Manual on Information Systems (IS) Audit 2024

A Practitioner's Guide

SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

COMPTROLLER AND AUDITOR GENERAL OF INDIA

Manual on
Information Systems (IS) Audit
2024

A Practitioner's Guide

SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

COMPTROLLER AND AUDITOR GENERAL OF INDIA


act, { useEffect
STransition } from
/index.css";
odal.css";
l = (props) => {
by state
by "esc"
OnEscapeKeyDown = (e) =>
ode || e.keyCode === 27) {
Close();
to detect click "esc"
=> {
body.addEventListener("keydown", closeOnEscapeKeyDown);
tion cleanup() {
body.removeEventListener("keydown", closeOnEscapeKeyDown);

Edit <code>src/App.

<a
className="App-link"
href="https://reactjs.org"
target="_blank"
rel="noopener noreferrer"
>
Learn React

</header>

);
}

Preface

Information systems have always been an important driver for organizations to achieve their objectives. Even before the advent of the digital age, information systems consisting of manually maintained records were crucial for efficient and effective decision making by leaders and managers. The emergence of Information Technology (IT) over the last century has made information systems ubiquitous and has transformed the scale and potential at which they enable organizations to achieve higher performance outcomes. In public sector organizations as well, there has been a significant increase in the volume and variety of internal business processes and external service delivery through IT-enabled information systems.

This digital transformation places a solemn obligation on us, as a Supreme Audit Institution committed to excellence. We not only have to ensure that the investment of public funds into modern information systems has resulted in realization of the intended benefits to the audited entities and the citizens at large, but also that the information systems facilitate compliance with the business rules of the public sector organizations. Building the required capacity to conduct meaningful audit of information systems and exercising due diligence in our examination is an indispensable part of our fiduciary responsibility.

In this context, this updated version of the Information Systems Audit Manual is an attempt to define the broad contours of how we intend to do justice to the role entrusted to us by the Constitution. The Manual has practical guidance and case studies on aspects of information systems that we need to focus on- governance mechanisms, general controls and application controls. It also contains guidance on decision making for design of IS Audits- related to the Scope, Methodology and preparation of Audit Matrices. The Manual is intended to facilitate the adoption of a uniform and consistent approach to planning, execution and reporting of IS Audits across the Department.

I am sure that the Officers and officials of the Department would find this Manual very useful in guiding their decisions and actions towards enhancing the quality of IS Audits.

K Sanjay Murthy
Comptroller and Auditor General of India
December 2024

Foreword

SAI India, in its capacity as the Chair of the INTOSAI Working Group on IT Audit (WGITA), had collaborated with the INTOSAI Development Initiative (IDI) to develop the "Handbook on IT Audit for SAIs 2022 Version". The Handbook is classified as a Global Public Good. In view of the target audience of the world-wide community of SAIs and the varied levels of maturity for conducting IS Audits among them, the Handbook offers guidance at a level of granularity which necessarily requires additional inputs which are relevant to the specific operating context of an individual SAI.

It is in this background that the "IS Audit Manual 2024- A Practitioner's Guide" has been developed. It is intended to provide last-mile connectivity for our audit teams to the values, concepts and principles elucidated in the WGITA-IDI Handbook, and function as a bridge to translate its higher level guidance into practical points of action.

IT-enabled information systems in the public sector should protect the data and assets of the audited entities and support their core business objectives. Equally, they should also support the eternal values of good governance- fairness, transparency, accountability and compliance. Modern information systems carry risks related to data security due to increased connectivity to internal and external networks, and potential lapses on account of genuine errors/ deliberate non-compliance which may be harder to detect.

The Manual focusses on a hands-on approach to emphasize the maintenance of a clear mapping between IS Audit Objectives, the Design Matrix, the Findings Matrices and the IS Audit Report; the factors to be considered and the trade-offs involved in deciding the Audit Scope; the need to standardize the Design Matrix for IS Audits to ensure consistency during Reporting; identification of core business processes and their mapping into information systems in the form of application controls implemented; and a number of succinct case studies.

Given the nature of the subject matter and the rapid pace of emergence of new technologies, it is anticipated that periodic modifications will have to be incorporated into this Manual. I am confident that all Department will rise up to this challenge, and that we will up-skill ourselves to preserve and enhance our reputation for excellence.

S Ramann
Chief Technology Officer,
Office of the CAG of India
December 2024


PLATFORM
Research
FINANCE
COMMUNICATION
DATABASE
NETWORK
WEBSITE
APPLICATION
MONITORING
ABORATION
SEARCH
RUNTIME
OBJECT STORAGE
IDENTITY
CONTENT
BLOG STORAGE
INFRASTRUCTURE

Contents

CHAPTER 1

I. Introduction

The adoption of new technology in the creation, use and maintenance of information systems has consistently changed the way in which organizations function and has impacted their performance. In the public sector, the processes for essential functions such as tax administration, law enforcement, budget and expenditure management, procurement, material management, production planning and generation of accounts have witnessed very significant improvements on the dimensions of efficiency, transparency and real-time supervisory control, due to the transition from manually maintained, book-keeping-based information systems to modern, software technology-based information systems.

Information systems implemented with software applications have matured from being merely data processing systems to the current versions where they now are capable of collection, storage, computation and dissemination of large amounts of data. This data is used for real-time decision making and play a major role in audited entities' core business functions. Systems today communicate with each other and exchange data over networks - both public and private.

This transition has resulted in commensurate changes needed in the process of examination of controls by audit professionals. The objectives of such audit examination remain the same, with tests for completeness, accuracy and supporting documentation. However, these controls are now typically technology-based application controls implemented in the information system, rather than manual and general controls which were required to be exercised by individual users in the maintenance of registers, ledgers and other records.

The adoption of information technology undoubtedly contributes to more robust controls and enables the shifting of the burden of compliance from individual users to the application implemented for information systems. This shift is intended to provide higher levels of assurance that the risks of errors and/ or deliberate actions which result in non-compliance with business rules have been mitigated.

However, the actual level of assurance is dependent on the details of implementation, and the task for auditors in this context is to conduct a thorough test of the functionalities and application controls which have been implemented. Vulnerabilities and risk areas which may arise on account of incomplete/ incorrect mapping of business rules have to be identified, mitigated, and controlled by audited entities; and assessing the adequacy of each control requires appropriate methods of auditing[1]. Even when the audited entities have implemented some risk-mitigation measures, an

independent audit is required to provide assurance that adequate controls (General Computer Controls[2] and/or Application[3] Controls) have been designed and are implemented.

There have been a few major trends during the last 15 years which have contributed to heightened levels of risk for information security in modern information systems. These trends include the integration of erstwhile stand-alone applications for industrial equipment (such as manufacturing and production plants, Supervisory Control and Data Acquisition/ Programmable Logic Controller systems) into broader Information Technology (IT) networks and the Industrial Internet of Things (IIoT); the increased use of mobile and portable devices at workplaces; the increased use of remote work arrangements through Internet/ Virtual Private Network connectivity; and increased risks associated with the human element, due to the lack of proper training of the IT system users and lack of sensitization on Data Governance and Data Security policies of key personnel responsible for the information systems.

The scope and the investment in Information Technology for information systems in the public sector is only expected to increase. The India Digital Enterprise Architecture (InDEA) framework proposed by the Ministry of Electronics and IT, Government of India contemplates that the boundaries between functions, jurisdictions and public-private organizations will get Blurred due to increasing interdependencies and the need for citizen-centric approaches to designing digital services, as opposed to organization-centric approaches. The need to provide end to-end services, adopting the methods of digital transformation, agile development methods, disruptive business models, and the opportunities offered by the emerging technologies like Machine Learning, Internet of Technologies and Distributed Ledger Technology are strong forces pushing the limits towards the evolution of digital ecosystems in India.

It is therefore imperative that auditors re-skill and up-skill themselves continuously, to ensure that relevant and actionable inputs are provided to all the stakeholders on controls related to information security, data privacy, transparency, equality of access to information and maintenance of level playing fields in the public sector. This would result in the discipline of Audit of Information Systems serving public interest, in line with the overall goals of the Indian Audit and Accounts Department.

---

[1] IT Audit Manual, Volume I, Comptroller and Auditor General of India

[2] General IS Controls are not specific to any individual transaction stream or application and are controls over the processes in an IT Implementation which support the development, implementation, and operation of an IT System. They would typically involve IT Governance, Organisation and Structure, Physical and Environmental Controls, IT operation, IS Security, and Business Continuity.

