business processes to a location inside national borders, but in a lower-cost area. Typically, this occurs from a metropolitan, developed area in the country to a non-metropolitan one. "Nearshoring'' is when jobs are transferred to geographically closer countries, thus, avoiding cultural and time differences between members and saving travel and communication costs.

Cloud Computing and Central Servers

3.5 Cloud computing is a model of computing that enables the delivery of computing services over the internet. It is a way of delivering computing services such as servers, storage, databases, networking, software, analytics, and more over the internet. Cloud computing technology is used to provide a wide range of services including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and more.

There are four different models of cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Function as a Service (FaaS).

- Infrastructure as a Service (IaaS) is a cloud computing model in which the service provider provides the customer with the hardware and software infrastructure needed to run applications and services. This includes servers, virtual machines, storage, networking, and other services.

- Platform as a Service (PaaS) is a cloud computing model in which the service provider provides the customer with a platform on which to develop, deploy, and manage applications. This includes the operating system, development tools, database, and other services.
- Software as a Service (SaaS) is a cloud computing model in which the service provider provides the customer with a software application or service. This includes applications such as web-based email, customer relationship management (CRM), project management, and other services.
- Function as a Service (FaaS) is a cloud computing model in which the service provider provides the customer with a platform on which to develop, deploy, and manage functions. This includes functions such as serverless computing, event-driven computing, and other services.

Each of these cloud computing models has its own advantages and disadvantages, so it's important to understand them before making a decision. By understanding the different cloud computing models, one can ensure the best solution is applied to the unique business requirements.

Cloud computing is a colloquial expression used to describe a variety of different computing concepts that involve a large number of computers that are connected through a real-time communication network (typically the Internet). In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. Some of the benefits of cloud computing and central servers are:

- Increase in volume output or productivity with fewer people. Cost per unit, project or product plummets.
- Reduced spending on technology infrastructure.
- People worldwide can access the cloud, provided they have an Internet connection.
- The process will be streamlined.
- It will reduce capital costs as there is no need to spend on hardware, software and licenses.
- It will improve accessibility.
- Projects can be monitored more effectively.
- It will improve flexibility.

Reviewing Cloud Strategy and Governance

- Cloud Strategy and Governance is an integral part of Cloud Computing. It is a process of setting up a plan for how an organization will use the cloud, and what steps they will take to ensure that the cloud is being used in a secure, efficient and cost-effective manner.
- The first step in developing a Cloud Strategy and Governance is to assess the organization's current cloud environment. This includes looking at the existing infrastructure, applications, and services, as well as the security and compliance needs. This assessment should also include an analysis of the cloud providers and services available, and the cost implications of each.
- Once the assessment is complete, the organization can then develop a strategy for how they will use the cloud. This includes deciding which cloud providers they will use, what type of services they will use, and how they will ensure that the cloud is being used securely and cost-effectively. The strategy should also include a plan for how the organization will monitor and manage the cloud environment.
- The next step in developing a Cloud Strategy and Governance is to create a governance framework. This framework should include policies and procedures for how the organization will use the cloud, and who will be responsible for monitoring and managing it. It should also include a risk assessment to identify any potential risks associated with the cloud environment and strategies for mitigating those risks.

The organization should create an implementation plan for how the cloud strategy and governance will be implemented. This plan should include a timeline for implementing the various components of the strategy, as well as budget for the implementation.

Enterprise Blockchain Based Systems

Introduction to Enterprise Blockchain based Systems

3.6 Enterprise Blockchain-based systems, being a part of complex network technology, are an emergent realm in digital transformation that provides a decentralized and distributed ledger system. These systems are mainly used by enterprises for business transactions, increasing transparency and trust between parties, and improving operational efficiency by reducing costs and time.

These systems are primarily designed to transfer and protect valuable data in a secure and scalable way. This is done through the use of cryptography, consensus algorithms, and smart contracts to control and validate transactions within the blockchain.

Enterprise Blockchain-based systems are not just limited to financial transactions, but have also found relevance and applicability in logistics, supply chain management, healthcare, and many more sectors, where data integrity, visibility, traceability, security and automation of processes are of key importance.

However, with the growing expansion of blockchain technology, ensuring the effectiveness and efficiency of these systems, and protecting them from possible risks is crucial. Hence, the importance of carrying out the internal audit for these Enterprise Blockchain-based systems, which is the focus of this Technical Guide. An internal audit serves to review whether the blockchain system is adhering to established governance procedures, risk controls, and compliance regulations, making the entire blockchain operation more secured, reliable and trustworthy for all parties involved.

Thus, such audits provide deep insight into the functioning of these systems so as to robustly manage the operations, while giving the stakeholders a confidence about the governance and risk management aspects of the blockchain systems being used by the respective enterprises.

1. Evolution of Blockchain Technology

Blockchain technology, also referred to as Distributed Ledger Technology (DLT), has rapidly evolved from a technological framework that underpins cryptocurrencies, such as Bitcoin, to a transformational technology with potential applications in various aspects of business. The onset of this revolutionary technology can be traced back to the aftermath of the 2008 financial crisis, which drove a demand for a decentralized and transparent system of transactions, devoid of central interference.

Blockchain emerged in 2009 as the backbone of Bitcoin, as a public, transparent ledger that records all transactions of the digital currency. This first generation blockchain focused primarily on enabling peer-to-peer transactions of digital assets in a secure and anonymous environment.

The second generation of blockchain introduced the concept of programmable contracts, also known as smart contracts. Ethereum, unveiled in 2015, was the first to leverage this technology. Smart contracts enabled blockchain to stretch beyond mere transactions, allowing the execution of

complex applications, such as Decentralized Autonomous Organizations (DAOs).

In the current wave, i.e., the third generation of blockchain, the technology is being tailored to suit various industry requirements, such as scalability, inter-blockchain communication, energy efficiency, and regulatory compliance. Noteworthy examples include Cardano and IOTA.

A. Types and categories of Blockchain

Public Blockchains

Public blockchains are open, permissionless systems where anyone can join, validate transactions, run nodes, etc. Examples include Bitcoin and Ethereum. While public blockchains are transparent, they can pose certain risks, including privacy and scalability issues, which the audit needs to assess.

Private Blockchains

Private blockchains are closed, permissioned systems where only selected entities can join or validate transactions. Due to their restricted nature, private blockchains often come with higher risks regarding centralization and potential manipulation – crucial factors for the audit team to consider.

Consortium Blockchains

These are semi-decentralized and operate under the leadership of a group or consortium. Auditing such systems require ensuring that all group members follow the prescribed protocols and tackle risks associated with consortium disagreements or discrepancies.

Hybrid Blockchains

Hybrid blockchains combine elements of public and private blockchains. They allow selected parties to access certain data while keeping other data public. The audit team must therefore be well-equipped to handle the complexity of auditing these dual systems.

B. Other Considerations

Tokenized Blockchains

These blockchains use a digital token or cryptocurrency as an integral part of their functioning. Audits for these systems should be capable of verifying transactions and ensuring the proper functioning of the underlying token economics.

Smart Contracts

Found in systems like Ethereum, smart contracts self-execute transactions under specific conditions. Auditors are required to test the appropriate design and adequate controls of these smart contracts.

Interoperable Blockchains

Interoperable blockchains are able to share and access information across different blockchain networks. Auditing these systems implies a robust understanding of multiple blockchain environments and the security controls for data exchange.

Decentralized Finance (DeFi)

The DeFi applications run on blockchain, typically public, and deal with financial transactions and contracts. The audit teams need to ensure appropriate risk management practices are in place due to high risks of DeFi operations.

2. Role of Blockchain in Enterprise Systems

Enterprise blockchain systems are specifically designed for business processes, focusing on scalability, efficiency, security, and privacy. Here are keyways in which they have been leveraged:

- Security and Trust: Blockchain's immutable and transparent nature greatly amplifies the trust in the system and significantly reduces the fraud risk.
- Increased Efficiency: Blockchain can streamline cumbersome processes, automate routine tasks through smart contracts, and eliminate intermediaries, leading to substantial cost savings and increased efficiencies.
- Traceability and Transparency: In supply chain and logistics, blockchain has provided unprecedented traceability, enabled real-time tracking of goods, and ensured authenticity.
- Interoperability: Blockchain facilitates more efficient data exchanges between different systems, thereby improving interoperability.

3. Internal Audit of Enterprise Blockchain-Based Systems

Given the unique characteristics of blockchain, internal audit professionals must adapt their audit techniques to provide effective assurance. They may

understand the distributed nature, consensus mechanisms, cryptography, and smart contract functionality. The audit approach may include substantial testing on the design and operating effectiveness of systems' controls, evaluation of governance structures over the blockchain, and verification of compliance with legal and regulatory standards.

4. Focusing on Security

In an enterprise blockchain-based system, the security of data, transactions, and digital assets is of critical importance. The internal audit team needs to thoroughly evaluate the framework of security controls to ensure they are robust and working as expected.

Understanding Blockchain Security: A strong understanding of the blockchain's operational and security infrastructure is crucial for auditors. Familiarize yourself with key aspects such as consensus mechanisms, node security, private key management, smart contract validity and so on.

Risk Assessment: Conduct a blockchain-specific risk assessment focusing on security. Identify potential weaknesses that might lead to unauthorized access to data, fraud or cyber threats. Review the architecture, the encryption methods used, the integrity of the chain, the validation processes, and the disaster recovery procedures in place.

Private Key Security: In any blockchain system, private keys are a vital layer of security. Regular audits must be done to ascertain that keys are securely stored, confidentiality is maintained, and they are safeguarded from loss.

Smart Contract Validity: Smart contracts are integral to most enterprise blockchains. Auditors should substantiate that they've been correctly implemented and test them for vulnerabilities (like re-entrancy, arithmetic overflows, etc.) using forensic techniques.

Node Security: Conduct regular audits to evaluate node security. Consider aspects like permissions, firewalls, and protocols in place to limit access, secure data, and prevent DoS attacks.

Consensus Mechanism and Control Activities: In the context of different consensus algorithms (e.g. Proof of Work, Proof of Stake, or Delegated Proof of Stake), check whether the system is operating in a reliable manner. Auditors should understand how control activities are performed and assess their effectiveness.

Blockchain forks: Audit must ascertain that appropriate controls are in place to avoid losses or uncertainty during blockchain forks.

Monitoring and Updating: Ensure robust monitoring systems are in place to identify potential security threats in real-time. Also, evaluate the system's capability to keep up-to-date with global blockchain developments and threat patterns.

Chain Forensics: Frequently examine all transactions in the chain. The investigation can expose suspicious activity, help track assets, and verify data integrity.

Regulatory Compliance: Compliance with applicable regulations should always be part of the audit scope. Review internal policies to ensure they are in line with regional and global benchmarks or regulatory requirements.

Audit Reporting: The final audit report should be comprehensive, covering all the audit processes and findings. The report should draw out areas of concern, security points that need stronger controls and actions taken to mitigate identified risks.

5. Key Internal Control Mechanisms

User Access Controls:

Controlling who has access to blockchain data is crucial. Access permissions should be granted on a need basis along with stringent password policies. A segregation of duties can further curtail the risk of unauthorized transactions.

Data Integrity and Validation:

Blockchains rely on the accuracy of the data input. Therefore, measures must be taken to ensure the accuracy and completeness of source data. This can be done via automated data validation checks.

System Resilience:

The blockchain network should be robust enough to withstand malicious attacks. Security measures like cryptographic functions, consensus protocols, strong network architecture and regular penetration testing can ensure its resilience.

Control Over Cryptographic Keys:

Management of cryptographic keys is essential to safeguard transactions and data within the blockchain. Keys should be securely stored and immediately revoked when lost or no longer needed. In case custodian is involved then comfort on the controls at custodian end should also be obtained.

Smart Contract Controls:

Smart Contracts automatically execute transactions when conditions get fulfilled. They should be audited to detect vulnerabilities that could compromise the transactions. In private blockchain specifically these controls are more critical as often they don't augment trust from decentralization but derive the same from the authorization and access controls.

The chosen internal control mechanisms need to be considered in the broader context of the organization's blockchain strategy. All parties involved in the implementation and operation of blockchain controls must understand their individual responsibilities. Control mechanisms should be periodically reviewed and tested for effectiveness.

6. Key Factors to Consider During Audit

Public and Private Nodes: In a public blockchain, all transactions are visible to anyone. Conversely, in a private blockchain operated by an enterprise, the visibility may be limited to certain nodes. On such networks, the auditor should examine access restrictions and their implications on transparency.

Smart Contract Functioning: Smart contracts execute transactions and the process should be transparent to all parties involved. The audit should verify the proper functioning and sufficient transparency of these contracts.

Validation Processes: The process through which transactions are approved or declined should be open and understood by all participants.

Data Management: Management of the system's blockchain data is crucial. All changes and updates should be transparent.

7. Auditing Techniques

Document Review: Review system and network documentation detailing blockchain operation.

Interviews: Conduct interviews with system administrators and users for insight into operations.

System Tracing and Chain Analysis: Trace sample transactions through the system to verify transparent processing.

Standard Auditing Framework for Artificial Intelligence

Artificial intelligence (AI) and Machine Learning (ML) technology are transforming business processes across industries, creating new opportunities but also bringing many challenges, including managing and mitigating risk. One way to address these challenges can be through auditing of AI systems, and to do so, a Standard Auditing Framework for AI can be a vital tool.

A Standard Auditing Framework for AI (SAFAI) concerns itself with evaluating AI systems' design, development, deployment, and operation. It is an analysis designed to assess AI's impact, performance, reliability, safety, and transparency.

1. Components of a Standard Auditing Framework for AI

Fairness: This involves testing whether the AI system is biased or not, and how it affects its decision-making processes. It also involves a comprehensive analysis of the AI's dataset and how it is collected and processed.

Transparency: An AI system's decision-making process should be transparent and explainable. Auditors must be able to understand and inspect how the AI system makes its decisions.

Robustness: This measures an AI system's ability to continue functioning correctly amidst changes in the environment or the presence of adversarial attacks.

Reliability: This involves testing the AI system's consistency in decision-making processes. It should provide reliable output regardless of the changes in input.

Privacy: Auditors should ascertain whether an AI system is respecting privacy rights and regulations. This includes how it collects, processes and stores personal information.