[3] Application Controls are controls specific to an IT System and involve mapping of business rules into the application thus providing For Input, Processing, Output and Master Data controls.

In this overall context, the objective of this Manual is to build on the guidance previously notified by the Department and to supplement the same with constructive and hands-on guidance covering the nuts and bolts of IS Audits, targeted at the members of our audit teams.

1. Relevant Guidelines, Frameworks and Standards

1.1 Compliance Audit Guidelines 2016

Audit of Information Systems (IS Audit) is a Subject Specific Compliance Audit. Hence, this Manual is intended to build on the Compliance Audit Guidelines 2016 issued by the CA G of India. These provisions in these Guidelines related to the processes for risk assessment, the definition of key Audit elements (objectives, scope, sampling, audit design matrix and audit findings matrix), engagement with audited entities, gathering of evidence, reporting of audit observations and the follow up of previous audit efforts shall be applicable to IS Audit assignments undertaken in the Department.

1.2 IDI-WGITA Handbook

This Manual is intended to link organically with the Handbook on IT Audit developed by the INTOSAI Development Initiative (IDI) and the Working Group on IT Audit (WGITA) of the INTOSAI. The guidelines from the Handbook related to identification of domains and the audit methodologies and best practices have been referred to, in this Manual. This ensures that IS Audit processes in the Department are aligned with globally recognized standards, enhancing their credibility and effectiveness.

1.3 Standing Order on auditing in IT environment

The contents of this Manual draw on this Standing Order issued by the CAG of India. This ensures that the Department's IS Audit processes are uniformly aligned, promoting consistency and compliance with audit requirements.

1.4 COBIT 2019

As a central framework, COBIT 2019 principles are integrated into the manual to govern and manage enterprise information technology. The Manual aligns the Department's IS Audit processes with the COBIT framework, ensuring robust governance and adherence to international best practices.

1.5 ISO/ IEC 27001: 2022[4]

The ISO/ IEC 27001 is an international Standard published by the International Organization for Standardization on the subject of Information Security Management Systems, and services as a benchmark for best practices on IT Governance and Security. Reference to this Standards ensures that IS Audit analysis and recommendations are aligned with the globally recognized framework, fostering credibility and trust.

[4] International Organization for Standardization on IT Governance and IT Security

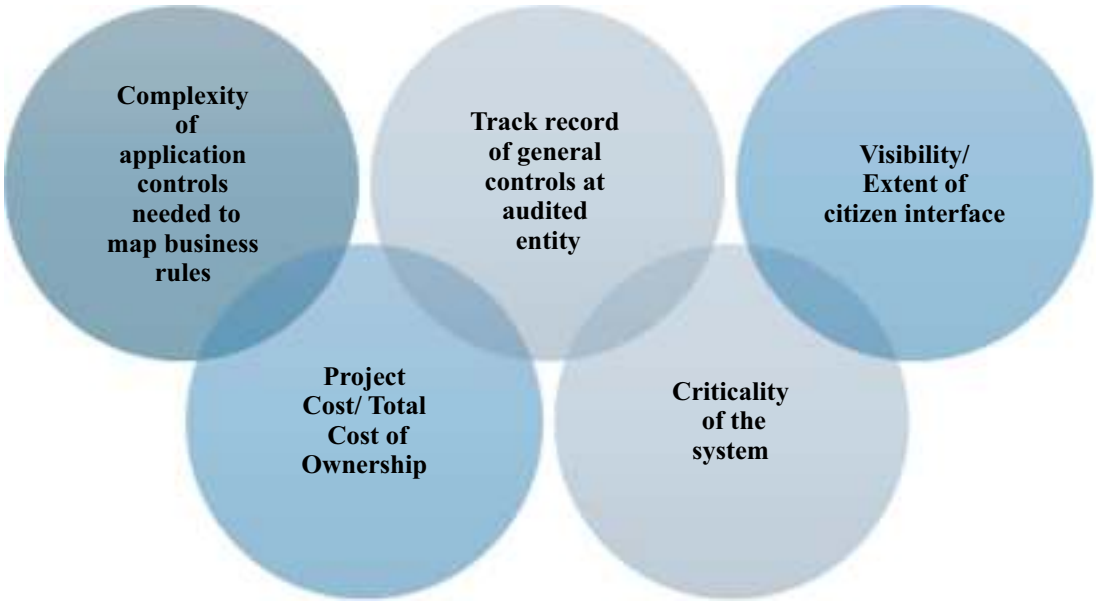
CHAPTER 2

II. IS Audit Planning

1. Strategic Audit Plan

The Department formulates and adopts Strategic Audit Plans at regular intervals. These Plans intend to prepare a list of subject matters which are to be audited over the next 3-5 years, based on rigorous risk assessment. In addition to the preparation of the list, the priority and sequence in which these subject matters are to be audited is also specified, so that the Department continues to fulfill its Constitutional mandate and serves public interest through relevant and meaningful Audit products. The Strategic Audit Plan includes subject matters related to all audit streams- Revenue Audit, Social Welfare Audit, Commercial Audit, Railways Audit, Defense Audit and IS Audit.For the IS Audit section in the Strategic Audit Plan of the Department, a list of information systems (as subject matters) which are intended to be audited during the Plan period is to be prepared. This list may include information systems which have been previously audited, those which have been implemented during the period of the previous Strategic Audit Plan to cover new functions and business processes, as well as those which have been implemented by deploying emerging technologies such as Artificial Intelligence, Internet of Things, Distributed Ledger Technology etc.

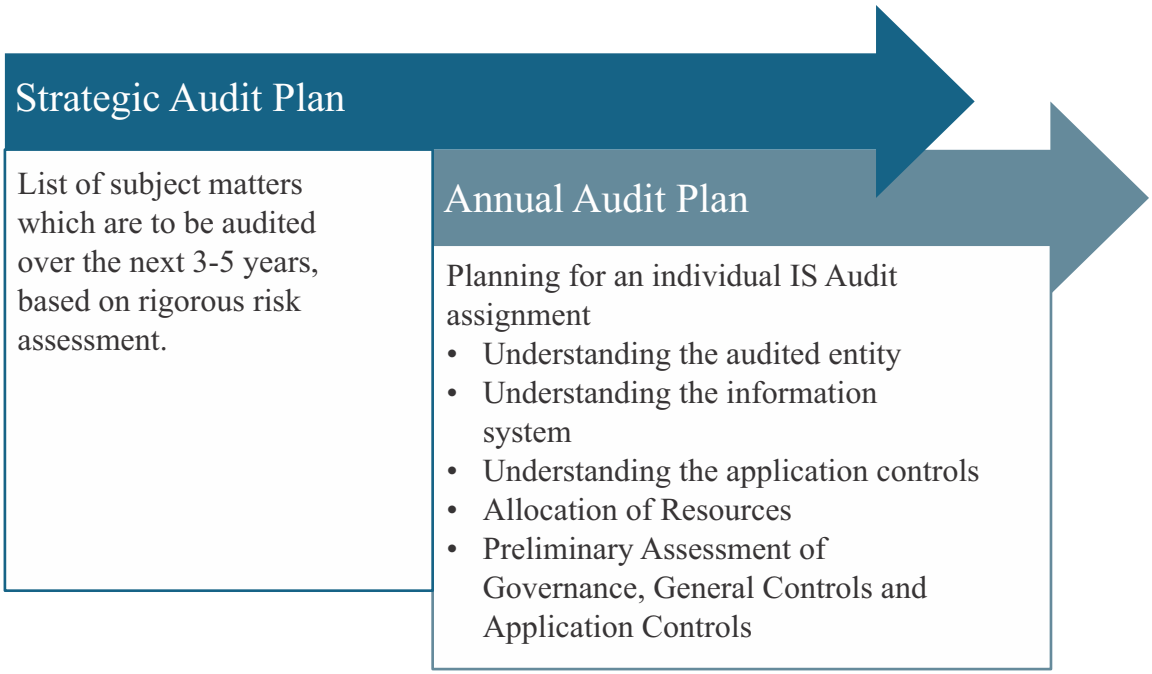
In view of the extent of the vast audit jurisdiction of the Department- which includes the high and increasing number of IT applications for information systems used by the audited entities- it is vital that a data driven, well-reasoned, and adequately documented risk-based approach is followed to prepare the list of information systems to be covered during the Strategic Audit Plan period. The criteria/ parameters which may be considered to evaluate the priority of the overall set of IT applications may include the following:



The provisions in the Compliance Audit Guidelines 2016 which are related to the preparation of the Strategic Audit Plan may be followed by the field audit Offices, for the preparation of a prioritized list of IT applications to be audited, from their overall audit jurisdiction based on the above criteria/ parameters. These lists are then intended to be consolidated at the Department level, to identify commonalities, review the data, reasoning and impact of the criteria used for risk assessment and finalize the overall list of information systems to be audited during the Strategic Audit Plan period.

2. Annual Audit Plan

The Department formulates and adopts Annual Audit Plans. These Plans intend to prepare a list of subject matters which are to be audited during the next financial year, based on rigorous risk assessment. This list of subject matters to be audited during the next financial year is typically drawn from the list of pending subject matters in the Strategic Audit Plan, along with new subject matters that have either emerged as important for coverage over the course of the current financial year or which have been requested to be audited by the audited entities themselves.



The preparation of an Annual Audit Plan by every field audit Office in the Department is a mandatory requirement. The Annual Audit Plan for a field audit Office would include the subject matters related to all the Audit Management Groups of that Office. The list of subject matters may also include

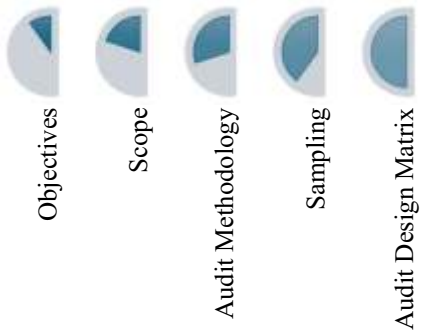
information systems which are planned to be audited during the next financial year. The provisions in the Compliance Audit Guidelines 2016 which are related to the preparation of the Annual Audit Plan may be followed by the field audit Offices, for the preparation of a prioritized list of IT applications to be audited during the next financial year, based on a data-driven, well-reasoned and adequately documented risk-based approach.

Every field audit Office shall make efforts to plan and execute at least one IS Audit as part of every Annual Audit Plan. This is a desirable stipulation and IS Wing, HQ Office shall follow up with the larger field audit Offices for achievement.

Every field audit Office shall plan and execute at least one IS Audit during any three consecutive Annual Audit Plans. This is a mandatory stipulation and IS Wing, HQ Office shall follow up with all field audit Offices for compliance.

3. Planning for an individual IS Audit assignment

The deliverable documents for the planning phase for individual IS Audit assignments are the Audit Implementation Guidelines (Guidelines hereafter) and the Audit Design Matrix, to be prepared as per the provisions of the Compliance Audit Guidelines 2016.



To prepare these documents, it is essential that decisions are taken to define key IS Audit elements such as Objectives, Scope, Methodology, Sampling and the Audit Design Matrix.

In turn, these decisions may be taken based on the following sequence of steps.

3.1 Understanding the audited entity

This step addresses the 'Inherent Risk' factor pertaining to the nature of operations of the audited entity. This step requires a detailed review of documentation such as legislation, Rules and Regulations, and executive instructions governing the functions of the audited entity. Also, documentation generated and published by the audited entity itself- such as Annual Reports, financial statements, media releases and social media posts may be reviewed. Finally, third party sources of information such as media reports, complaints and grievances may be reviewed. The core

business processes should be identified at this stage. The objectives of the audited entity, the compliance framework within which it operates and the risk areas inherent in its operating environment should be clearly understood.

3.2 Understanding the information system

This step addresses the 'Inherent Risk' factor pertaining to the risks arising from the very nature of operations of the audited entity and the 'Control Risk' factor pertaining to the quality of the internal control mechanism adopted to mitigate risks. This step requires a detailed comparison of the compliance framework of the audited entity with the system documentation, to identify potential gaps in the coverage of the business processes by the information system.

An indicative list of documents to be requisitioned from the audited entity is placed at *Annexure-I*. Field audit Offices may consider issuing the requisition for these documents for each information system that they have listed in their Strategic Audit Plan and obtain the responses from the audited entities well in advance. This would reduce turn-around time when a particular information system is proposed to be taken up as a subject matter in the next Annual Audit Plan.

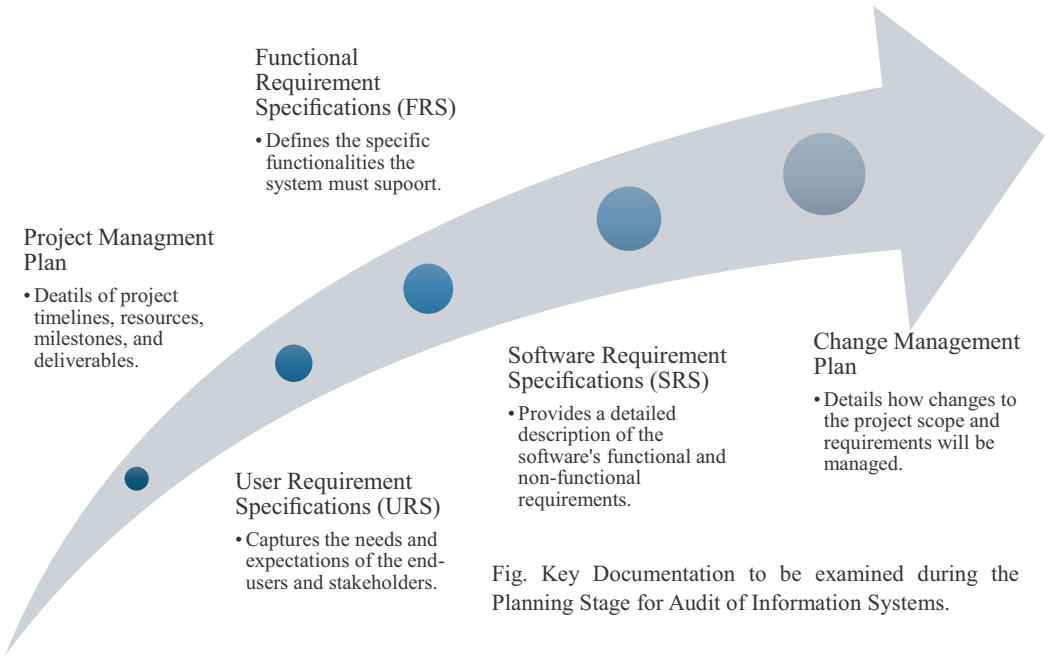


Fig. Key Documentation to be examined during the Planning Stage for Audit of Information Systems.

Review of these documents, especially the Functional Requirements Specification and the User Manual, is crucial to identify the extent to which business processes of the audited entity was planned to be automated and the points at which manual interventions are required to be made by users. By analysing the intended workflows as per the system documentation, field audit

Offices may be able to estimate the extent to which the information system is able to fulfil the business processes of the audited entity. This in turn enables the estimation of quantum of inherent risk associated with the core business processes which are not covered by the information system, and the quantum of control risk associated with the manual interventions for the uncovered processes. Such understanding in turn would enable field audit Offices to take decisions on the Scope and Audit Design Matrix for the IS Audit, with sound reasoning.

3.3 Understanding the application controls

This step addresses the 'Control Risk' factor pertaining to the quality of application controls implemented in the information system. This step requires a detailed comparison of the system documentation with the analysis of the data from the information system. For this purpose, field audit Offices should requisition the data set/ data dump from the information system for the period initially proposed for audit coverage (typically 5 years) from the audited entity.

Before commencement of data analysis, it is vital to ensure that the audited entity does not, at a later point of time, raise doubts on the integrity of the data set provided or repudiate the data set. For this purpose, it is desirable that suitable controls are adopted, such as obtaining a letter from the audited entity which specifies the data source (through reference to time stamp of generation of the data set/ hash value for the data set), along with the details of the parameters for extraction used to create the data set, i.e. queries/ scripts executed. If such a letter is not forthcoming from the audited entity, internal documentation may be generated by the field audit Offices for the above purpose, noting the date of receipt of the data set, the name of the personnel of the audited entity who handed over the data set, and the hash value for the data set and communicating/ getting confirmation on the same from the audited entity before commencing any data analysis. To the extent feasible, control totals for the data set may be reviewed and cross-verification from other sources may be carried out to derive assurance regarding the accuracy and completeness of the data set respectively.