2. Key Stages in Auditing of AI Systems

Planning: This involves identifying key areas of focus, understanding how the AI system works, its purpose, and setting the scope and objectives of the audit.

Fieldwork: This includes conducting tests and reviews, including examining models, datasets, decision-making processes, fairness, and privacy measures.

Reporting: Documenting findings, identifying areas of improvements and providing recommendations.

Regular Review and Follow-Up (Post-Audit): This helps to know if the recommendations made during the audit have been implemented and to evaluate AI systems' overall performance.

Regulators globally are identifying the need for an AI auditing framework, including Singapore's Personal Data Protection Commission (PDPC) that released the Model AI Governance Framework, or the UK's Information Commissioner's Office (ICO). However, it's important to note that this field is relatively new, and there is still ongoing work globally to establish standardized best practices for AI auditing. In India NASSCOM has issued several white papers on AI.

3. Specific Requirements for AI Audits

Artificial Intelligence (AI) has become a valuable tool in many industries and fields, including audits. However, the nature of AI applications requires specific needs to be met to ensure its safe, efficient, and effective use. Here are some crucial elements required for AI audits:

1. **Verification and Validation:** AI applications should always be verified and validated to ensure they are working as intended. This can involve making sure the algorithms are coded correctly, cross-checking system outputs with manual calculations, and verifying the AI outputs against expectations and real-world outcomes.

2. **Understandability and Explainability (xAI):** AI auditors must be capable of interpreting and explaining how the AI system works, including its decision-making process. This is essential for building trust and confidence amongst stakeholders. There are various frameworks (like IBM openscale AI, H2O.ai etc) which supports model explainability.

3. **Data Integrity and Quality:** The AI system needs clean, reliable, and high-quality data to function correctly. Auditors must assess data used and generated by the AI system for accuracy and integrity.

4. **Security and Privacy:** Auditors must ensure that the AI system maintains established security standards and meets necessary privacy requirements. This can include verifying that the system has robust

cybersecurity measures in place and adheres to data privacy laws such as The Digital Personal Data Protection 2023 or GDPR.

5. Compliance: The AI system should be compliant with applicable legal, regulatory, and professional standards. These can differ depending on the use case and jurisdiction.

6. Impact Assessment: Auditors must appraise the potential impacts (both positive and negative) of the AI system. This may include analysis of technical, operational, organizational, societal impacts, and more.

Accounting of Software Tools

3.6 A software company will be utilizing a lot of softwares to run its own business. Few of the softwares might be purchased and the rest developed by the company itself. Such softwares will be of high cost and it has to be verified that such expenses are capitalised. The provisions relating to intangibles as per Accounting Standard (AS) 26 have to be followed. If the software is purchased, then it has to be entirely capitalised but if the same is internally generated then it has to be verified if the treatment of the expenses in the research stage and the development stage are in accordance with AS 26.

Project wise Costing

3.7 The software companies will be serving many clients and usually maintain accounts in such a way as to ascertain the project wise costing of all the projects in hand. If the books of accounts are maintained for the company on an overall basis and not bifurcating the projects the management should be in a position to identify the costs to be allocated and be in a position to determine the profitability of the individual projects.

Legal Software

3.8 Software piracy is copying and use of software without proper license from the developer. Similarly, simultaneous use of single user license software by multiple users or loading of single user license software at multiple sites also amounts to software piracy. Using trial version software for commercial gains is also piracy. Piracy is punishable offence. By using legal licensed software, it is ensured that critical updates are available when needed, the products are fully supported, reliable and above all it is legal. Any person or company who indulges in unauthorized copying, sale,

downloading or loading of software is punishable by imprisonment or by fine. Hence, the software companies should use legal versions of the software.

Confidentiality of Source Code

3.9 IT companies should have a secure network complete with firewall, anti-spyware and ant-virus mechanisms to guard itself against threats from outside. But often the threat is more from inside than from outside and this is what companies often ignore. Perpetrators of information theft often resort to social engineering methods than hacking to gain access to confidential information. Software companies should opt for employee surveillance measures like monitoring of e-mails and IMs to be informed of any possible information theft. Cyber criminals often target smaller companies which handle confidential information. In order to protect such confidential information and source codes the company has to restrict the access of source codes. It also has to enter into a non-disclosure agreement with the employees to safeguard its source code.

Software Used for Internal Use

3.10 Due to the advent of technology most of the software companies use softwares for internal use like, leave management, payroll management, HR records, performance appraisal, and intranet for communication of policies. Due to such softwares, there might not be any manual record maintained for such purposes. Hence, the internal auditor has to verify the data maintained in the softwares commensurate with the size of the company. The Internal Auditor may run some test checks in such softwares. In case, there ais discrepancy the internal auditor may suggest measures to the management to control it.

Chapter 4
Legal Framework

Governing Regulations

4.1 In recent times, software development and technical competence, domain knowledge, information technology enabled services experience and expertise for offering quality IT (ITES) including business process outsourcing services and their exposure to working on BPO knowledge process outsourcing various platforms and systems services industry in India has emerged as one of the most dynamic and vibrant sectors in India's economy.

The Government of India has announced promotion of IT as one of the top priorities of the country. India has embarked on a policy agenda which aims to restructure its economy with enhanced global participation. The FDI to supplement domestic investment in for achieving a quantum jump in growth rate is now an integral part of Government of India policy initiative impairing the greater transparency to business procedure and integration with the global marketplace are seen as the hallmark of new industrial, trade and fiscal policies.

Some of the Act that applicable to IT Industry are as follows:

Information Technology Act, 2000

The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures. It also defines cybercrimes and prescribes penalties for them. The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Indian Information Technology Act addresses the following issues:

- Tampering with computer source documents
- Hacking with computer system
- Receiving stolen computer or communication device
- Using password of another person
- Cheating using computer resource

- Publishing private images of others
- Acts of cyberterrorism
- Publishing information which is obscene in electronic form, etc.

The Reserve Bank of India (RBI) Guidelines for IT Governance and Security

The Reserve Bank of India (RBI) has issued guidelines for IT governance and security for banks and other financial institutions. The guidelines aim to ensure the confidentiality, integrity, and availability of information.

The Digital Personal Data Protection Act, 2023

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

National Cyber Security Policy-2013

The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace.

Governing Regulators

Ministry of Electronics & Information Technology

4.2 The Ministry of Electronics and Information Technology is an Indian government ministry.

Mission

To promote e-Governance for empowering citizens, promoting the inclusive and sustainable growth of the Electronics, IT & ITeS industries, enhancing India's role in Internet Governance, adopting a multipronged approach that includes development of human resources, promoting R&D and innovation, enhancing efficiency through digital services and ensuring a secure cyber space.

Objectives

- e-Government: Providing e-infrastructure for delivery of e-services
- e-Industry: Promotion of electronics hardware manufacturing and IT-ITeS industry
- e-Innovation / R&D: Implementation of R&D Framework - Enabling creation of Innovation/ R&D Infrastructure in emerging areas of ICT&E/Establishment of mechanism for R&D translation
- e-Learning: Providing support for development of e-Skills and Knowledge network
- e-Security: Securing India's cyber space
- e-Inclusion: Promoting the use of ICT for more inclusive growth
- Internet Governance: Enhancing India's role in Global Platforms of Internet Governance.

Functions of Ministry of Electronics and Information Technology

1. Policy matters relating to information technology; Electronics; and Internet (all matters other than licensing of Internet Service Provider).
2. Promotion of internet, IT and IT enabled services.

2A. Promotion of Digital Transactions excluding Digital Payments.

3. Assistance to other departments in the promotion of E-Governance, E-Commerce, E- Medicine, E- Infrastructure, etc.
4. Promotion of Information Technology education and Information Technology-based education.
5. Matters relating to Cyber Laws, administration of the Information Technology Act. 2000 (21 of 2000) and other IT related laws.

5A. Matters relating to online gaming.

6. Matters relating to promotion and manufacturing of Semiconductor Devices in the country.
7. Interaction in IT related matters with international agencies and bodies e.g. Internet for Business Limited (IFB), Institute for Education in Information Society (IBI) and International Code Council — online (ICC).
8. Initiative on bridging the Digital Divide: Matters relating to Digital India Corporation.

9. Promotion of Standardization, Testing and Quality in IT and standardization of procedure for IT application and Tasks.
10. Electronics Export and Computer Software Promotion Council (ESC).
11. National Informatics Centre (NIC).
12. Initiatives for development of Hardware/Software industry including knowledge—based enterprises, measures for promoting IT exports and competitiveness of the industry.
13. All matters relating to personnel under the control of the Ministry.
14. Unique Identification Authority of India (UIDAI).
15. Semi-Conductor Laboratory, Mohali.

MeitY Organisations

Attached Offices of MeitY

- National Informatics Centre (NIC)
- Standardisation, Testing and Quality Certification (STQC) Directorate

Statutory Organisations of MeitY

- Controller of Certifying Authorities (CCA)
- Indian Computer Emergency Response Team (ICERT)
- Unique Identification Authority of India (UIDAI)

Section 25 Companies of MeitY

- Digital India Corporation(DIC)
    1. NeGD
    2. MyGov
- National Informatics Centre Services Inc.(NICSI) (PSE under control of NIC)
- National Internet Exchange of India(NIXI)

Autonomous Societies of MeitY

- Bhaskaracharya National Institute for Space Applications and Geo-informatics(BISAG-N)
- Centre for Development of Advanced Computing (C-DAC)
- Centre for Materials for Electronics Technology (C-MET)

- Education & Research in Computer Networking(ERNET)
- National Institute of Electronics and Information Technology (NIELIT - Formerly DOEACC Society)
- Society for Applied Microwave Electronics Engineering and Research (SAMEER)
- Software Technology Parks of India (STPI)
- Semi-Conductor Laboratory

Company registered under Company Act, 1956

- CSC e-Governance Services India Ltd.

The Government of India (GoI) has taken various initiatives to promote Information Technology and Information Technology enabled Services (IT/ ITeS) sector in the country. Some of the initiatives are as detailed below:

National Association of Software and Services Companies (NASSCOM)

4.3 The National Association of Software and Services Companies (NASSCOM), a not-for-profit industry association, is the apex body for the $245 billion technology industry in India, an industry that has made a phenomenal contribution to India's GDP, exports, employment, infrastructure and global visibility. In India, this industry provides the highest employment in the private sector.

Established in 1988 and ever since, NASSCOM's relentless pursuit has been to constantly support the technology industry, in the latter's continued journey towards seeking trust and respect from varied stakeholders, even as it reorients itself time and again to remain innovative, without ever losing its humane and friendly touch.

NASSCOM is focused on building the architecture integral to the development of the technology sector through policy advocacy and help in setting up the strategic direction for the sector to unleash its potential and dominate newer frontiers.

NASSCOM's members, 3000+, constitute 90% of the industry's revenue and have enabled the association to spearhead initiatives at local, national and global levels. In turn, the technology industry has gained recognition as a global powerhouse.

Software Technology Parks of India (STPI)

4.4 Software Technology Parks of India (STPI) is a government agency in India, established in 1991 under the Ministry of Communications and Information Technology that manages the Software Technology Park scheme.

Software Technology Park (STP) Scheme

The STP Scheme is a 100% export-oriented scheme for the development and export of computer software, including export of professional services using communication links or physical media. As a unique scheme, it focuses on one sector, i.e., computer software. The scheme integrates the government concept of 100% Export Oriented Units (EOU) and Export Processing Zones (EPZ) and the concept of Science Parks/Technology Parks, as operating elsewhere in the world. The unique feature of the STP scheme is the provisioning of single-point contact services for member units, enabling them to conduct exports operations at a pace commensurate with international practices.

Scheme Benefits and Highlights

- Approvals are given under single window clearance system.
- An STP unit may be set up anywhere in India.
- Jurisdictional STPI authorities can clear projects costing less than Rs.100 million with Indian Investment.
- 100% foreign equity is permitted.
- All the imports of Hardware & Software in the STP units are completely duty free, import of second-hand capital goods are also permitted.
- Re-export of capital goods is also permitted.
- Simplified Minimum Export Performance norms i.e., "Positive Net Foreign Exchange Earnings".
- Use of computer system for commercial training purposes is permissible subject to the condition that no computer terminals are installed outside the STP premises.
- Sales in the Domestic Tariff Area (DTA) are permissible.
- The capital goods purchased from the DTA are entitled for refund of GST.

- Capital invested by foreign entrepreneurs, know-how Fees, royalty, dividend etc., can be freely repatriated after payment of Income Taxes due on them, if any
- The items like computers and computers peripherals can be donated to recognized non-commercial educational institutions, registered charitable hospitals, public libraries, public funded research and development establishments, organizations of Govt. of India, or Govt of a State or Union Territory without payment of any duties after two years of their import.
- 100 Percent Depreciation on computers and computer peripherals over a period of five years.

(Source: https://stpi.in/en/statutory-services)

Special Economic Zones (SEZs) Act, 2023

Ministry of Commerce and Industry has issued the Special Economic Zones (Third Amendment) Rules 2023, which bring significant changes to the import and export procedures of ships by units operating in the International Financial Services Centre.

The SEZ Act, 2005, supported by SEZ Rules, came into effect on 10th February, 2006, providing for simplification of procedures and for single window clearance on matters relating to central as well as state governments. The main objectives of the SEZ Act are:

- generation of additional economic activity
- promotion of exports of goods and services
- promotion of investment from domestic and foreign sources
- creation of employment opportunities
- development of infrastructure facilities

The exports by IT/ITeS units in SEZs for the year 2020-21 were Rs. 5.1 lakh crore.

i. **National Policy on Software Products-2019:** GoI has approved National Policy on Software Products-2019 with an aim to develop India as the global software product hub, driven by innovation, improved commercialization, sustainable Intellectual property (IP), promoting technology start-ups and specialized skill sets, for development of the sector, based on ICT. The objective of the policy is

to create a robust Indian Software Product development ecosystem leading to ten-fold increase in India share of the Global Software product market and so as to generate direct and in-direct employment for 3.5 million people by 2025.

ii. **Next Generation Incubation Scheme (NGIS)** has been approved to support software product ecosystem and to address a significant portion of National Policy on Software Product (NPSP 2019). It is envisaged to create a vibrant software product ecosystem to complement the robust IT Industry for continued growth, new employment and enhance competitiveness.

iii. Some other initiatives to promote IT sector exports include Future Skills PRIME, Market Development Initiative in Nordics and Africa Region, Market Outreach Initiatives etc. under Champion Sector Services Scheme (CSSS).