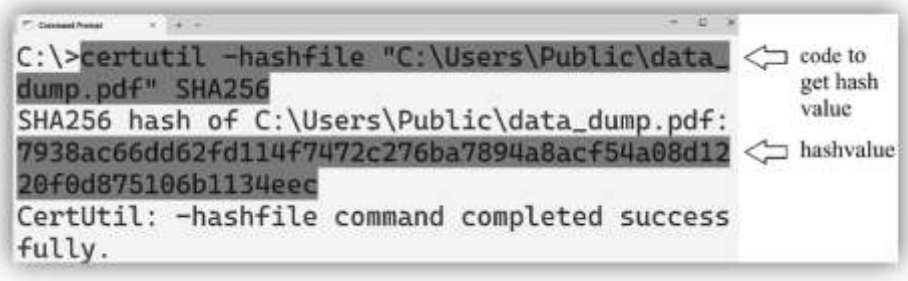


Fig. An illustration for generation of a SHA256 hash value of a (.pdf) file using command prompt.

The data analysis may then be commenced, with the objective of evaluating the extent to which the business rules for each business process have been correctly mapped into the information system. Each business rule is typically enforced in the information system as one or more application controls.

Three examples from analysis of data from information systems are enumerated below, as illustrations.

1. If analysis of a data set for the Integrated Financial Management System of a State Government reveals that the data table for recording details of Bills processed by DDOs has blank entries under the column for Sanction Order Number, this may be indicative of missing application controls to enforce linkage of each Bill with an underlying Sanction Order in the system.
2. If analysis of a data set for the e-Procurement system of a State Government reveals that the data table for recording time permitted for submission of Bids by vendors for e-tenders is lesser than the minimum prescribed time permitted by the applicable Rule, this may be indicative of missing application controls to enforce the minimum prescribed time for submission of Bids in the system.
3. If analysis of a data set for the Crime and Criminal Tracking and Networking System of a State Government reveals that the data table for recording timestamps of Arrests has entries which are chronologically earlier than the timestamps recorded for the associated First Information Report, this may be indicative of missing application controls to enforce chronological sequencing of dependent actions in the real world, in the system.

These red flags/ leads from the data analysis should then result in the formulation of appropriate Audit Issues in the Audit Design Matrices to be developed for these IS Audit assignments.

Data analysis should accordingly be carried out with reference to the system documentation and with such specificity, to identify the red flags/ leads/ risk areas which are to be included in the Scope and Audit Design Matrix for the IS Audit assignment. It may be noted that the results of the data analysis should be considered as corroborative evidence of the audit finding- the missing application control to enforce linkage of Bills with Sanction Orders- and not as the audit finding itself. The objective of IS Audit is to comment on such deficiencies in the application controls implemented in the information system (front end of the system i.e. from the user's perspective in various roles), by using the results of data analysis as red flags/ leads which indicate such deficiencies in the system at

the back end. For this purpose, field audit Offices should requisition access to a User Acceptance Testing (UAT)/ Training Module or assisted access to the Production Module *(without compromising the sanctity of data)* of the information system to check the for missing validation and application controls.

As part of the data analysis, field audit Offices should also carry out an evaluation of the integration of the information system with other IT applications. Discrepancies in the data transmitted to and received from other IT applications may be indicative of deficiencies in the application controls related to the interface between the two systems, and result in the formulation of an appropriate Audit Issue in the Audit Design Matrix to be developed.

3.4 Allocation of Resources

IS Audit assignments require allocation of appropriate human resources, who should have developed the understanding of the entity, business processes, system documentation and the risk areas from data analysis as outlined above.

Apart from IAAD personnel, field audit Offices may consider engaging domain experts (academics, researchers, consultants) with specific skills to augment the capacity of the audit team. The audit team should also be provided with adequate budget towards number of person-days for the IS Audit, infrastructure and software tools for data analysis and access to the Centre for Data Management and Analytics (CDMA), HQ Office as needed.

The standing instructions issued by HQ Office for such engagement with domain experts and CDMA, as well as for procurement and issue of software tools may be complied with.

3.5 Preliminary Assessment of Governance, General Controls and Application Controls

Based on the above steps, the audit teams should conduct a preliminary assessment, which should include:

i. Assessment that governance mechanism for the implementation and Monitoring of the information system has been adopted and is functioning as intended.

ii. Assessment that general controls for the standard list of domains[5] for information systems have been adopted. General controls relate to the operating environment within which all information systems are developed, implemented, and maintained. General controls are therefore not specific to any individual transaction stream or application but are concerned with the audited entity's overall IT infrastructure, policies, and processes for the standard list of domains, which are essentially horizontal support functions for an IT application-based information system.

iii. Assessment that business rules have been mapped into the information system and application controls to enforce business rules have been implemented. Application controls may be categorized as input controls, validation controls, processing controls and output controls.

The details of the aspects to be examined as part of the assessment have been elaborated in the next section of this Manual.

[5] List of domains which are to be examined in general for all types of information systems, derived from the IDI-WGITA Handbook on IT Audit. These domains include Procurement, Access Management, Change Management, Information Security Management, Disaster Recovery Management, Incident Response Management, Master Data Management, Maintenance Management and Consultant Management.

III. Definition of key IS Audit Elements

The definition of the Objectives, Scope, Methodology, Sampling and other elements for IS Audit assignments shall be prepared and approved as part of the draft Audit Implementation Guidelines document. The preparation and approval for the draft Guidelines document and the Audit Design Matrix document for IS Audits shall be carried out as per the processes prescribed by SMU/ PPG Wing, HQ Office for this purpose. This section of the Manual focusses on four elements for IS Audits- the Objectives, Scope, Methodology and the Audit Design Matrix, building upon the existing guidance.

1. Objectives

The Objectives of IS Audit assignments shall be to examine-

i. ***Whether governance mechanism had been adopted to ensure that the information system has been implemented in compliance with the approved functionalities, timelines and costs.***

ii. ***Whether general controls related to the operations of the information system have been implemented, in compliance with executive instructions.***

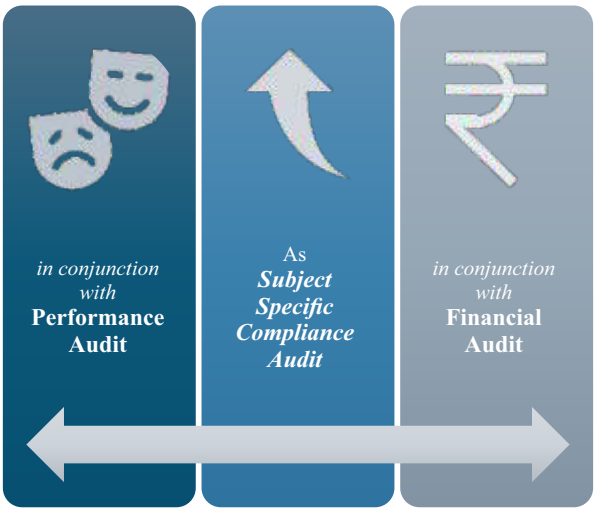
iii. ***Whether business rules have been correctly mapped and application controls have been Implemented in the information system, to ensure compliance with executive instructions.***

These Objectives correspond to the three broad functional aspects of Governance, General Controls and Application Controls. Aligned with the concept of Mutually Exclusive and Cumulatively Exhaustive (MECE), all potential risk areas and corresponding issues related to IS Audits may be categorized under the above three Objectives.

In all IS Audits, the audit teams shall organize the sub-Objectives and issues to be examined for individual assignments under the above three Audit Objectives. The extent of coverage under each Objective is dependent on the Scope of the IS Audit.

2. Scope

IS Audit can be conducted as a stand-alone Subject Specific Compliance Audit or in conjunction with a Financial Audit (to assess the conformity of an entity's financial statements with the statutory reporting framework) or a Performance Audit (to assess the aspects of efficiency, economy and effectiveness of the functioning of an entity).



IS Audit is not categorized under Financial Audit, since the objective when it is conducted in conjunction with a Financial Audit is to assess whether business rules have been correctly mapped and the required application controls have been implemented in order to enforce compliance with accounting standards, accounting policies and the statutory framework applicable to the audited entity for financial reporting.

IS Audit is not categorized under Performance Audit, since the variable of performance of an information system is dependent on other independent variables such as quantum of budgetary resources, adequacy of timelines for implementation and quality of human resources; the attribution of direct cause-effect relationships between these variables is challenging.

The scope of IS Audits shall consider three dimensions of coverage- time-period, list of entity-units and functionality.

i. Time-period

This Scope dimension refers to the period of audit coverage. The period shall typically be proposed as the latest five completed financial years (may be shorter if the period from inception of the IS project to the date of audit is less than five years). It is important to note that this time-period is required mainly to define the boundary for analysis of data to be extracted from the information system. It does not preclude analysis for the root-cause of any specific deficiency or irregularity that is identified by the audit team- which may be traced back to decisions taken during the implementation or further change management of the information system during a time-period well before the defined Scope of the IS Audit.

ii. Functionality

This Scope dimension refers to the list of functionalities and application controls which are proposed to be examined. This is arguably the most crucial Scope dimension, since it also impacts the Entity-Units dimension, as described below.

The process of selection of functionality proposed to be included in the Scope of the IS Audit shall accord higher priority to the core business processes of the audited entity, compared to the supporting business processes. In case of time and resource constraints, the core business processes may be covered in the first IS Audit assignment and the supporting business processes may be taken up as a subsequent IS Audit assignment. Core business processes are those which are required to fulfil the main organizational objectives of the audited entity, i.e. the purposes for which it has been constituted in the public sector. For example, in case IS Audit of the Enterprise Resource Planning (ERP) system of the Solar Energy Corporation of India Limited is being planned, the Scope shall prioritize the inclusion of the core business processes- power trading and power generation- over the supporting business processes such as human resources management and tax compliance.

Modern information systems are implemented with modular architecture, with individual Modules intended to fulfill a group of related and sequentially dependent business processes.

For example, some of the Modules in the **ERP system** of a Government PSU in a manufacturing sector may fulfill business processes as follows-

Sl. No.	Name of Module	Group of business processes fulfilled by the Module
1	**Finance and Control**	Invoicing, Receipts Management, Payments Management, Generation of Financial Statements, MIS Reports, Budget Management, Cost Accounting, Tax Compliance.
2	**Material Management**	Procurement, Inventory Management, Movement of input materials across organizational units

3	**Production Planning**	Production Shift Management, Production Target Management
4	**Quality Management**	Product Sampling, Quality Test Reporting
5	**Sales and Distribution**	Customer Account Management, Sales Order Management, Movement of finished products to customer
6	**Human Resources**	Recruitment, Training, Promotion, Transfer, Payroll, Exit Management for employees

For example, some of the Modules in the **Integrated Financial Management Systems** of State Governments may fulfill business processes as follows-

Sl. No.	Name of Module	Group of business processes fulfilled by the Module
1	**Budget Preparation, Approval and Distribution**	Preparation of budget estimates by administrative Departments, review of Budget estimates by Finance Department, approval of budget estimates by Legislative Assembly, allotment of approved budget to administrative Departments
2	**Sanctions**	Creation of Sanction Order by junior employee, review and approval of Sanction Order by Competent Authority, transmission of approved Sanction Order to DDO.
3	**Bills**	Creation of Bill by junior employee, review and approval of Bill by DDO, transmission of approved Bill to Treasury.
4	**Treasury**	Review of Bills received from DDO, payment of Bill amount to beneficiaries, transmission of Bill and payment data to Accounts.
5	**Government Receipts Accounting System**	Data entry into receipt form by user, receipt of payment from user, transmission of receipt data to Accounts.

6	**Accounts**	Compilation of Head-wise Accounts and Treasury-wise Accounts, Effecting Transfer Entries/ Alteration Memos, Effecting Inter-Government Adjustments, Effecting year end Accounting Adjustments.

Therefore, in an information system having modular architecture, the audit teams shall first review the system documentation to gain a clear understanding of the mapping and integration between the various Modules and the business processes which they fulfill, and then propose the inclusion of a specific list of Modules and a specific list of associated business processes under each Module accordingly. The selection of Modules and business processes in turn forms the basis for the selection of user-roles and individual workflows under those Modules and related to those business processes.

These are crucial decisions during audit planning which have a material impact on the overall relevance and viability of the resulting IS Audit product, and therefore should be taken after exercising due diligence in the assessment of risks involved, and the available time and resources.

iii. Entity-Units

This Scope dimension refers to the list of organizational units of the audited entity, where the audit teams propose to verify the status of implementation and use of the information system. Modern information systems are implemented with distributed architecture at various geographic locations where the audited entity has physical presence, the business processes of the audited entity are executed by different types of organizational units (nature of work differs) and the hierarchy of users in different organizational units of the entity may also differ widely (more senior, supervisory roles at HQ and junior roles at field formations). Based on assessment of risks associated with the geographic locations, nature of business processes and the user roles for each business process, the Scope of coverage of organizational units of the audited entity shall be proposed by audit teams, subject to availability of time and resources and nature of access available to the Audit.

3. Audit Design Matrix

i. Mapping between the ADM and the Audit product

To reiterate the provisions of the Compliance Audit Guidelines 2016, the Audit Design Matrix (ADM) shall maintain a clear mapping between the Audit Objectives, Sub-Objectives, Audit Issues, and the resulting Chapters (in case of stand-alone IS Audit Reports)/ Sections (in case the IS Audit is part of a longer Compliance or Performance Audit Report), Audit Paragraphs and Audit Sub-Paragraphs respectively.

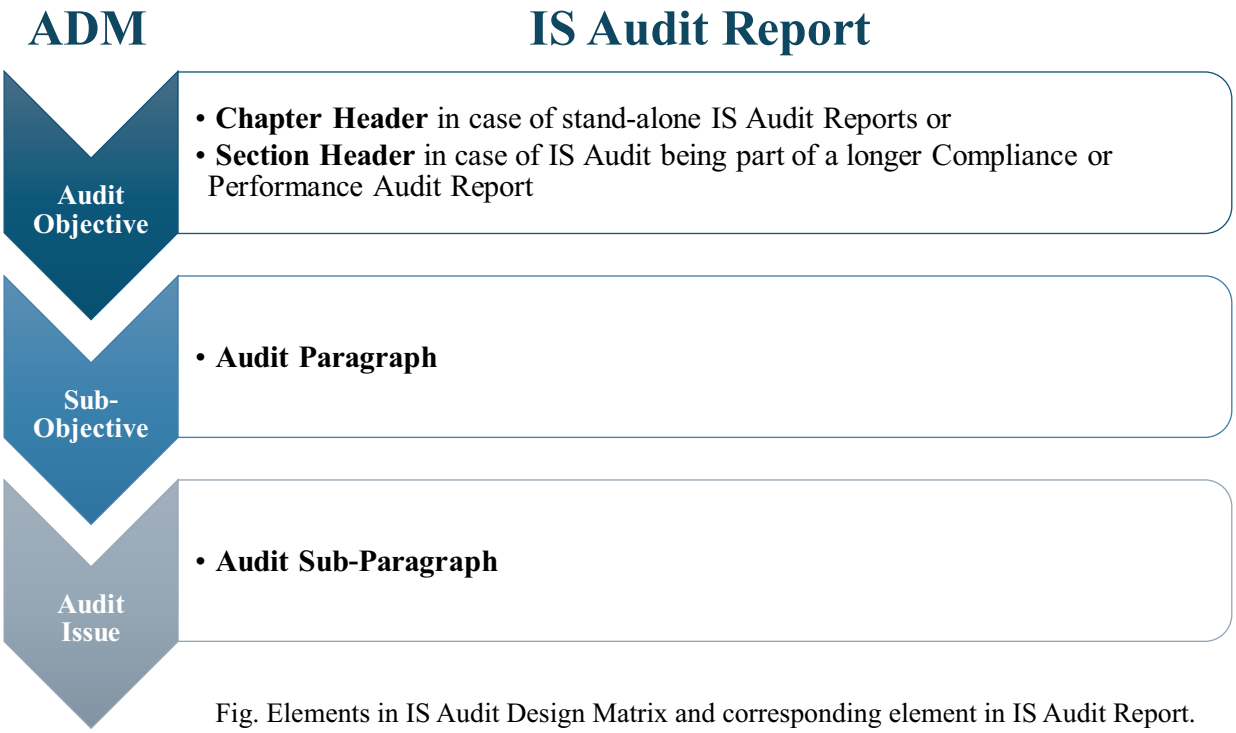


Fig. Elements in IS Audit Design Matrix and corresponding element in IS Audit Report.

ii. Rationale for the ADM document

The ADM is intended to serve dual purposes-

1. **Control-** To enable the Group Officer, the HoD of the field audit Office and IS Wing at HQ Office (though the Audit Findings Matrix) to derive assurance that the IS Audit has been executed by the audit team in compliance with the approved Scope. This aspect of control is intended to guard against potential scope creep/ roving expeditions during audit execution, and retains the focus on completing the examination of all the issues listed in the ADM.