This information was given by the Minister of State in the Ministry of Commerce and Industry, Smt. Anupriya Patel, in a written reply in the Rajya Sabha.

(Source: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1797593)

A Gist of Important Regulations that may be Applicable to Software Industry

4.13 The important regulations that may be applicable to Software Industry are as follows:

- The Companies Act, 2013
- Partnership Act, 1932 / Limited Liability Partnership Act, 2008
- Shops and Establishments Act of respective states.
- The Sale of Goods Act, 1930
- The Negotiable Instruments Act, 1881
- The Income tax Act, 1961
- Service Tax under the Finance Act, 1994
- The Indian Contract Act, 1872
- Sales tax Act of respective states
- Foreign Exchange Management Act 1999

- Information Technology Act 2000
- State Specific Shops and Establishment enactments.
- Central Excise and Customs Act
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- The Payment and Settlement Systems Act, 2007
- The Reserve Bank of India (RBI) Guidelines for IT Governance and Security
- Personal Data Protection Bill, 2019
- Cyber Security Policy, 2013
- Patents Act, 1970
- Copyright Act, 1957
- Trademarks Act, 1999
- Consumer Protection Act, 2019

Chapter 5
Risk Assessment and Internal Controls

5.1 As multinational enterprises have recognized an increasing array of risks facing the organization, it is no surprise that the demand for risk management professionals has risen dramatically. Any disciplined approach to growth and value creation assumes that the organization is managing all manner of significant and likely risks effectively. Risk can be considered both at the macro or portfolio level (enterprise-wide risk management) as well as the micro or departmental level. Risk management is frequently an area in which internal audit can contribute greatly by furnishing analyses and providing wise counsel to top management and the board of directors.

The internal audit function also performs micro level risk assessment for its own purposes to identify those areas which demand the greatest efforts on the part of the internal audit function and for achieving appropriate audit coverage of the audit universe over defined periods of time. Internal auditors can play a significant “partnering” role with management in establishing and monitoring business processes for the assessment, measurement, and reporting of risks in general and in implementing enterprise risk management initiatives.

Modern approaches to risk-based internal auditing allow for the assessment of risks and linking them to business objectives systematically. Indeed, the internal audit function can facilitate the processes by which business units “can develop high quality risk assessments,” and this can in turn be very useful to the internal audit function in planning its own work, primarily by enhancing the quality of decision-relevant information and minimizing duplication of effort.

Business Risks

5.2 Business risks can be uncertainty in profits or danger of loss and the events that could pose a risk due to some unforeseen events in future. Business risks may take place in different forms depending upon the nature and size of the business. Business risks can be categorized as, internal risks which arise from the events taking place within the organization and external risks which arise from the events taking place outside the organization. Business risks can be further classified into following:

(i) Strategic Risk

These are risks associated with the operations of that particular industry. It can be caused by changes in supply and demand, competitive structures, and introduction of new technologies, mergers and acquisitions. Strategic risks are also determined by board decisions about the objectives and direction of the organisation. Sometimes strategic risks are often risks that

organisations may have to take in order to expand, and even to continue in the long term. An organisation may accept other strategic risks in the short term but take action to reduce or eliminate those risks over a longer timeframe.

(ii) Economic/ Financial Risk

These are risks associated with the financial structure and transactions of the particular industry. Also the possibility that shareholders will lose money when they invest in a company that has debt, if the company's cash flow proves inadequate to meet its financial obligations. When a company uses debt financing, its creditors will be repaid before its shareholders if the company becomes insolvent.

(iii) Operational Risk

These are risks associated with the operational and administrative procedures of the particular industry. Few of the examples of such risks are, misappropriation of assets, theft of information, fictitious employees, misrepresentation of cash balances, third-party theft and forgery, data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets, etc.

(iv) Compliance Risk (Legal Risk)

These risks are associated with the need to comply with the rules and regulations of the government. There are various Acts which are applicable to the software companies. The company has to comply with a variety of compliances as per various Acts. Even if the company does not comply with any one of the statutory compliances the respective government department will issue notices and also might levy fine and penalty. Hence the company has to employ well trained staff to follow all the compliance requirements.

(v) Disaster Risk

There would be different risks like, natural disaster (floods) and others depend upon the nature and scale of the industry. It has been dealt with in the Business continuity plan mentioned below.

(vi) Political Risk

It refers to the complications businesses may face as a result of what are commonly referred to as political decisions that alters the expected outcome and value of a given economic action. For example, political decisions by governmental leaders about taxes, currency valuation, trade tariffs or

barriers, investment, wage levels, labour laws, environmental regulations and development priorities, can affect the business conditions and profitability. Similarly, non-economic factors like, political disruptions such as, terrorism, riots, coups, civil wars, international wars, and even political elections that may change the ruling government, can dramatically affect businesses' ability to operate. Political risk is extremely difficult to quantify yet the companies and investors must examine and understand the potential for political risks. Companies should have a comprehensive framework for identifying and assessing all the risks they face, and assessing the impact of risk. Such a framework enables development of mitigation strategies that support company operations through crisis and change. The formal process of gathering and assessing data on political developments should be overseen by a risk manager and disseminated at the corporate, operating unit, and regional level. Companies must monitor political risk on an ongoing basis and use this information proactively to inform investment and operating decisions. At the same time companies have to capitalize on opportunities resulting from political change.

(vii) Human Capital Risk

It refers to the gap between the goals of the organization and the skills of the workforce. Indian IT sector has become an HR manager's nightmare. Their biggest challenge is marinating good people in organisation and keeping the attrition rate in control. The demand for good resources is more than the present supply and they are paid premium salaries. The rising cost of people is reducing the profit margins of the companies though the profit has been increasing by leaps and bounds. With many global companies opening up captives in India to reduce their cost of operations the salaries have shot northward and this has augmented the trouble of Indian IT players. The supply and demand of quality engineers who are capable of working in the IT field is having a huge gap. Companies have started looking for additional options of hiring science graduates and providing them adequate training to enable them to work in IT sector, but still the quality of talent is declining which in turn means lack of quality in work. Companies are struggling to hire new resources and salary war is becoming worse every day.

(viii) Brand/ Reputation Risk

Every company, every organization develops a reputation and, while it may take many years to form and is usually quite durable, a company's reputation can be undone in fairly short period. Reputation is more than just a company's good name, it's a composite of those factors affecting how others, particularly those outside of the organization, view the company.

Safeguarding a company's reputation has become a key factor in every company's long-term strategic planning. To safeguard the reputation of a company regular investment in the structures, activities, staff, is essential. The company must take steps to measure its reputation in the market by opting for brand valuation. The checklist for brand valuation is given in the relevant section below.

(ix) Technology Risk

One of the main risk in technology implementation is to keep it relevant. Sometimes, in case of emerging technologies where the underlying technologies are rapidly changing, it becomes difficult to manage technological obsolesce.

Security by Design is a concept of implementing effective security measures at the beginning of system or application design, rather than adding them in later stages. The idea is to identify and mitigate potential security risks during the design phase, thereby making the system more robust against potential threats. This approach considers security in every part of the software development process and requires a comprehensive understanding of how potential attackers may interact with the system.

On the other hand, Zero Trust Security Framework is a security strategy based on the principle of maintaining stringent access controls and not trusting any entity by default, regardless of their location or whether the request comes from inside or outside the network. This approach demands that every user and device is authenticated and authorized before accessing the system resources, therefore reducing the risk of insider threats and data breaches. It also includes a least privilege strategy, meaning granting users only the permissions they need to perform their work. Both Security by Design and Zero Trust are significant in achieving a robust security posture.

(x) Cyber Security Risk

The IT industry faces various cybersecurity threats and challenges, including hacking, phishing, and malware attacks. These threats can result in data breaches, financial loss, and damage to reputation. To combat cybersecurity threats, the Indian government has introduced various compliances like the IT Act, 2000, and the Cyber Security Policy, 2013. These compliances aim to ensure that organizations implement adequate security measures to protect their IT infrastructure.

The Indian Computer Emergency Response Team (CERT-In): The Indian Computer Emergency Response Team (CERT-In) is the nodal agency

responsible for responding to cybersecurity incidents in India. It provides support to government agencies, critical infrastructure, and other organizations to enhance their cybersecurity readiness and prevent cyber-attacks. CERT-In operates 24/7 and offers a range of services, including incident response, vulnerability assessment and penetration testing, and security audit and compliance. It also collaborates with international organizations and governments to exchange information and best practices in the field of cybersecurity. CERT-In has played a critical role in addressing major cyber-attacks in India, such as the 2016 cyber-attack on Indian banks and the 2017 WannaCry ransomware attack. By providing timely and effective response to cyber incidents, CERT-In has helped to safeguard India's digital assets and promote a secure and resilient cyberspace.

In order to mitigate the above-mentioned risks it is necessary for the company to have a proper control of the operations of the business.

The ICAI has issued Standard on Internal Audit (SIA) 130, Risk Management. The Internal Auditor may refer this Standard in detail to understand the important terms, various responsibilities of Management and Internal Auditor and how this Standard may be used in the context of mitigating and managing risks.

Risk Mitigation Techniques

5.3 The Management may follow the following Risk Mitigation Techniques:

- In the current environment, the entity should be fully aware of the risks and implement risk management practises and programmes to handle those risks.
- Prioritising risks, developing a plan to strategically manage risks, implementing the plan and monitoring plan execution and evaluate and suggest improvements thereto.
- It may be necessary for the entity to have a comprehensive insurance policy to cover a large portion of the risks.
- The installation of a risk identification system would be required. The Management Information System should have specific yardsticks that will allow management to identify important risks and their impact on the company.

The internal auditor may conduct a comprehensive assessment of risks and advise on risk mitigation strategies. For this purpose, the internal auditor may create a questionnaire or a checklist.

Internal Control

5.4 Standard on Internal Audit (SIA) 120, "*Internal Controls*" as issued by the ICAI states that Internal Controls are systemic and procedural steps adopted by an organization to mitigate risks, primarily in the areas of financial accounting and reporting, operational processing and compliance with laws and regulations.

5.5 Internal Controls (ICs) are essentially risk mitigation steps taken to strengthen the organization's systems and processes, as well as help to prevent and detect errors and irregularities.

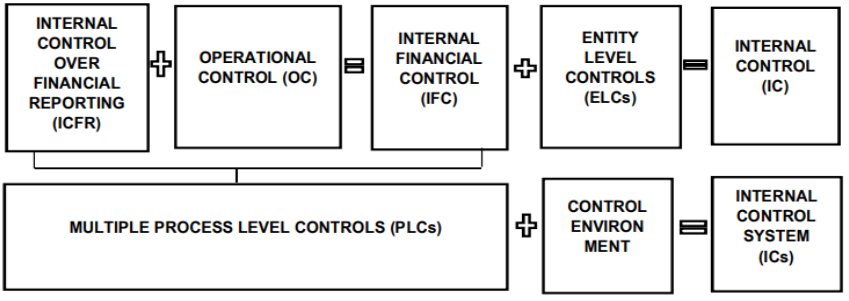
5.6 The actual steps of mitigation (e.g., review, approval, physical count, segregation of duty, etc.) are referred to as "Control Activities". When ICs mitigate the risk of financial exposure, they are also referred to as Internal Financial Controls (IFCs) and when they mitigate operational risks, they are also referred to as Operational Controls (OCs). ICs generally operate with human intervention (Manual Controls), but in an automated environment, computer controls are deployed to secure the systems and called IT General Controls (e.g., access controls) or check transaction processing at an application level and called Application Controls (e.g., sequential numbering of invoices, etc.).

5.7 The term "Internal Controls System" is an all-encompassing term generally used to refer all types of controls put together, covering ELCs, IFCs and OCs. The Control Environment (ELCs) includes the overall culture, attitude, awareness and actions of Board of Directors and management regarding the internal controls and their importance to the organization. The control environment has an influence on the effectiveness of the overall Internal Control System since it provides the basis for establishing and operating process level controls (such as IFC and OCs) in the organization.

5.8 The internal auditor may obtain an understanding of the significant processes and internal control systems sufficient to plan the internal audit engagement and develop an effective audit approach. The internal auditor should use professional judgment to assess and evaluate the maturity of the entity´s internal control. The auditor should obtain an understanding of the

control environment sufficient to assess management´s attitudes, awareness and actions regarding internal controls and their importance in the entity.

5.9 Below is a pictorial depiction of Internal control and Internal control systems:



Chapter 6
Internal Audit Approach

6.1 Effective Internal Audit provides a tool to ease out all complexities, ensures that systems and processes are adequate to support the growth and are adapted to the changes in various regulations, thereby ensuring sustained growth and development.

6.2 The following points highlight importance of internal audit:

- Understanding and assessing the risks and evaluate the adequacies of the prevalent internal controls.
- Identifying areas for systems improvement (manual and by automation support) and strengthening controls.
- Ensuring optimum utilization of the resources of the entity, for example, human resources, physical resources, etc.
- Ensuring proper and timely identification of liabilities, including contingent liabilities of the entity and taking a merit-based view on contingent liabilities.
- Ensuring compliance with internal and external guidelines and policies of the entity as well as the applicable statutory and regulatory requirements.
- Safeguarding the assets of the entity and adequacy of title to the assets.
- Reviewing and ensuring adequacy of information systems security and control.
- Reviewing and ensuring adequacy, relevance, reliability and timeliness of management information system flowing from common data base.

6.3 Framework Governing Internal Audits, issued by the Institute of Chartered Accountants of India defines the term Internal Audit as:

*"*Internal audit provides independent assurance on the effectiveness of internal controls and risk management processes to enhance governance and achieve organisational objectives.*"*

Brief explanation of the key terms used above is as follows:

(i) Independence: Internal audit shall be an independent function, achieved through the position, organization structure and reporting of the internal auditor. At times, in addition to providing assurance, the internal auditor may adopt an advisory role to help an organization achieve its objectives, provided this does not compromise the independence of the internal auditor.

(ii) Internal controls and risk management are integral parts of management function and business operations. An internal auditor is expected to evaluate the design and operating effectiveness of internal controls and risk management processes (including reporting processes) as designed and implemented by the management.

(iii) Governance is a set of relationships between the company and its various stakeholders and provides the structure through which the company's objectives are achieved. It includes compliance with internal policies and procedures and laws and regulation.

(iv) Organizational objectives incorporate the interests of all stakeholders and include the short- and medium-term goals that an organisation seeks to accomplish.

Standards on Internal Audit

6.4 Internal auditor should carefully go through Standards on Internal Audit (SIAs) issued by ICAI. Standards on Internal Audit (SIA) is recommendatory in nature for the initial period. These standards shall become mandatory on such date as notified by the Council.

These standards have been classified and renumbered as follows:

(i) 100 Series: Standards on Key Concepts

(ii) 200 Series: Standards on Internal Audit Management

(iii) 300-400 Series: Standards on Conduct of Audit Assignments

(iv) 500 Series: Standards on Specialized Areas

(v) 600 Series: Standards on Quality Control

(vi) 700 Series: Other/Miscellaneous Matters

(vii) Standards issued up to July 1, 2013

100 Series: Standards on Key Concepts

SIA 110: Nature of Assurance

SIA 120: Internal Controls

SIA 130: Risk Management

SIA 140: Governance

SIA 150: Compliance with Laws and Regulations

200 Series: Standards on Internal Audit Management

SIA 210: Managing the Internal Audit Function

SIA 220: Conducting Overall Internal Audit Planning

SIA 230: Objectives of Internal Audit

SIA 240: Using the Work of an Expert

SIA 250: Communication with Those Charged with Governance

300–400: Series: Standards on the Conduct of Audit Assignments

SIA 310: Planning the Internal Audit Assignment

SIA 320: Internal Audit Evidence

SIA 330: Internal Audit Documentation

SIA 350: Review and Supervision of Audit Assignments

SIA 360: Communication with Management

SIA 370: Reporting Results

SIA 390: Monitoring and Reporting of Prior Audit Issues

500 Series: Standards on Specialised Areas

SIA 520: Internal Auditing in an Information Technology Environment

SIA 530: Third Party Service Provider

The Standards issued up to July 1, 2013

SIA 5: Sampling

SIA 6: Analytical Procedures

SIA 7: Quality Assurance in Internal Audit

SIA 11: Consideration of Fraud in an Internal Audit

SIA 18: Related Parties

Objectives of Internal Audit

6.5 The purpose of defining objectives of Internal Audit as mentioned in SIA 230, Objective of Internal Audit, issued by ICAI are to:

(a) Document the formation and functioning of the Internal Audit activity and the terms of the out-sourced internal audit arrangement;

(b) Provide clarity to the Internal Auditor and its stakeholders regarding the nature of the internal audit set-up and its working;

(c) Ensure linkage between what is expected of the Internal Auditor and how those expectation can be met within the Framework governing Internal Audits; and

(d) Promote better understanding on key operational areas, such as, accountability and authority, roles and responsibility, and such other functional matters.

Once the objectives of internal audit are defined, they help to establish the operating parameters within the overall internal audit agenda. These objectives and operating parameters are formally recorded in one of these two documents:

(a) An Internal Audit Charter, primarily designed for the in-house team of internal auditors and its stakeholders; and

(b) An Engagement Letter is a formal agreement signed with the out-sourced internal audit service provider.

Internal Audit Planning

6.6 As per SIA 220, Conducting Overall Internal Audit Planning as issued by ICAI:

"Knowledge of the entity, its business and operating environment shall be undertaken to determine the types of audit assignment which could be conducted. As part of the planning process, a discussion with management and other stakeholders shall be undertaken to understand the intricacies of each auditable unit subject to audit.

The Internal Auditor shall gather all the information required to fully understand the entity's business environment, the risks it faces and its operational challenges.

The extent of information required shall be sufficient to enable the Internal Auditor to identify matters which have a significant effect on the

organisation's financials. Hence, there is a need to connect the financial aspects of the business with other business elements, such as industry dynamics, company's business model, operational intricacies, legal and regulatory environment, and the system and processes in place to run its operations.

Audit Planning, Materiality and Sampling

6.7 SIA 220, Conducting Overall Internal Audit Planning, as issued by the ICAI involves the following key elements:

(a) It is undertaken prior to the beginning of the plan period (generally, the financial year).

(b) It is comprehensive in nature covering the entire entity.

(c) It is directional in nature and considers all the Auditable Units (i.e., locations, functions, business units and legal entities including third parties, where relevant), along with the periodicity of the assignments to be undertaken during the plan period.

(d) It is normally prepared by the Chief Internal Auditor (or the Engagement Partner, where an external service provider is appointed to conduct internal audits).

(e) The outcome of this exercise is an "Overall Internal Audit Plan" (or the "Audit Engagement Plan," if outsourced).

6.8 SIA 220 "Conducting Overall Internal Audit Planning" and SIA 310 "Planning the Internal Audit Assignment" as issued by ICAI provides guidance in respect of planning an internal audit for the whole entity and particular part of entity respectively. The Internal Auditor may consider referring these standards before commencement of the Internal Audit

6.9 While designing an audit sample, the internal auditor may consider the specific audit objectives, materiality, population from which the internal auditor wishes to select the sample, area of audit significance and the sample size. Standard on Internal Audit (SIA) 5, "Sampling" provides that when using either statistical or non-statistical sampling methods, the internal auditor may consider designing and select an audit sample, perform audit procedures thereon, and evaluate sample results so as to provide sufficient and appropriate audit evidence to meet the objective of internal audit engagement unless otherwise specified by the client.

Overview of Compliance

6.10 Compliance means ensuring conformity and adherence to Acts, Rules, Regulations, Directives and Circulars.

6.11 Standard on Internal Audit (SIA) 150 "Compliance with Laws and Regulations" issued by Institute of Chartered Accounts of India requires that internal auditor to provide independent assurance to management and to those charged with governance on the compliance framework. The nature and extent of internal audit procedures to be applied is dependent on the framework in place and maturity of the processes.

6.12 In case the management has implemented the formal compliance framework, the internal auditor shall plan and perform internal audit procedures to evaluate the design, implementation and operating effectiveness of such framework.

6.13 In case there is no formal compliance framework, the internal auditor shall design and conduct the audit procedures with a view to highlight any exposures arising from weak or absent compliance activities and processes, internal auditor shall make recommendations to implement and strengthen those processes and thereby, improve compliance.

6.14 Where the independent assurance requires the issuance of an audit opinion over the design, implementation and operating effectiveness over compliance, this shall be undertaken in line with the requirements of SIA 110, Nature of Assurance.

Overview of Governance

6.15 Governance is an important aspect of internal audit. The definition of Internal audit elaborates on the term Governance by clarifying how this is a critical operation. Governance is a key concept and integral part of internal audit. The definition of 'Internal audit' elaborates on the term Governance by clarifying how this is a critical operation of the company and fulfilling expectations of its various stakeholders.

6.16 Standard on Internal Audit (SIA) 140, Governance as issued by Institute of Chartered Accountants of India with the objective to:

(a) Provide a common terminology on governance to prevent ambiguity or confusion on the subject matter.

(b) Explain the responsibilities of the Board of Directors and Management, Audit Committee with regard to governance, as mandated by law and regulations; and

(c) Specify responsibilities of the Internal Auditor, especially, when providing independent assurance on the governance framework.

6.17 SIA 140 defines Governance as a set of relationships between the company and its various stakeholders (both internal and external) and provides the structure through which the company's objectives are achieved. The relationship and structure help to guide the behaviour of individuals and groups in the right direction. The following are well accepted underpinnings of good governance:

(a) Integrity and Accountability

(b) Trust and Equity

(c) Transparency and Justice

Third Party Service Providers

6.18 Some of the crucial business operations, processes and information of a retail entity could be outsourced to Third Party Service Providers (TPSP) such as supply chain management, delivery operations, getting sales order through web aggregator and etc. Many more operations or processes of the retail entity can be outsourced to TPSP. The TPSP who is doing such operations would collect store and process, transmit, maintain and dispose information concerning the retail entity, it presents unique challenges of risk management.

6.19 ICAI has issued a Standard on Internal Audit (SIA) 530, Third Party Service Providers with primary objective of prescribing the key requirements for providing an independent assurance over business operations at TPSP. The key requirements are in the nature of:

(a) Assessment of risks associated with outsourcing, especially, in securing and protecting its information;

(b) Evaluation of adequacy of controls to address risks of errors and irregularities with respect to financial, operational processing and reporting;

(c) Cost and operational efficiencies in the collection, storage, processing and continuous availability of User Entities' information; and

(d) Ensuring compliance with IT policies and standards, as well as contractual, statutory and regulatory requirements.

6.20 The requirement of Internal Auditor is to study and evaluate the scope of TPSP's services, governance and oversight process in place to outsource and manage risks of deploying TPSPs, especially, risks arising from direct access and control over critical information of the Retail Entity.

6.21 The Internal Auditor shall review both, the Pre-engagement and Post engagement due diligence undertaken by the Retail Entity, including an assessment of the control environment at the TPSP. This review shall include a control assessment (especially an evaluation of controls retained, in-house and outsourced), so that a scope and audit plan can be defined to conduct a comprehensive audit procedure necessary at both, the User Entity and the TPSP.

6.22 The Internal Auditor who is evaluating the retail entity with such TPSP may refer the SIA 530, Third Party Service Provider to complete the other audit procedures as specified in the SIA.

Internal Auditing in an Information Technology Environment

6.23 Most of the retail entities operate in Information Technology Environment (ITE) where information is captured, stored and processed through automated means and is managed through various policies and procedures to support business operations and objectives. The two main components of ITE include:

(a) IT infrastructure (including, but not limited to, hardware, IT architecture, operating systems, communication network storage systems); and

(b) Application software and data (including, but not limited to, Interface, Enterprise Resource Planning, Customer Relationship Management, Dealer and Channel Management System, E-commerce applications, Robotic Process Automation).

6.24 For example, a retail pharmacy store will maintain its inventory in the computer which will have an operating system. Further for billing, the pharmacy will use an accounting software. In this case, the pharmacy is using both the components as specified above. Similarly, most of the retail entities will operate in the ITE. When the entity is operating in an ITE, it will have a new set of risks and issues.

6.25 The ICAI has issues Standard on Internal Audit (SIA) 520, Internal Auditing in an Information Technology Environment with the objective of dealing the risk by defining the essential requirements for auditing in an IT environment so that:

(a) Audits are undertaken after due study and understanding of the Organisation's ITE, which covers the IT strategy, policies, operating procedures, the risks and governance mechanism in place to manage the ITE.

(b) An independent risk assessment, along with an evaluation of the controls required to mitigate those risks, forms the basis of the audit procedures; and

(c) The audit procedures, as designed and executed, are sufficient to allow an independent assurance, especially in the areas of (indicative list):

    (i) Security and reliability of information.

    (ii) Efficiency and effectiveness of information processing.

    (iii) Analysis and reporting of the information.

    (iv) Continuous access and availability of the information.

    (v) Compliance of the IT related laws and regulations.

6.26 This Standard sets out requirements of internal auditor to gain an understanding of the business operations and the corresponding IT Environment. This information shall assist the auditor to perform an independent IT risk assessment and identify the nature of controls required to mitigate those risks, before commencing any IT audit activities.

6.27 Also, the SIA requires the Internal auditor to have or acquire the requisite qualifications, skill sets and experience to perform IT audits. Specialized skills in the areas of IT governance, Application Controls, Infrastructure reviews, IT Cyber Security and Data Privacy regulation are essential to perform audit.

6.28 SIA 520 sets the illustrative audit areas to be considered as part of the internal audit scope while conducting an internal audit in an IT environment. Also the SIA sets the illustrative IT controls to be reviewed during an internal audit in an IT environment.

6.29 The Internal auditor doing the audit of retail entity operating in the ITE environment shall study SIA 520, Internal Auditing in an Information Technology Environment in detail and perform other audit procedures and mitigate the risks involved.

Chapter 7
Major Areas of Internal Audit Significance

Business Areas

Business Vision and Strategy

7.1 Most of the IT companies will have a vision and a strategy for their business. A description of what an organization would like to achieve or accomplish in the mid-term or long-term future is known as a vision statement of a company. It is intended to serve as a clear guide for choosing current and future courses of action.

Strategy can be defined as a combination of the ends (goals) for which the company is striving and the means by which it is seeking to get there. The most important part of implementing the strategy is ensuring the company is going in the right direction which is towards its vision.

A written declaration of an organization's core purpose and focus that normally remains unchanged over time is called as a mission statement. It serves as filters to separate what is important from what is not and clearly state which markets will be served and how, and communicate a sense of intended direction to the entire organization.

Mission Defines what they have to do, Vision defines what they want to do. The Internal auditor has to first read the vision and mission statement and strategy drafted to achieve the same, in order to get a fair idea of the business of the company.

Market Differentiators of the Company

7.2 Market differentiators or differentiation is the process of distinguishing a product or service from others, to make it more attractive to a particular target market. This involves differentiating it from competitors' products as well as a firm's own products. This is done in order to demonstrate the unique aspects of a firm's product and create a sense of value. The objective

of differentiation is to develop a position that potential customers see as unique.

Market capitalization

7.3 Market capitalization (Market Cap) represents the aggregate value of a company or stock. Market capitalization is calculated by multiplying a company's shares outstanding by the current market price of one share. The investment community uses this figure to determine, a company's size, as opposed to sales or total asset figures. For example if a company has 10 Lakh shares outstanding, each with a market value of Rs.100, the company's market capitalization is Rs. 1000 Lakhs (10,00,000 x Rs.100 per share). This can be done in case of listed companies. Observing trends of Market Cap helps to understand the perceived value of the company both in terms of financial as well business fundamentals.

Industry *Vs*. Company growth

7.4 The growth of a company means the rate at which the company is growing. Industry growth rate means the rate at which the industry as a whole is growing. The growth rate of both the company and the industry need not be the same. If the industry growth rate is abnormally higher than that of the company growth rate, the auditor has to ascertain as to why the growth rate of the company is low in spite of having a high industry growth rate.