2. **Accountability-** To enable the maintenance of a clear trail of the list of issues that were included in the Scope of IS Audit and examined during audit execution. If, after the conclusion of the IS Audit assignment, a particular deficiency or irregularity in the information system which was not included in the Audit product is subsequently detected by either the audited entity or a whistleblower or through a media report, the IAAD would be able to review the ADM and working papers and determine whether the highlighted issue had been included in the ADM or not. This would then form the basis for concluding either that the issue had not been examined since the risk factors were not known/ could not be substantiated at that point of time or that the issue had been reportedly examined but due diligence had not been exercised.

   In view of these aspects, the audit teams and all Officers responsible for review of the Guidelines, ADM and the resulting product for IS Audits are expected to be very careful in preparing the Audit Design Matrix and ensure that they maintain adequate documentation in support of either the resulting audit observation for each issue in the ADM or the basis on which they were able to derive assurance on status of compliance for each issue in the ADM.

iii. Contents and granularity of details in ADM

For the first two Objectives of IS Audit assignments related to Governance and General Controls, the contents and granularity of details in the ADM shall be largely standardized, as per the indicative Checklist of Issues in Annexure-II. For the third Objective of IS Audit assignments,

1. The contents of the ADM shall be specifically organized Module-wise (in case of information systems with modular architecture) or business process-wise at the level of Sub-Objectives.
2. The contents of the ADM shall be specifically organized business rule/ application control-wise at the level of Audit Issues. This is because mapping each business rule applicable to the audited entity into the information system would require the implementation of application control(s) to enforce that business rule.

As can be seen from the indicative Checklist at Annexure-II, the level of granularity for Sub-Objectives and the Audit Issues listed under each Sub-Objective is intended to be sufficiently clear and specific, so that visualization of the contents of the resulting Paragraphs and Sub-Paragraphs in the IS Audit product is facilitated.

To reiterate, achieving this clarity at the granularity level of Audit Issues is a key determinant of the relevance and viability of the IS Audit product.

Two examples (for audit of e-Procurement Systems and Integrated Financial Management Systems implemented by State Governments) of ADM for Audit Objective 3 related to Application Controls are placed in Annexure-III, which may be used as ready reference for the purpose of deciding the level of granularity in the ADM for audit of information systems.

The selection of Modules and business processes in turn forms the basis for the selection of user-roles and individual work flows under those Modules and related to those business processes.

The decisions related to the listing and selection of Audit Issues in the ADM are crucial decisions during audit planning which have a material impact on the overall relevance and viability of the resulting IS Audit product, and therefore should be taken after exercising due diligence in the assessment of risks involved, and the available time and resources.

4. Methodology

The provisions in the Compliance Audit Guidelines 2016 which are related to Audit Methodology shall be applicable to IS Audit assignments.

Apart from review of documents, engagement with the audited entity and analysis of data sets extracted from the information system, one additional Audit technique which shall be employed during IS Audits is conduct of Joint Walk-through.

Joint Walk-through refers to the formal observation of a demonstration of the workflow implemented in the information system for a selected business process by a selected user role in the production/ test environment, conducted in the presence of the members of the audit team and representatives of the audited entity. Participants attending the Joint Walk-through then jointly certify the facts observed during the demonstration, with emphasis on recording the fact of any

missing application controls (input controls to ensure completeness of data entered, validation controls to ensure that only permissible values/ ranges of data are entered, processing controls to ensure that computations are carried out correctly, output controls to ensure that data is presented in the correct formats/ graphical representations and security controls to ensure that view/ modify access rights have been implemented in compliance with business rules) further corroborated/ supported by the evidence of such observations in the audit product through data analysis.

This technique is equivalent to the Joint Physical Inspections (for assets) which have been consistently conducted by audit teams in the Department. The use of this technique is necessary to establish the fact of missing application controls, since the workflows where there are absent may require a particular user role to be logged into the system. Only the sequential screenshots and the bare fact of the absent application controls shall be recorded in the joint certification- any analysis on the potential impact of the missing controls shall not be included. This is intended to mitigate the risk of representatives of the audited entity being reluctant to participate. Field audit Offices may consider nominating Group Officers to conduct Joint Walk-throughs for an identified list of workflows (drawing from the Audit Issues in the ADM), and request for the presence of an appropriately senior representative from the audited entity for this exercise.

In the absence of joint certification of the fact that application controls are indeed absent, the evidence in support of this fact would be restricted to the results of data analysis and sequential screenshots of the workflow. That would result in the quality of the audit evidence not being as robust as would be the case if Joint Walk-throughs were conducted.

IV. Mapping the domains for IS Audit

This section provides an overview of the recommended mapping of the domains listed in the IDI-WGITA Handbook on IT Audit Handbook and the COBIT 2019[6] framework, with the standardized Objectives and Sub-Objectives for IS Audits, as placed in the Indicative Checklist of Issues at Annexure II of this Manual.

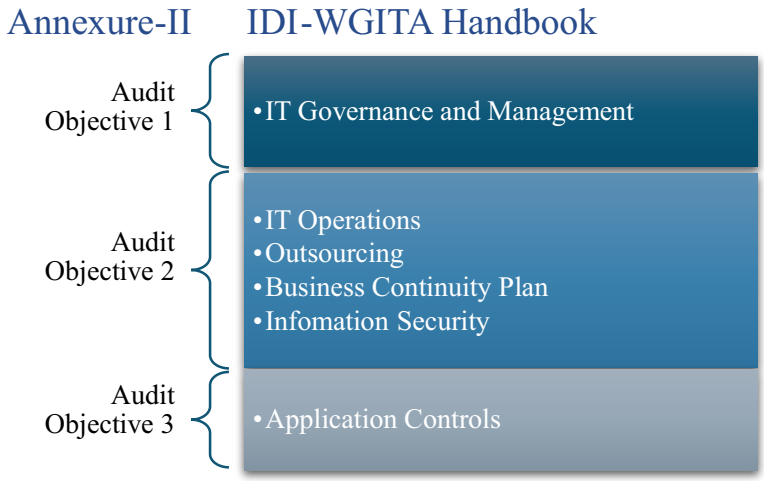


Fig. Reference to the Indicative Checklist of Issues at Annexure-II *(Audit Objectives)* to Name of the domain in the IDI-WGITA Handbook on IT Audit.

Any specific reference to an Audit Issue which can be categorized under the domains listed in the IDI-WGITA Handbook may therefore be appropriately incorporated into the Indicative Checklist of Issues, to prepare the ADM for IS Audit assignments.

A brief explanation of the domains listed in the COBIT 2019 framework is as follows.

- **Evaluate, Direct and Monitor (EDM)** addresses the evaluation of strategic options by the governing body, directions issued to senior management and the monitoring of the achievement of the selected strategy.
- Management objectives are grouped in four domains:
  - ✓ **Align, Plan and Organize (APO)** addresses the organization, strategy and supporting activities.
  - ✓ **Build, Acquire and Implement (BAI)** treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
  - ✓ **Deliver, Service and Support (DSS)** addresses the operational delivery and support of I&T services, including security.
  - ✓ **Monitor, Evaluate and Assess (MEA)** addresses performance monitoring and conformance of I&T with performance targets and control objectives.

[6]Https://www.isaca.org/resources/cobit

The recommended mapping of the domains listed in the COBIT 2019 framework with the Indicative Checklist of Issues is as follows.