Financial Planning, Budgeting and Forecasting Robustness

7.5 A financial plan is an estimate of the total capital requirements of the company. It selects the most economical sources of finance. It also tells us how to use this finance profitably. Financial plan gives a total picture of the future financial activities of the company.

Financial budgeting is used to project future income and expenses. It is done to estimate whether the person/ company can continue to operate with its projected income and expenses.

Financial forecast is a prediction concerning future business conditions that are likely to affect a company. It is important to understand the rigor of financial planning, budgeting and forecasting practices of the company. This demonstrates the organization’s ability to predict and influence their business levers to achieve the desired results.

Contracts

7.8 Contracts play a vital role in the IT industry. The Revenue model shall be based on the Contracts entered into and the adherence to the contract is the basic requirement of the business. Written contracts provide businesses with a legal document stating the expectations of both parties and how negative situations will be resolved. Contracts also are legally enforceable in a court of law. Contracts often represent a tool that companies use to safeguard their resources. The model checklist is as follows:

Sl.No	Particulars	Remarks
(i)	Review terms and conditions of contract	
(ii)	Income Recognition and the Compensation Clause needs to be clearly examined	
(iii)	Analyse the impact on the entity on non-compliance of terms mentioned there in	
(iv)	Verify non competence agreement, if any in favour/against the company and its compliance.	
(v)	Verify the termination clause, warranties or representations due on company and dispute resolution terms involved.	
(vi)	Verify how contract compliance is monitored and reviewed periodically.	
(vii)	Verify the terms of the contract are prejudicial to the interests of the company.	
(viii)	Verify the company has accepted any contracts the business objectives of which are not in the MOA & AOA of the company.	
(ix)	Verify the contract is the governing document or at times the terms of the SOW could override the contract.	
Statement of Work (SOW)		
(i)	Verify that the SOW has defined the scope of work and the deliverables.	
(ii)	Verifythe SOW (for other than Time & Material projects) mention the scope and deliverables in detail to avoid acceptance of work at later stages.	

(iii)	Verify the SOW has defined the place where the service has to be provided.	
(iv)	Verify the payments to be received are up front or phased.	
(v)	Verify the deliverables schedule and payment schedule are primarily in sync or not, for validating the revenue recognition method.	
(vi)	If the project requires any special hardware or software or specialized workforce requirements, verify as to who will provide the same i.e. the company or the client.	
(vii)	Verify there are any limitations on the number of hours that can be billed per week or month. This at times could also determine the revenue recognition method.	
(viii)	Verify there are any criteria for the buyer or receiver of goods to determine if the product or service is acceptable.	

Fixed Assets

7.9 The entity requires having sufficient control in such cases to ensure that the assets put into proper usage and periodic physical verification might be of paramount importance. There could be instances wherein the entity might lease. The internal auditor might be required to verify whether there is proper control over such leased assets.

If the internal auditor is required to perform fixed asset verification procedures too as part of the scope of his work, the auditor can refer to 'Guidance Note on Audit of Fixed Assets' issued by the ICAI.

The model checklist for verification of fixed assets is as follows:

Sl.No	Particulars	Remarks
(i)	Proper authorisation for acquisition/ disposal/ restoration of Fixed Assets.	
(ii)	Physical verification of assets/ update of fixed assets registers at regular intervals.	
(iii)	Compliance with Accounting Standard 10"	

	Accounting for Fixed Assets" and Compliance with Accounting Standard 19 " Leases" in relation to leased assets, issued by the ICAI.	
(iv)	Revaluation of assets value and useful life at regular intervals by independent professional valuers. Especially assets procured for specific one time projects and cannot be reused.	
(v)	Insurance coverage for assets of the entity.	
(vi)	Proper recording/ authorisation for inter/ intra entity transfer of fixed assets.	
(vii)	Segregation of responsibilities among employees handling custodian and verification activities.	
(viii)	Verify calculation of depreciation, amortisation, and capitalisation of expenditure incurred.	
Ix	Verify If cost of asset is reimbursed by the customer, then the asset value is recorded in the books at Zero value for purposes of monitoring.	

Government Grants

7.10 Government grants are assistance given by government in cash or kind to an enterprise for past or future compliance with certain conditions. They may be either accounted under the 'capital approach', under which a grant is treated as part of shareholders' funds, or the 'income approach', under which a grant is taken as income over one or more periods. The treatment depends upon the type and reason for the grant.

The model checklist for verification of government grants is as follows:

Sl no	Particulars	Remarks
(i)	Verify the grant letter issued by the government and study the conditions specified therein.	
(ii)	Verify whether the grant is in monetary or non-monetary.	
(iii)	If the grant is monetary verify the accounting method followed to record the grant.	
(iv)	Verify the entity utilising the monetary grant for the purpose stated is by the government.	

(v)	If non-monetary assets are granted verify it is recorded at acquisition cost or nominal cost.	
(vi)	If the grant is relating to a specific asset, verify the grant has been deducted from the gross value of the asset.	
(vii)	In case, the grant is refundable, then verify it is accounted as an extraordinary item	
(viii)	If grants are received as compensation for expenses or losses incurred in a previous accounting period, verify it has been accounted as per AS 5.	

Loans and Borrowings

7.11 In an industry such as, the IT industry there tends to be borrowing of some sort. It may be short term or long term; it may be taken from banks or financial institutions, from members or directors, etc.

An important feature of such liabilities which has a significant effect on the related audit procedures is that these are represented only by documentary evidence which originates mostly from third parties in their dealings with the entity.

An illustrative list of procedures that an internal auditor might perform would include:

Sl no	Particulars	Remarks
(i)	Verify the credit/ borrowing limits of the board of directors.	
(ii)	Verify the terms of the borrowing is prejudiced against the interest of the entity.	
(iii)	Verify whether the long term loans are being applied for long term purposes and not for working capital purposes.	
(iv)	Verify all the statutory compliances have been met by the entity w.r.t borrowings.	
(v)	Verify interest is paid regularly or a provision for the same has been created.	

(vi)	Verify the repayment is as per the repayment schedule or is there any variations.	
(vii)	Verify the closing balance with the confirmation letter given by the entity who has provided the loan.	

Foreign Currency Transactions

7.12 The IT Industry has gone beyond the geographical boundaries. As a result of globalisation, a lot of foreign companies have set up their branches all over India. Hence, there will be inflow of foreign currency by way of capital, repatriation, export receivables, etc. The model checklist on foreign currency transactions is as follows:

Sl no	Particulars	Remarks
(i)	Check FCNR and other non-resident accounts	
(ii)	Check whether the inward/ outward remittances have been duly accounted	
(iii)	Ensure compliance with RBI/ FEMA compliance in relation to cross border transactions	
(iv)	Review minutes of board meetings pertaining to foreign investments, if any	
(v)	Compliance with Accounting Standard 11 "Effects of Changes in Foreign Exchange Rates".	
(vi)	Compliance with Income tax/ Service tax regulations on payments made to non-residents	
(vii)	Compliance with DTAA/ foreign tax reliefs on taxation of foreign income earned by resident production houses.	
(viii)	Tax issues on Satellite/ Optic fibre Transmission companies/ Foreign companies.	

Related Party Transactions

7.13 As per Indian Accounting Standard (Ind AS) 24, "*Related Party Disclosures"* issued by the Institute of Chartered Accountants of India, ensures that an entity's financial statements contain the disclosures necessary to draw attention to the possibility that its financial position and profit or loss may have been affected by the existence of related parties and

by transactions and outstanding balances, including commitments, with such parties.

Related party disclosure requirements as laid down in this Standard do not apply in circumstances where providing such disclosures would conflict with the reporting entity's duties of confidentiality as specifically required in terms of a statute or by any regulator or similar competent authority.

In case a statute or a regulator or a similar competent authority governing an entity prohibits the entity to disclose certain information which is required to be disclosed as per this Standard, disclosure of such information is not warranted. For example, banks are obliged by law to maintain confidentiality in respect of their customers' transactions and this Standard would not override the obligation to preserve the confidentiality of customers' dealings.

As per Section 2(77) of Companies Act, 2013 "relative", with reference to any person, means anyone who is related to another, if

(i) they are members of a Hindu Undivided Family;

(ii) they are husband and wife; or

(iii) one person is related to the other in such manner as may be prescribed.

Section 2(41) of Income Tax Act, 1961, lays down that '*Relative'* in relation to an individual, means the husband, wife, brother or sister or any lineal ascendant or descendant of that individual. Further, a person shall be deemed to have a substantial interest in a business or profession if:

(i) In case of company, the person, at any time during the year, carries not less than 20% of the voting power.

(ii) In any other case, the person, at any time during the year, is beneficially entitled to not less than 20% of the profits of such business or profession.

7.14 Given the increased linkages between the Indian companies with their counterparts across the globe (coupled with the impressive growth achieved and targeted for the sector), the transactions between Indian players and their related parties overseas have increased manifold. Such related party transactions come under the purview of Transfer Pricing ('TP') regulations and require the same to be carried out at an arms-length price.

Sl no	Particulars	Remarks
(i)	Obtain sufficient audit evidence on related party transactions.	
(ii)	Review the procedure followed by the entity to identify a related party.	
(iii)	Obtain information on key management personnel and their substantial interest held by them in companies if any.	
(iv)	Understand the pricing norms followed by the company in relation to transactions with related parties.	
(v)	Review the methodology followed by the entity in relation to apportionment of cost between related parties.	
(vi)	Review compliance with Transfer pricing regulations.	
(vii)	Review bank transactions and reconcile receivables/ payables if any from/ to related parties.	
(viii)	Review minutes of board meetings and registers maintained under Companies Act, 2013 to understand the transactions entered by the directors.	
(ix)	Obtain explanation for abnormal transactions, if any, among related parties	

Legal and Statutory Compliance

7.15 The internal auditor shall perform the following audit procedures to help identify instances of non-compliance with other laws and regulations that may have a significant impact on the entity's functioning:

(a) Inquiring of management and, where appropriate, those charged with governance, as to whether the entity is in compliance with such laws and regulations; and

(b) Inspecting correspondence, if any, with the relevant licensing or regulatory authorities.

The internal auditor is not responsible for preventing non-compliance and cannot be expected to detect non-compliance with all laws and regulations in case of inherent limitations in scope of audit, if any.

Sl no	Particulars	Remarks
(i)	Obtain understanding on legal and regulatory framework applicable to the entity.	
(ii)	Verify compliance with the following regulations: • The Companies Act, 2013 • Partnership Act, 1932 / Limited Liability Partnership Act, 2008 • The Income tax Act, 1961 • FEMA regulations • The Indian Contract Act, 1872 • Information Technology Act 2000 • The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 • Compliance with IPR/ copyrights/ patents • STPI • The Reserve Bank of India (RBI) Guidelines for IT Governance and Security • Cyber Security Policy, 2013 • Personal Data Protection Bill, 2019 • Ministry of Electronics and Information Technology (MeitY) .	
(iii)	Obtain sufficient appropriate audit evidence regarding compliance with the provisions of applicable laws and regulations.	
(iv)	Perform specified audit procedures to help identify instances of non-compliance with other laws and regulations.	
(v)	Communication appropriately to non-compliance or suspected non-compliance with laws and regulations identified during the internal audit.	
(vi)	If appropriate obtain written representations from management stating that all known non compliances/ suspected non-compliances have been disclosed to internal auditor.	

Sl no	Particulars	Remarks
(vii)	If the company has a policy of working for 24 hours in shifts, verify all the labour laws have been complied with.	
(viii)	Verify and obtain sufficient audit evidence that the company has registered with all the statutory authorities like, PF, ESI, Service Tax, Sales Tax etc (if applicable).	
(ix)	Verify any notices are issued by any of the department and the company has replied the same else has appointed any professional to do the same.	
(x)	Verify that the company is adhering to all statutory compliances like, deduction and remittance of TDS, filing of monthly/quarterly returns, etc	

Information Security and Privacy of Data

7.16 Data security is an important aspect in the IT industry. Any loss or misuse of data will result in huge loss to the entity. At the same time data security is also a major problem in the industry. The following various types of the ways of threat to data security:

(a) Natural Calamity

Fire, flood, earthquake, etc., can cause damage to hardware including server, computers and other physical storage devices.

(b) Theft of Data

Data theft is a growing problem primarily perpetrated by workers with access to technology such as, desktop computers and hand-held devices capable of storing digital information such as, flash drives, iPods and even digital cameras. Since employees often spend a considerable amount of time developing contacts and confidential and copyrighted information for the company they work for, they often feel they have some right to the information and are inclined to copy and/or delete part of it when they leave the company or misuse it while they are still in employment. A common scenario is where a salesperson makes a copy of the contact database for use in their next job.

(c) Hacking

There are chances that the system might be hacked if the security of the systems is not strong enough. Hackers might gain access the data stored in the entity's systems and publish it online or even sell it to the competitors.

The following is the checklist for data security:

Sl no	Particulars	Remarks
(i)	Is there a sound computer/ laptop usage policy formed by the entity?	
(ii)	Does the usage policy cover all possible areas?	
(iii)	Are there sufficient firewalls installed in the server to ensure proper security and is it frequently updated?	
(iv)	Is there a frequent systems audit done to ensure in time detection of all irregularities?	
(v)	Does the entity take all possible steps to prevent, detect and punish fraud?	
(vi)	Verify the company takes back up of the data regularly and stores them at a secure location.	
(vii)	Verify the record of lapses tracked by the company and the nature of action steps taken to prevent recurrence.	

Books of Accounts

7.17 The internal auditor is required to verify the sufficiency of controls related to maintenance of books of accounts by the entity. The internal auditor is also required to verify the controls for allocation of costs between different departments in every location and whether it is adequate and reliable in the light of overall business operations. Model Checklist is as follows:

Sl no	Particulars	Remarks
(i)	Does the entity have proper accounting system commensurate with the regulatory requirements?	
(ii)	Are the control Systems in place in estimating the revenue generated location-wise sufficient to ensure that proper books are maintained for the location?	

Sl no	Particulars	Remarks
(iii)	Does the entity have location wise employee details to ensure proper allocation of payroll cost to the location?	
(iv)	Check frequency of closing the books of accounts i.e. monthly, quarterly, etc.	
(v)	Are the controls for operating the books proper to ensure that prevention of manipulation?	
(vi)	Are the books maintained in a manner to provide Information to the management for decision making?	