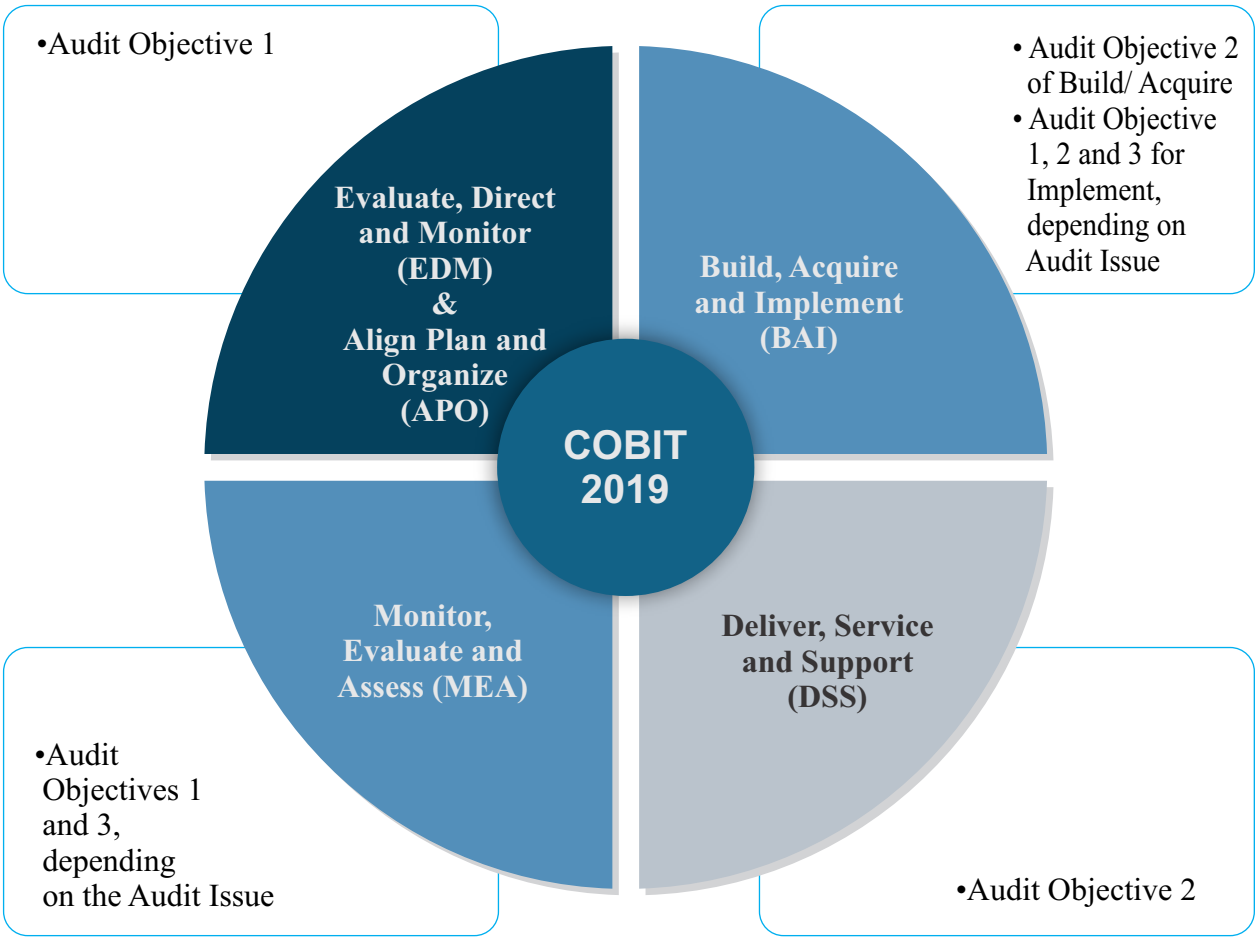


Fig. Mapping of domains in COBIT 2019 framework to the indicative checklist of issues in Annexure II

Any specific reference to an Audit Issue which can be categorized under the domains listed in the COBIT 2019 framework may therefore be appropriately incorporated into the Indicative Checklist of Issues, to prepare the ADM for IS Audit assignments.

V. IS Audit Execution

1. Governance Mechanism

IS Auditors shall examine the Audit Issues under the Audit Objective 1 as per the ADM, exercise the checks listed below against each Audit Issue and suitably comment on the deficiencies noticed.

1.1 Organizational Structures

Audit Issue	**Organisational Structures**
Checks to be exercised	1. Governance Committees (Apex Committee or Steering Committee or High-Level Committee or Implementation Committee etc.) have been constituted. 2. Senior representative of the entity has been designated as the CIO or Project Manager. 3. Project Management Unit has been constituted to implement the decisions taken by the Governance Committees. 4. Roles and responsibilities of the above organizational structures have been specified and documented. 5. Communication of the above documents has been made to the personnel concerned. 6. Minutes of meetings of the Governance Committees have been maintained and Committees have met at prescribed intervals.

IS Auditors should comment on the absence of organizational structures entrusted with governance and management responsibilities, and on shortfalls in the number of review meetings held by them to monitor the progress of implementation and status of operations of the information system.

1.2 Policies

Audit Issue	**Policies**
Checks to be exercised	Formal Policy documents have been adopted by the Governance Committees or higher-level organizational

	Structures and communicated to stakeholders, on the following subject matters 1. Procurement (for hardware and software assets as well as for hiring the project consultant and software services Provider) 2. Access Management 3. Change Management 4. Incident Response Management 5. Information Security Management 6. Business Continuity and Disaster Recovery

IS Auditors should comment on the absence of formal policies on these subject matters as they are likely to result in the risk of deficiencies in the related downstream functions during the operations phase of the information system. In the absence of formal policies, there would be no triggering mechanism to measure or report such deficiencies to the Governance Committees, resulting in reduced oversight.

1.3 Risk Management

Audit Issue	Risk Management
Checks to be exercised	1. Formal Risk Management document has been adopted by Governance Committees. 2. Documented Risk Register (using IT tools such as Jira or otherwise) to record the material risks has been maintained. 3. Evaluation and categorization of the material risks has been carried out, based on criticality to business functions 4. Timelines and sequence in which the material risks need to be addressed have been specified 5. Recommendations have been made by Governance Committees on mitigation measures to be adopted and identification of personnel responsible for such mitigation measures

	6. Governance Committees have followed up on their recommendations to verify that risks have been mitigated and if not, have held the concerned personnel accountable.

The material risks that may arise during the implementation and operations of information systems could include:

- Time overruns, with delays beyond scheduled timelines for project implementation
- Cost overruns, with actual expenditure exceeding budget
- Benefits from implementation not being realized due to continued parallel run with Manual processes or legacy systems
- Exit of key personnel from the audited entity or from the software services provider
- Excessive dependence on the software services provider even during the operational phase
- of the information system
- Absence of business continuity and disaster recovery processes
- Non-compliance with statutory requirements

IS Auditors should comment on the absence of formal Risk Management process or absence of the vital internal control of a Risk Register and associated practices outlined above, as it would result in the risk of delayed responses to adverse events and reflect deficiencies in the governance mechanism adopted for the information system.

1.4 Key Documentation

Audit Issue	Key Documentation
Checks to be exercised	1. User/ Functional requirements have been compiled and documented 2. Detailed Project Report has been prepared and updated regularly 3. Contract/ MoU/ Work Orders and SLA have been signed with/ issued to the software services provider with clear definition of work required to be done 4. Contract with the software services provider has clauses related to punitive actions for non-performance of obligations and for exit management (transfer of documentation to the audited entity prior

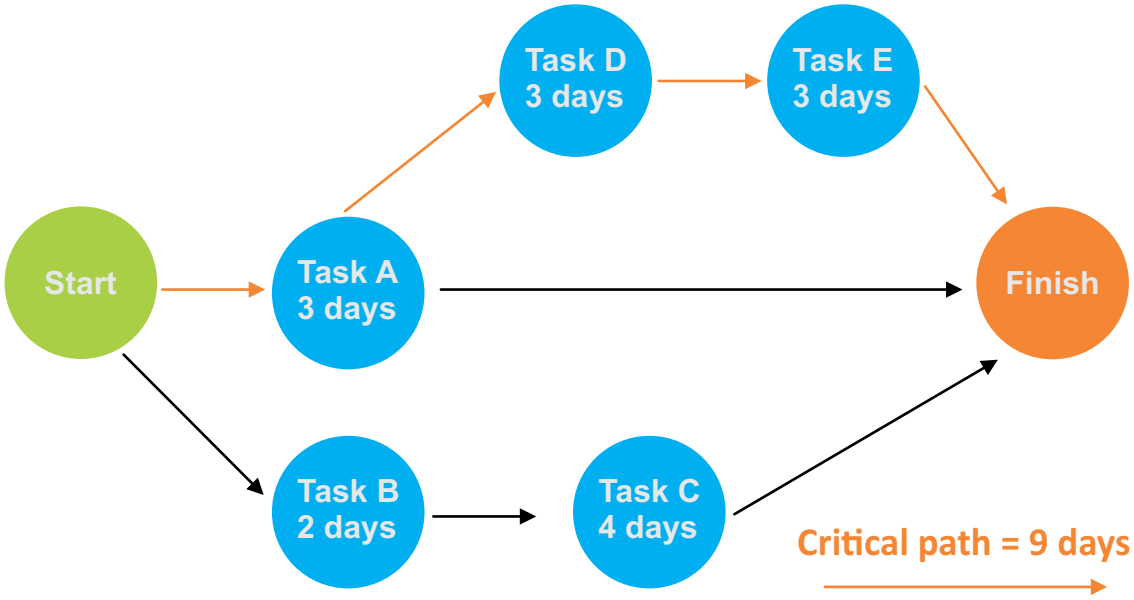
	to end of contract period and transfer of knowledge for a specified period to any successor software services provider after the end of the contract period). 5. Payments against invoices raised by the software services provider have been processed after verification of correctness of amounts payable.