Operating Costs

7.18 These are costs administered by a business on a day-to-day basis. They may be fixed or variable costs. Model checklist for few of the important operating costs is given below:

Sl no	Particulars	Remarks
Travelling Cost		
(i)	Evaluate the overall internal control environment resulting from the current processes.	
(ii)	Obtain a copy of travel policy of the company, if any.	
(iii)	Verify the travel voucher and the supporting documents.	
(iv)	If amounts are paid in advance and the expenses incurred are less than the advance, verify that the balance amount is received back from the employees.	
(v)	Verify there are any limits for incurring such expenses.	
(vi)	Verify that the expenses incurred during the year are for official purpose only.	
(vii)	If there is any personal expenses, verify it is approved by the authorised person.	
(viii)	Recalculate the total reimbursable amount to test accuracy.	

Sl no	Particulars	Remarks
Communication Expenses		
(i)	Verify the company has any contract with any of the telecom service provider.	
(ii)	If there is a contract, verify whether the rates agreed upon is not prejudicial to the interests of the company.	
(iii)	Verify there are necessary steps to prevent misuse of the telephone and internet service.	
(iv)	Verify the password of the internet and wi-fi is confidential.	
(v)	If there are no contract with any telecom provider verify the monthly bills.	
(vi)	Verify there are any huge deviances in the bills.	
(vii)	If there are such deviances verify the management has take steps to investigate the cause for such deviances.	

Software Development Cost and R&D Cost

(i)	Verify that the costs incurred on the development stage is capitalized.	
(ii)	Verify where the employees are not entirely dedicated to the development stage, the costs are appropriately allocated for capitalization.	
(iii)	If there are any interest costs relatable to software development verify it is capitalised as per AS 16.	
(iv)	Verify that cost of upgrades and enhancements are capitalized only if the upgrades or enhancements provide additional functionality.	
(v)	If existing software is retired from use, any unamortized costs of the old software shall be expensed.	
(vi)	Verify that expenditures on research should be recognised as an expense immediately and expenditure under development phase should be recognised as an intangible asset, if the recognition criteria given in AS 26 are satisfied.	

Business Continuity Plans

7.19 Business continuity plans are processes that help organizations prepare for disruptive events, the event might be a fire, storm or simply a power outage caused by short circuit. Management's involvement in this process can range from overseeing the plan, to providing input and support, to putting the plan into action during an emergency.

Disasters can be classified in two broad categories. The first is natural disasters such as, floods, storm or earthquakes. While preventing a natural disaster is very difficult, measures such as, good planning which includes mitigation measures can help reduce or avoid losses.

The second category is manmade disasters. These include hazardous material spills, infrastructure failure, or terrorism. In these instances surveillance and mitigation planning are invaluable towards avoiding or lessening losses from these events.

In an industry such as the IT industry where data plays a very crucial part, it has to be safeguarded in the event of any such disasters occurring. Following is a model checklist for preventing and dealing with disasters enabling the entity to continue its business:

Sl no	Particulars	Remarks
(i)	Verify the company has a business continuity plan in place or has outsourced the same to a third party.	
(ii)	If outsourced, verify the backup is taken in disks or stored through cloud storage.	
(iii)	If stored in cloud storage, verify that only authorised persons have access to such data.	
(iv)	Verify regular back up of the data is taken from on-site and automatically copied to off-site disk, or back up made directly to off-site disk	
(v)	Verify that only authorised persons have access to the backup data.	
(vi)	Verify the plan encompasses on how the employees will evacuate and communicate during such events.	
(vii)	Verify sufficient steps are taken to prevent fire in the premises by installing stabilizers and surge protectors.	

Sl no	Particulars	Remarks
(viii)	Verify fire prevention systems such as, alarms and fire extinguishers are existing in the company.	
(ix)	Verify CCTV's are installed to prevent any sort of theft.	
(x)	Verify that anti-virus, firewalls and other security measures are taken to safeguard the data	
(xi)	Verify uninterruptible power supply (UPS) and/ or backup generators are maintained in the company to keep systems going in the event of a power failure.	
(xii)	Verify the steps taken by the company to provide key operations even in case of exigencies.	
(xiii)	Verify the company has identified certain staff to provide services in case of contingencies.	

Analysis, Reporting and Financial Control

7.20 Financial analysis means assessment of the effectiveness with which funds (investment and debt) are employed in a firm and the efficiency and profitability of its operations. Financial control is management control exercised in planning, performance evaluation, and coordination of financial activities aimed at achieving desired return on investment. Financial reporting is consolidating the analysis and to determine the effectiveness of control in the form of a report. Funds management, project accounting, Profitability analysis, Management reporting form part of the analysis and reporting. Following is a model checklist for the same.

Sl no	Particulars	Remarks
Funds Management		
(i)	Verify the funds are applied in the assets as approved by the management.	
(ii)	Verify that the disbursement of large amounts is vested only with the top management.	
Project Accounting		
(i)	Verify that the books are maintained in such a way	

	as to know the financial position of every individual project.	
(ii)	Verify that the common costs are apportioned to every individual project in a proportionate manner.	
Profitability Analysis		
(i)	Verify that if the company is handling multiple projects whether it is maintaining a profitability analysis for each of the projects.	
(ii)	If any of the projects is not profitable, verify the reasons for the same has been disclosed.	
(iii)	If there are continuous losses in any of the projects, verify the steps taken to correct the same.	
(iv)	Verify there are expected future losses on, other than Time & Material projects, then a provision for such anticipated losses should be provided ; unless justified otherwise.	
Management Reporting		
(i)	Verify the company has a policy of preparing and sending a MIS for the management monthly.	
(ii)	Verify the frequency and accuracy of the MIS.	
(iii)	Verify the management has taken any action based on the MIS reports.	

Patents and Copyright

7.21 Copyright is the right given by law to the creators of literary, dramatic, musical, creation of computer software's and databases and their distribution and a variety of other works of mind. It ordinarily means the creator alone has the right to make copies of his or her works or alternatively, prevents all others from making such copies. The basic idea behind such protection is the premise that innovations require incentives. Copyright recognises this need and gives it a legal sanction. Moreover, commercial exploitation of copyright yields income to the creators and, thus, making pecuniary rewards to individuals' creativity.

A patent can be defined as a grant of exclusive rights to an inventor over his invention for a limited period of time. The exclusive rights conferred include the right to make, use, exercise, sell or distribute the invention. Patents are granted only after the satisfaction of certain requirements, which include the patentable subject-matter, utility, novelty, obviousness and specification. A patent can be obtained only if an invention is industrially applicable. An invention is said to be industrially applicable, if it can be made and used in an industry.

Infringement of a patent is the violation of the exclusive rights of the patent holder. If any person exercises the exclusive rights of the patent holder without the patent owner's authorization then that person is liable for patent infringement.

Copyright piracy is a phenomenon prevalent worldwide. Piracy means unauthorised reproduction, importing or distribution either of the whole or of a substantial part of works protected by copyright. The author of a copyrighted work, being the owner, enjoys certain exclusive rights with respect to his or her works. These include right to reproduce, to publish, to adopt, to translate and to perform in public. The owner can also sell, assign, license or bequeath the copyright to another party, if he wishes so. If any person other than the copyright owner or his authorised party undertakes any of the above-mentioned activities with respect to a copyrighted product, it amounts to infringement of the copyright. The model checklist is as follows:

Sl no	Particulars	Remarks
(i)	Verify the registrations under the Copyrights and Patents Act	
(ii)	Obtain documentary evidence on registration/ renewal of copyrights at regular intervals.	
(iii)	Advice the entity on regulatory compliances in case of infringement of copyrights/patents by third party against the company.	
(iv)	Compute contingent liability, if any, on infringement of copyrights of third party by the entity there by to provide realistic picture of financial statements.	
(v)	Advice the company on sharing of copyrights with domestic or foreign residents and legal issues involved.	
(vi)	Verify the company is taking serious legal action against those who have infringed their patents/ copyrights.	

Internal Controls

7.22 As many of the software companies in India are subsidiaries of companies of USA or of any other country, it would need to follow the Sarbanes-Oxley (SOX) Act requirements as per the rules prevailing in its parent company's country. As a best practice, a number of Indian IT companies as well started following SOX requirements. The Act requires all financial reports to include an internal control report. This is designed to show that not only are the company's financial data accurate, but the company has confidence in them because adequate controls are in place to safeguard financial data. Year-end financial reports must contain an assessment of the effectiveness of the internal controls. The issuer's auditing firm is required to attest to that assessment. The auditing firm does this after reviewing controls, policies, and procedures during a Section 404 audit, conducted along with a traditional financial audit. It is designed to review audit requirements to protect investors by improving the accuracy and reliability of corporate disclosures. These standards require management to:

- Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks;
- Understand the flow of transactions, including IT aspects, in sufficient detail to identify points at which a misstatement could arise;
- Evaluate the controls around "Electronic Audit Evidence "-critical documents relied on for accounting (Example :Spreadsheets) to ensure completeness, accuracy and maker checker reviews are demonstrated.
- Evaluate company-level (entity-level) controls, which correspond to the components of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework;
- Perform a fraud risk assessment;
- Evaluate controls designed to prevent or detect fraud, including management override of controls;
- Evaluate controls over the period-end financial reporting process;
- Scale the assessment based on the size and complexity of the company;
- Rely on management's work based on factors such as competency, objectivity, and risk;

- Conclude on the adequacy of internal control over financial reporting.

The model checklist for internal controls is as follows:

Sl no	Particulars	Remarks
(i)	Verify the requirements as per SOX are maintained by the company.	
(ii)	Select a set of controls and test it repeatedly	
(iii)	Verify the company has a sound password policy like instructing the employees not to have usual passwords like their name, date of birth, etc., as passwords.	
(iv)	Verify that the database has a strong authorisation program and does not have any loopholes.	
(v)	Verify the external auditor's report of the previous year and check if any loopholes pointed out by them are complied with by the company.	

Computer Assisted Audit Techniques (CAATs)

7.23 It is the practice of using computers to enhance the effectiveness and efficiency of audit procedures. They are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance, contained in an entity's information systems. The internal auditor should select a suitable CAAT keeping in mind the size and nature of business.

Following are few of the audit tools which the auditor can use in his internal audit.

(i) Microsoft Excel

It is a spreadsheet application used for calculation, graphing tools, pivot tables etc. It allows sectioning of data to view its dependencies on various factors for different perspectives.

(ii) Microsoft Access

It is a database management system with a graphical user interface and software-development tools. It stores data in its own format and can also import or link directly to data stored in other applications and databases.

(iii) ERPs like SAP, etc.

It provides easier global integration and real time information. It reduces the possibility of redundancy errors. It maintains a centralized library of electronic work papers and automates work paper review and approval.

(iv) SaaS

It is a software delivery model in which software and associated data are centrally hosted on the cloud. Access to cloud-based ERP systems allows internal auditors to gather audit information on their own, resulting in less internal time committed to the audit. Audit procedures can be performed throughout the year in real time. One of the major advantages is that all transactions create an 'audit trail' that cannot be manipulated by the company.

(v) Crystal Reports

It is a business intelligence application used to design and generate reports from a wide range of data sources. It allows users to graphically design data connection and report layout.

Business Enabling Functions

7.24 There are various departments which enable a software company business to function smoothly. Few of the important departments are HR, Finance, IT, Facilities, Administration, Quality, Risk management.

The model checklist for the same is as follows.

Sl no	Particulars	Remarks
Human Resources (HR)		
(i)	Verify the recruitments made are according to the talent acquisition policy of the company.	
(ii)	Verify that attendance records are maintained in case of trainings provided for the employees.	
(iii)	Verify non-disclosure agreement has been entered into with the employees.	
(iv)	In case of employee leaving the company verify the company has entered into a Non-Competence Agreement with the employees.	

Sl no	Particulars	Remarks
(v)	Verify the appraisal mechanisms in the company and check if the same has been followed or not.	
(vi)	Verify the attrition rate of the employees.	
(vii)	If the employee turnover is higher than that of the industry obtain the reasons for the same and report the same to the top management.	
(viii)	Verify there are any group or medical insurance policies on the employees taken by the company.	
(ix)	Verify there is any policy of human resource valuation in the company.	
(x)	If it is in existence, verify the method used to value the same and how it is accounted.	
(xi)	Verify the value of human resource has been quantified.	
(xii)	If the value of such an asset is very low, verify the reasons for the same.	
(xiii)	Verify the method selected to value the human resource is appropriate to the company.	
(xiv)	Verify the pay scale of the employees is on par with the industry or there is a very huge deviation.	
(xv)	Verify the entity maintains a checklist of statutory remittances to be made on account of PF, ESI, Labour Welfare Fund.	
(xvi)	Verify there are sufficient records maintained by the entity with regard to their recruitment, offer letter, and all other correspondences with the employee.	
(xvii)	Verify entity maintains separately all complaints and grievances received from the employees.	
(xviii)	Verify In cases of flexible timings and work from home option provided to an employee, has appropriate approval been obtained.	
(xix)	Verify the employee's day wise presence through: attendance to regularisation of attendance to Leave records and finally to timesheets recorded.	

Sl no	Particulars	Remarks
Finance		
(i)	Verify the various sources of finance of the company.	
(ii)	Verify the debt equity ratio of the company to find out the leverage of the company.	
(iii)	If the company has taken a loan, verify that the same is utilised for the specific purpose only.	
(iv)	Verify the collection period of the debtors.	
(v)	Verify the payment period of creditors.	
(vi)	Verify cheques/ bank instructions are prepared and authorised by two different employees.	
(vii)	Verify the operations team is sufficiently supported by the Finance department by providing variety of reports, analysis and insights for appropriate decision making	
(viii)	Verify cheques prepared and signed by two different employees.	
(ix)	If the entity opts for bank transfer, then is there sufficient level of authority to issue bank transfer instruction to the bank.	
Information Technology		
(i)	Verify the usage of IT policy of the company and whether the employees adhere to it.	
(ii)	Verify the company is utilising the software it develops for its internal purpose.	
(iii)	Verify the IT department circulates the relevant hardware and software usage policy to the employees.	
(iv)	Verify there is a rigorous IT helpdesk in place to ensure the IT requirements of the business are addressed on a timely basis.	

Sl no	Particulars	Remarks
Administration		
(i)	Verify the company has a separate administration department to adhere to the needs of the company.	
(ii)	Verify that the accounts department and administration department are not related.	
(iii)	Verify the requests received by the administration department and the action taken by them to address the issue.	
(iv)	Verify the administration department is in charge of all the statutory registrations of the company.	
Quality		
(i)	Verify the company has a defined set of principles to maintain quality of the products.	
(ii)	Verify there is a quality control team in the company.	
(iii)	Verify that the employees related to production are not related to the quality control team.	
(iv)	Verify the quality control team conducts tests on all the products and services and reports the same to the management.	
(v)	In case the quality requirements are not met with verify the procedure to be followed for further processing.	
(vi)	Verify the company obtains feedback from its customers regarding the products and service of the company.	
(vii)	In case of customer complaints verify their grievances has been addressed to by conducting a Root Cause Analysis and fixing the process gaps if any.	
(viii)	Verify a record of all the complaints and their details are maintained by the company.	
(ix)	In case the product/ service has to be reworked verify the cost is borne by the company or it is recovered from the customer.	

Sl no	Particulars	Remarks
(x)	After addressing the grievances of the customer verify the company has taken the feedback from the customer again.	
(xi)	Verify there are any steps/plans taken to improve the quality.	

Revenue Earned by the Company

7.25 The revenue earned by IT companies would be by sale of products or by providing services. There are various means of revenue which an IT company can earn, and the following is a model checklist for the same.

Sl no	Particulars	Remarks
(i)	Identify if the company in involved only in exports or even in domestic sales.	
(ii)	If it is into exports verify the service is provided by the company on site by deputing its employees abroad or from India.	
(iii)	Identify the billing mechanism for the project commensurate' s with the terms of the Statement of Work (SOW)	
(iv)	Verify proper time sheets are maintained by the company if it follows billing on Time and Material basis.	
(v)	Verify, in case of Fixed Price Deliverable based projects, besides maintaining proper time sheets, the estimated time required for completion (Estimated cost to complete) is also reviewed critically. This is important for Percentage of Completion (POC) based accounting of projects.	
(vi)	Verify the company is billing under the milestone method, time sheet method or cost-plus method.	
(vii)	Verify there is an escalation clause if the billing is done on progressive basis.	
(viii)	Verify the company provides warranty and post warranty services.	

Sl no	Particulars	Remarks
(ix)	Verify the amount charged by the company for post warranty services is different from normal charges.	
(x)	Verify the company has entered into an Annual Maintenance Contract (AMC) with its customers	
(xi)	Verify the number of services provide under AMC and the prices charged to them.	
(xii)	Verify there is any price difference in the service provided under AMC and as a standalone basis.	
(xiii)	Verify the company charges for any services not covered under the AMC.	
(xiv)	Verify the company also provides on demand services to its customers apart from post warranty services and is there any price difference for the same.	
(xv)	Verify that the company has a method to monitor revenue leakage or provide revenue assurance. .	
(xvi)	Verify for Time & Material Projects (T&M) that for all Billable resources deployed Timesheets hours is equal to Billable hours; unless justified with reasons.	
(xvii)	Verify for other than Time & Material Projects [Fixed Price (FP)or Service Level Agreement (SLA)] that for all Billable resources deployed, man hours or man-days should factor in the revenues of the project. If not, then the same should be justified with reasons.	
(xviii)	If there are any such revenue leakages what the steps are taken by the company to overcome it.	
(xix)	Verify the revenue recognition adopted by the company is as per AS 9.	

Value of Brand

7.26 Strong brands are necessary in IT industry because technology has increased the number of content providers and made it possible for many more competitors to seek the attention and loyalty of audiences and advertisers. Brands are crucial in separating IT companies and their products

from those of competitors, in creating continuity of quality and service across extended product lines, and in helping develop strong bonds with consumers.

The Model checklist is as follows:

Sl no	Particulars	Remarks
(i)	Understand the valuation methodology followed and verify the method selected is appropriated.	
(ii)	Verify the factors considered in valuing the brand like, growth rate, expected life, weights assigned to various factors, competition, and discount rate adopted.	
(iii)	Obtain brand valuation documents from independent valuers, if any,	
(iv)	Reconcile the value of brand with financial statements.	
(v)	Verify amortization/ impairment provided every year.	
(vi)	Advice the client on importance of brand value and the need to get them registered if they are not registered.	

Accounting for Recharges to the Clients

7.27 Accounting for recharges refers to reimbursement of expenses by the client to the company. Model checklist is as follows:

Sl no	Particulars	Remarks
(i)	Verify the SOW entered into by the company and the client and determine if there is a clause for reimbursement of expenses.	
(ii)	If there is reimbursement clause, verify there are any limits specified for the same.	
(iii)	Check that such a reimbursement is recorded as per appropriate classification required as per the respective accounting requirement income in the books of the company.	
(iv)	Verify that If cost of asset is reimbursed by the customer, then the asset value is recorded in the books at Zero value for purposes of monitoring.	

Sl no	Particulars	Remarks
(v)	Verify that such reimbursements are received basis billing done to the clients, separately for such specific line items.	
(vi)	Verify that there is adequate supporting documents are maintained for such reimbursement claims.	

Hedging

7.28 Hedging means reducing or controlling risk. This is done by taking a position in the futures market that is opposite to the one in the physical market with the objective of reducing or limiting risks associated with currency price changes. As majority of the income derived by software companies are by way of foreign exchange, they have to hedge in order to safeguard themselves against the fluctuating foreign exchange.

Alternatively, the entity can also maintain an Exchange Earner's Foreign Currency (EEFC) account with any of the authorised Dealers. It is a facility provided to the foreign exchange earners, including exporters, to credit 100 per cent of their foreign exchange earnings to the account, so that the account holders do not have to convert foreign exchange into Rupees and vice versa, thereby minimizing the transaction costs. Such accounts are offered without any minimum balance requirements. The EEFC account balances can be hedged. A unit located in a Special Economic Zone can open a Foreign Currency Account with an authorised dealer in India subject to certain conditions as prescribed by the RBI.

The Model checklist is as follows:

Sl no	Particulars	Remarks
(i)	Verify the company has safeguarded itself against foreign exchange fluctuations by entering into forward contracts, options etc.	
(ii)	Verify that such hedging is duly authorised by the Board of Directors.	
(iii)	Verify the profits or losses from such forward contracts or options as recognised as per the AS 11.	
(iv)	If necessary, advice the management of the company on the disclosure requirements as per AS 32.	

(v)	Verify that only the authorised persons are operating the EEFC account.	
(vi)	If the company is located in SEZ, verify the conditions mentioned by the RBI are followed to open the account.	

Annexure I
Checklist for Compliances

Sl No	Applicable Statute/Governing body	Requirement	Remarks
1	STPI	Registration aspects	A Company which is into Software development, IT/ITES, Electronic Hardware manufacturing can register under STPI for availing benefits of STP / EHTP schemes. Such company willing to register under STP / EHTP scheme must apply online through the portal https://stpionline.stpi.in Upon Successful registration, Letter of permission is issued. STP / EHTP units may renew their Letter of Permission after five years of operation. The unit has to file the online application for Renewal of License at least two months before the date of expiry of license. The units are required to obtain Green Card post STP /EHTP registration after accepting the terms and Conditions laid down in the LoP. Application for Green Card to be made as per prescribed annexure.

Sl No	Applicable Statute/Governing body	Requirement	Remarks
2	STPI	Bonding & Debonding	Bonding is done through a prescribed document which is an agreement of the STPI unit with the Development Commissioner of the STPI. This document binds the unit for importing duty free procurement against export. After the capital good reaches location of unit, details to be entered in bond registered duly maintained separately for each locations. In case of Re-warehousing, unit shall get the bond register endorsed by the bonding officer. Debonding of a unit is to relieve itself from this liability and pay applicable duty and GST (if applicable).
3	STPI	STP Scheme benefits	The scheme integrates the government concept of 100% Export Oriented Units (EOU) and Export Processing Zones (EPZ) and the concept of Science Parks/Technology Parks. Some of the benefits are: 1. All the imports of Hardware & Software in the STP units are completely duty free, import of second-hand capital goods are also

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			permitted. 2. Re-export of capital goods is also permitted. 3. Sales in the Domestic Tariff Area (DTA) are permissible. 4. The capital goods purchased from the DTA are entitled for refund of GST. 5. The items like computers and computers peripherals can be donated to recognized non-commercial educational institutions, registered charitable hospitals, public libraries, public funded research and development establishments, organizations of Govt. of India, or Govt of a State or Union Territory without payment of any duties after two years of their import.
4	STPI	Periodic Statutory Reports	*Monthly Progress Reports (MPR) & Quarterly Progress Reports (QPR):* All STP units are required to submit Monthly Progress Reports by 10th of a month on completion of previous month and Quarterly Progress

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			Reports by 30th of a month on completion of previous quarter respectively in the prescribed format. It is a mandatory requirement and units which are irregular in submitting MPRs & QPRs can be denied services of STPI. *Annual Performance Reports (APR):* Yearly performance report should be submitted as per the prescribed format with a signature of Chartered Accountant
5	STPI	Books of Accounts	Distinct Identity: If an industrial enterprise is operating both as a domestic unit as well as an EHTP/STP unit, it shall have two distinct identities with separate accounts, including separate bank accounts. It is, however, not necessary for it to be a separate legal entity, but it should be possible to distinguish the imports and exports or supplies affected by the EHTP/STP units from those made by the other units of the enterprise. Maintain the accounts as under: Maintenance of Sales

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			Invoices. Maintenances of Fixed Asset Registers. Maintenance of Foreign Inward Remittance Certificate file (FIRC) & Bank Realization Certificate (BRC) file where the original of the FIRCs and BRCs are kept. Maintenance of contract file, where copies of contracts received from buyers are maintained.
6	STPI	Export reporting Obligation	After completion of the project, the STP units will get the exports attested from STPI in prescribed following forms *Reporting Requirement* When export of software is made through data communication, it will be declared on SOFTEX form (which is available for sale to exporters through regional offices of Reserve Bank and STPI centres). The form has to be submitted to the concerned STPI within the stipulated time as per the guidelines of RBI.
7	STPI	Non STP registration	For getting the SOFTEX certification by STPI (which is the Designated Authority), the companies have to become

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			STP members by either registering under STP scheme or as NON-STP unit with STPI. The company registered under STPI as NON-STP unit will be issued a Registration Certificate with a validity of 3 years by the respective jurisdictional STPI Director
8	STPI	Non STP – Renewal	Renewal of registration will have to be applied three months prior to the expiry of the registration. Letter of permission for Non STP registration is issued for the period of 3 years. During the last three months prior to the expiry of LoP, NON STP registered unit should approach Director STPI for renewal of LoP.
9	STPI	Non STP	Reporting requirement: Once registered with STPI, the Non-STP units shall submit quarterly report, annual reports and Tenative Annual Performance report to respective STPI centers as per the prescribed format.
10	STPI	SOFTEX Form filing	As per the prevailing RBI Master Circular No. RBI/2013-14/14 dated 1st July 2013, RBI Circular No.80 dated 15th February 2012, RBI Circular

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			No.43 dated 13th September 2013, "any company who does IT/ITES exports through Data communication links needs to submit the Softex to Designated Authority for certification." A common monthly Softex in the form of Excel summary sheet as prescribed by RBI can be filed for all invoices raised in a month. The Softex is required to be filed within 30 days from the date of last invoice raised in that month.
11	RBI	On receipt of Foreign Investment	Intimation to RBI: Once the fund is received from the foreign entity investor, the Indian entity is required to file an intimation with the RBI (i.e. inform its AD Category 1 Bank) that it has received FDI into its company through bank within 30 days of receiving the funds. While receiving funds ensure the following: (a) Funds must flow only from the investors' bank accounts (b) The purpose of remittance should be stated as "Towards Investment in Share Capital"

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			(c) Know Your Customer information to be transmitted along with remittance.
12	RBI	Issue of Shares	Once this intimation is sent, your next step is to issue the shares to the foreign investor within 180 days of receiving the funds, failing which you are bound by law to transfer the money back to your investor. (However, Rule 2(c) (vii) of the Companies (Acceptance of Deposits) Rules, 2014 requires company to issue securities within 60 days of receipt. And in case refund is not made within 15 days from completion of the above said 60 days, then proceeds from share shall be declared as 'Deposits' as per companies Act) Reporting on Issue of Shares: Form FC-GPR (Within 30 days of issue of shares) Along with: a) FIRC/ Debit Statement and KYC: at the specified attachments b) A Certificate from the Company secretary for all applicable compliances. c) A Certificate from CA/ SEBI registered Merchant

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			Banker indicating the manner of arriving at the price of shares issued to the persons resident outside India. d) A letter stating the reason for delay in submission of FC-GPR (in case of delay) e) Debit authority letter f) Board Resolution or PAS – 3 ROC filing acknowledgment. g) Government approvals, if any. h) For Rights/ Bonus issue: Acknowledgement letter of FC-GPR/FC-TRS, as applicable of the original investment. i) Merger/ Demerger/ Amalgamation: If applicable, relevant extracts to be attached at the specified attachment "relevant approvals from the competent authority". j) Declaration by the authorised representative of the Indian company The Business user (Authorised by Entity) shall get a Business user registration from FIRMS portal of RBI and later file the said FC-GPR Form via Single

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			master form (SMF) in FIRMS Portal of RBI.
13	RBI	Overseas investment and initial reporting	As per Foreign Exchange Management (Overseas Investment) Directions, 2022 (dated August 22, 2022) Issued by RBI: Overseas Direct Investment (ODI) means: (i) acquisition of any unlisted equity capital or subscription as a part of the Memorandum of Association of a foreign entity, or (ii) investment in 10% or more of the paid-up equity capital of a listed foreign entity, or (iii) investment with control where investment is less than 10% of the paid-up equity capital of a listed foreign entity. Overseas Portfolio Investment (OPI) means: Investment, other than ODI, in foreign securities and as provided in above said Direction. A) Initial reporting and permissions: A person resident in India, who has made Overseas Direct Investment (ODI) or is

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			making any financial commitment or undertaking restructuring or undertaking disinvestment in a foreign entity, shall report it in 'Form FC'. A person resident in India other than a resident individual, making any Overseas Portfolio Investment (OPI) or transferring such investment by way of sale, shall report the same in 'Form OPI'. Permission for making overseas investment: a) Prior approval from the Central Government is required or overseas investment/financial commitment in Pakistan/other jurisdiction as may be advised by the Central Government b) Prior approval from the Reserve Bank for Financial commitment by an Indian entity, exceeding USD 1 (one) billion (or its equivalent) in a financial year even when the total FC of the Indian Party is within the eligible limit under the automatic route (i.e., within 400% of the net

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			worth as per the last audited balance sheet). Annual reporting requirement is explained in below topic.
14	RBI	Annual Reporting (FLAIR and APR)	A) Applicability FLAIR (Foreign Liabilities & Assets information return)- Any entity which: (i) has received Foreign Direct Investment. (or) (ii) has invested in any foreign entity (Overseas Direct Investment) Once applicable, Submit Annual Return of Foreign Liabilities & Assets information return (FLAIR), with the Reserve Bank of India through online Business user registration, before 15th July of every year till there is such outstanding foreign assets/ liabilities. Audited Version of Financials can be updated in FLA Return after obtaining prior approval of RBI in this regard. B) Applicability of Annual Performance report (APR): Any person resident in India acquiring equity capital in a foreign entity which is reckoned as ODI, shall submit an APR with respect to each foreign entity every year till

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			the person resident in India is invested in such foreign entity, by December 31st. Non-Applicability of APR Filing: i) holding less than 10 per cent of the equity capital without control in the foreign entity. ii) When the foreign entity is under liquidation iii) In case such foreign investment is divested during the year, then only such transactions before divested to be reported in Form FC.
15	RBI	External Commercial Borrowings	As per RBI master circular-RBI/FED/2018-19/67, (latest update issued till 30.09.2022)- AUTOMATIC ROUTE: All ECB can be raised under the automatic route if they conform to the parameters prescribed under the framework issued. (i) Eligible borrowers: (a) FCY denominated ECB: All those entities which are eligible to receive FDI. Further, the following entities are also eligible to raise ECB: 1. Port Trusts.

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			2. Units in SEZ. 3. SIDBI. 4. EXIM Bank of India. (b) INR denominated ECB: 1. All entities eligible as per FCY denominated ECB criteria mentioned above. 2. Registered entities engaged in micro-finance activities, viz., registered Not for Profit companies, registered societies/trusts/ cooperatives, and Non-Government Organisations. (ii) Recognised lenders: The lender should be resident of FATF or IOSCO compliant country, including on transfer of ECB. Also, a) Multilateral and Regional Financial Institutions where India is a member country will also be considered as recognised lenders. b) Individuals as lenders can only be permitted if they are foreign equity holders or for subscription to bonds/debentures listed abroad; and c) Foreign branches / subsidiaries of Indian

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			banks are permitted as recognised lenders only for FCY ECB (except FCCBs and FCEBs). A "foreign equity holder' means: (a) direct foreign equity holder with minimum 25% direct equity holding in the borrowing entity, (b) indirect equity holder with minimum indirect equity holding of 51%, or (c) group company with common overseas parent. (iii) Borrowing Limit and leverage: All eligible borrowers can raise ECB up to USD 750 million or equivalent* per financial year under the automatic route. Further, in case of FCY denominated ECB raised from direct foreign equity holder, ECB liability-equity ratio for ECB raised under the automatic route cannot exceed 7:1. However, this ratio will not be applicable if the outstanding amount of all ECB, including the proposed one, is up to USD 5 million or its equivalent. (iv) Interest and maturity period:

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			Maturity period of ECBs shall comply with the Minimum Average Maturity Period (MAMP) based on purposes as stated in the circular. Interest and any other costs shall comply with All-in-cost ceiling per annum as stated in the circular. (v) End-uses not permitted: (a) Utilisation of ECB proceeds is not permitted for on-lending or investment in capital market including equity instruments in India, except in permitted cases of conversion into equity (Refer conversion to equity topic) (b) Utilisation of ECB proceeds is not permitted in real estate. (c) Utilisation of ECB proceeds is not permitted for working capital, general corporate purpose and repayment of existing Rupee loans, except permitted Minimum Average Maturity Period (MAMP) as per circular. (d) On-lending to entities for the above activities,

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			except in case of ECB raised by NBFCs as permitted in master circular. Procedures Borrowers may enter into loan agreement complying with ECB guidelines with recognised lender for raising ECB under Automatic Route without prior approval of RBI. However, reporting requirements mentioned in the next checklist item is to be complied. APPROVAL ROUTE: If any borrower does not conform to above mentioned framework, shall approach the RBI with an application in prescribed format (Form ECB) for examination through their AD Category I bank
16	RBI	External Commercial Borrowings-reporting Requirement	(a) With a view to simplify the procedure, submission of copy of loan agreement is dispensed with. (b) For allotment of loan registration number, borrowers are required to submit duly certified Form ECB, which also contains terms and conditions of the ECB,

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			in duplicate to the designated AD Category I. One copy is to be forwarded by the designated AD bank to the Director, RBI, Department of Statistics, and Information Management, External Commercial Borrowings Division, Bandra-Kurla Complex, Mumbai – 400 051 (c) The borrower can draw-down the loan only after obtaining the loan registration number from Reserve Bank of India. (d) Borrowers are required to submit 'ECB-2 Return' certified by the designated AD bank on monthly basis so as to reach DSIM, RBI within seven working days from the close of month to which it relates. (e) Changes in terms and conditions of ECB in consonance with the ECB norms, including reduced repayment by mutual agreement between the lender and

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			borrower, should be reported to the DSIM through revised Form ECB at the earliest, in any case not later than 7 days from the changes effected.
17	RBI	Conversion of ECB	*Conversion of ECB into equity is permitted subject to the following conditions:* (a) The activity of the company is covered under the Automatic Route for Foreign Direct investment or Government approval for foreign equity participation has been obtained by the company, (b) The foreign equity holding after such conversion of debt into equity is within the sectoral cap, if any, (c) Applicable pricing guidelines for shares are complied with. *Conversion of ECB may be reported to the Reserve Bank as follows:* (a) Borrowers are required to report full conversion of outstanding ECB into equity in the form FC-

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			GPR to the concerned Regional Office of the Reserve Bank as well as in form ECB-2 submitted to the DSIM, RBI within seven working days from the close of month to which it relates. The words "ECB wholly converted to equity" should be clearly indicated on top of the ECB-2 form. Once reported, filing of ECB-2 in the subsequent months is not necessary. (b) In case of partial conversion of outstanding ECB into equity, borrowers are required to report the converted portion in form FC-GPR to the concerned Regional Office as well as in form ECB-2 clearly differentiating the converted portion from the unconverted portion. The words "ECB partially converted to equity" should be indicated on top of the ECB-2 form. In subsequent months, the

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			outstanding portion of ECB should be reported in ECB-2 form to DSIM. Additionally, following to be ensured in conversion cases: 1. If the borrower concerned has availed of other credit facilities from the Indian banking system, applicable prudential guidelines of Reserve Bank are to be complied with. 2. Information regarding conversions is exchanged with other lenders of the borrower.
18	Income Tax	Sec 10 B- 100% Export Oriented Unit	Special Incentive has been given to the newly established 100% EOU. Under this section the profits and gains derived from the 100% EOU shall not be included in the total income of the taxpayers. This benefit is available for the income earned during a period of five consecutive assessment years falling within a period of eight years from the commencement of production. This exemption is available to all the taxpayers including the foreign companies and the Non-Resident taxpayers. NO DEDUCTION AFTER the

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			assessment year beginning on the 1st day of April, 2012 and subsequent years: (Refer Sec 10B (1) 3rd Proviso)
19	Income Tax	Reporting in respect of international and specified domestic transaction.	1) If any Indian company has done any international transaction with associated enterprise or specified domestic transaction, then apart from regular provision compliances, such Indian entity is obliged to get the report from a Chartered Accountant in 'Form 3CEB' before 31st Oct of relevant AY. 2) As per rule 10DA of income tax, Master file reporting to be made in 'Form 3CEAA' before 30th Nov of relevant AY: Part A to be filed by every entity that has entered into any international transaction, irrespective of any limits or threshold of the value. Part B Only the following entities who meet the given two conditions shall file this form: i) The consolidated group revenue for the preceding

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			accounting year exceeds Rs.500 crore. ii) The total value of the international transactions conducted has exceeded Rs.50 crore for the present accounting year, or if there have been any international intangible property-related transactions, the value of such transactions exceeds Rs.10 crore. 3) If the turnover of the group of companies exceeds Rs 6400 crore, then COUNTRY-BY-COUNTRY REPORT needs to be furnished in 'Form 3CEAD' by a parent entity or an alternate reporting entity or any other constituent entity, resident in India.
20	Employee's Provident Fund and Miscellaneous Provisions Act, 1952	Reporting Requirements	Preparation of monthly PF remittance ECR statement. Preparation of PF challan in prescribed formats and specified copies as follows: 1. Monthly Regular contribution - Along with ECR. 2. Direct Challan - Generally used when organisation is having Nil Employees (say during liquidation) to file

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			Nil Return 3. 7Q-14B Challan - Generally used for paying any interest or damages due to Arrears/ Delayed payments. Preparation and filing of necessary forms and returns. Obtaining Self-declared Form No.11 from new entrants joined during the month. (Mandatory to keep this with Employer) and Form No. 2 (Nominee Details of Employee on optional basis) Maintenance of a database of all employees giving the details of their names, PF number, Aadhaar, PAN, transfer/ withdrawal, etc., for future reference and also to follow up with RPFC for transfer /withdrawal till process is complete.
21	The Employee's State Insurance Act, 1948	Reporting Requirements	Preparation of monthly ESI remittance statement. (Regular / Nil Returns Mandatory) Preparation of half yearly statement (Form 5) Preparation of ESI challan. Preparation of ESI challan in prescribed formats and specified copies.

Sl No	Applicable Statute/Governing body	Requirement	Remarks
22	Special Economy Zone	Eligibility Criteria	As per Sec 10AA of Income tax Act- It has commenced business (Goods/service) anytime during AY 2006-07 to AY 2020-21 It is not formed by the splitting up, or the reconstruction, of a business already in existence. It is not formed by the transfer to a new business, of machinery or plant or capital goods previously used for any purpose. Other procedural requirements are fulfilled as per provisions and rules made under The SEZ Act 2005.
23	Special Economy Zone	Reporting Requirements	To submit annual performance report duly certified by CA (FORM I as per rule 22 of SEZ Rules) within specified time from the close of Financial Year, to development commissioner. SEZ units are required to maintain a Positive Net Foreign Exchange earning cumulatively for a period of 5 years from the commencement of operation. Reporting to be done in Annual performance report (Annexure B as per Rule 53) For Availing Benefit during

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			final 5 AYs, 'SEZ Re-investment Reserve Account' to be maintained which needs to be certified by CA in Form 56FF to be submitted in this regard as per rule 16DD of the Income tax Rules. The Unit shall execute a Bond-cum-Legal Undertaking in Form H. (Rule 22) As per Instruction 89 (Govt of India – Doc) undertake not to change name, style and location except with approval of development commissioner. To intimate change in Board of directors, etc. Units are required to maintain proper books of accounts financial year wise which include records in respect of import/export/ procurements/inter unit transfer/ DTA sale/sub-contracting/ destruction, etc. (Rule 22) Unit engaged in both trading and manufacturing activities shall maintain separate records for trading and manufacturing activities. (Rule 22) The Developer shall maintain a proper account of the import or procurement, consumption

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			and utilization of goods and submit quarterly and half-yearly returns to the DC (in Form E). The Developer shall submit a half-yearly certificate every financial year regarding utilization of goods from an independent Chartered Engineer to DC and SO and every certificate shall be filed within period specified. (Rule 12) The goods admitted into a Special Economic Zone shall be used by the Unit or the Developer only for carrying out the authorized operations but if the goods admitted are utilized for purposes other than for the authorized operations or if the Unit or Developer fails to account for the goods as provided under these rules, duty shall be chargeable on such goods as if these goods have been cleared for home consumption. (Rule 34)
24	Special Economy Zone	Benefits Available	i) 100% Income Tax exemption on export income for SEZ units under Section 10AA of the Income Tax Act for first 5 years of incorporation, 50% for next 5 years thereafter and 50% of the

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			ploughed back export profit for next 5 years via 'Special Economic Zone Re-investment Reserve Account. ii) Exemption from Central Sales Tax, Service Tax and State sales tax. These are now subsumed into GST and supplies to SEZs are zero rated under IGST Act, 2017. However, All Goods and services supplied by SEZ units to DTA are treated as imports into India and is subject to all procedures and rules applicable in case of normal imports into India (Sec.30 of SEZ Act 2005) iii) SEZs are deemed to be an airport, port, Land Custom Stations, and Inland Container Depot under the Customs Act and a dedicated customs formation is there for ensuring clearance for exports, imports, deemed exports, intra SEZ sales, domestic procurement and domestic sales iv) Exempt from Customs duty if purchased for authorised operations

Sl No	Applicable Statute/Governing body	Requirement	Remarks
			towards development, operation and maintenance of SEZ units after obtaining approval of Development commissioner. v) Single window clearance for Central and State level approvals.
25	Professional Tax	Payment and Returns	In India professional tax is levied by respective state govt. The tax rates are notified in the schedule to Profession tax of respect. In case of a company, it is liable to deduct from employees and deposit such tax to state govt and file monthly return within such time limit as prescribed by respective state govt. Also, annual tax to be deposited by the employer and also annual return to be filed within such time limit as prescribed by respective state govt.

References

http://www.nasscom.in/

http://www.stpi.in/

http://www.sezindia.nic.in/

http://www.rbi.org.in/

http://www.incometaxindia.gov.in/

http://www.esic.nic.in/

http://www.epfindia.gov.in/

http://www.nic.in/

http://www.assocham.org/

https://www.meity.gov.in/

https://stpi.in/

Notes

Notes

ISBN : 978-81-8441-681-7

Price: ₹ 165/-

BIAMA-007-0124

January | 2024 | P3540 (Revised)

www.icai.org