IS Auditors should comment on deficiencies observed on the above areas, as they can result in incomplete/ incorrect implementation of the functionalities of the information system, inability to transition key personnel due to the absence of updated FRS/ Detailed Project Report, inability to penalize the software services provider even when there are defaults on the contractual obligations, excessive dependence and vendor lock-in with respect to the software services provider and excess payments due to lack of due diligence in verification of contractual deliverables when processing payments against invoices. Such instances would indicate severe deficiencies in the governance mechanism adopted for the information system

1.5 Monitoring the Progress of Implementation

Audit Issue	Monitoring the progress of implementation
Checks to be exercised	1. Whether task level details have been defined for the IT project, and sequential dependencies identified to determine the Critical Path for the project 2. Whether analysis has been carried out on the list of functionalities/ Modules not yet implemented (along with reasons) 3. Whether analysis of time and cost overruns (if any) has been carried out.

IS Auditors should review whether project plan had been prepared, clearly defining individual tasks, the interdependencies between tasks, and the critical path for project completion with a detailed timetable at the task level. The Project Monitoring Unit should have prepared such a project plan for review of the progress made in the implementation against the scheduled timelines for completion, by the Governance Committees.



The project plan may be prepared and monitored using Project Management tools (such as MS Project or otherwise). IS Auditors should review the project plans and highlight deficiencies. Some of the deficiencies that may be noticed from such review could include-

- Absence of a well-defined critical path for the project schedule, i.e. the sequence of dependent tasks[7] which establish the overall time requirement for the project had not been identified.
- Incomplete listing of tasks required to be completed to achieve completion of the overall project. Instead, the PMU may have only recorded scheduled dates for major tasks or milestones, without recording any sequentially dependent tasks.
- Non-utilization of the provision in the project planning tool for estimating resource costs, thereby resulting in lack of visibility over granular costs at the task level.
- Non-utilization of the provision in the project planning tool for estimating quantum of allocation of work to personnel, thereby resulting in unrealistic workloads for personnel.

[7]In Project Management, tasks are usually defined at the level of granularity of work assigned to each member of the project team which must be completed, for that member to take up the next task. Example of a set of tasks with sequential dependency could be "Write the source code for Module 3", "Perform Unit Test on Module 3", "Perform Integration Test for Module 3 with rest of the IT application", "Perform User Acceptance Test for Module 3", "Conduct user training for Module 3", "Deploy Module 3 in production environment".

- Absence of logical and sequential dependency between tasks, resulting in recording of infeasible sequencing such as initiation of testing phase for the project before the completion of build phase.
- Recording of sets of tasks with no details of either predecessor or successor tasks dependent on them, i.e. presence of unconnected references, not linked to any other tasks in the project in the plan.
- Absence of a clear revised timeline by which the entire project would be completed, based on delays already incurred during project implementation.

If such deficiencies in the project plan are noticed by IS Auditors, it would be challenging to derive assurance on the quality and effectiveness of the project planning and monitoring mechanism adopted. The absence of clarity on a sequential, task-wise baseline schedule and on allocation of work to personnel would result in the risk of implementing the project only on a best effort basis, which may in turn result in significant time overruns.

IS Auditors should also mandatorily comment on the list of functionalities/ Modules which have not yet been implemented despite the lapse of the scheduled timelines for completion, as on the date of audit. Absence of reporting the accurate status of implementation of these functionalities/ Modules to the Governance Committees and lack of review/ analysis of reasons for the delays would reflect severe deficiencies in the governance mechanism adopted for the information system.

1.6 User Adoption

Audit Issue	User Adoption
Checks to be exercised	1. Whether training has been imparted to users 2. Whether User Manual has been published 3. Whether extent of adoption of the application by users has been analysed Whether there is any continued parallel use of offline work processes (if any) even after implementation of the system (along with reasons).

IS Auditors should comment on the absence of user training and User Manual, as they carry the risk of adversely impacting user adoption.

IS Auditors should review whether there are any instances of continued parallel use of offline work processes or legacy systems even after the implementation of the information system being audited. Such instances typically highlight deficiencies in implementation of application controls, necessitating manual interventions or the use of other legacy systems for specific business process requirements which have not been fulfilled by the new information system.

For example, even the implementation of the Integrated Financial Management System by State Governments, the Drawing and Disbursing Officers as well as the District Treasury Officers in many States continue to use and rely on manually maintained Bill Registers. This continued reliance on manually maintained Registers is due to the fact IFMS in those States does not have application controls to keep track of available balances of sanctioned amounts in the Sanction Orders against which sequential Bills are drawn. As a result of this deficiency, the risk of excess drawal of Bill amounts (exceeding the Sanction Order amount) remains even after the implementation of IFMS. To prevent such excess drawal, DDOs and DTOs continue to use manually maintained Bill Registers. Such instances would indicate severe deficiencies in the governance mechanism adopted for the information system.

2. General Controls

IS Auditors shall examine the Audit Issues under the *Audit Objective 2* as per the ADM, exercise the checks listed below against each Audit Issue and suitably comment on the deficiencies noticed.

2.1 Procurement

Audit Issue	**Procurement**
Checks to be exercised	1. Whether engagement of software services provider has been carried out in compliance with the applicable Rules and executive instructions. 2. Whether engagement of project management consultant has been carried out in compliance with the applicable Rules and executive instructions. 3. Whether hardware and software has been procured in compliance with requirements identified and approved by the competent authority. 4. Whether engagement of service providers for outsourcing of functions of the information system has been carried out in compliance with the applicable Rules and executive instructions.

Audited entities may choose to either hire the services of a software services provider for building the IT application or procure a Commercial-Off-The-Shelf (COTS) IT application along with support services, for the information system to be implemented. This decision is also known as the Develop or Acquire decision or the Build or Buy decision.

Procurement (build or buy) is typically initiated by audited entities through solicitation (Request for Proposal). Solicitation is the process of documenting the requirements of the organization and collecting relevant documentation which will assist the potential software services providers in proposing solutions through either developing a custom-built IT application or through customization of a COTS IT application, for the information system to be implemented. The RFP is typically prepared by the audited entity with the help of project management consultants whose services have been hired for this purpose. General controls for Consultant Management have been discussed in a subsequent section of this Manual.

After the RFP is published, proposals received in response to RFP are evaluated, pre-bid meetings are conducted with the respondents to offer clarifications, tender is designed and published, bids received are evaluated and contract is awarded.

Outsourcing is the process of contracting an existing business process that the audited entity previously performed internally or of a new business function, to an external service provider. The service provider is then responsible for providing the contractually required services for the agreed charges. Audited entities may have chosen to outsource only selected parts or all its IT infrastructure, services or processes. Areas which may be outsourced could include:

- Operating infrastructure (which may include data centre and related processes)
- Cloud computing with options such as Infrastructure as a Service (IAAS), Platform as a Service (PAAS) and Software as a Service (SAAS)
- Processing of in-house applications by a service provider
- Systems development or maintenance of applications
- Installing, maintaining, and managing the desktop computing and associated networks.

IS Auditors should examine the status of compliance of the procurement process with the Procurement Policy and applicable statutory framework for the engagement of the main software services provider as well as any other outsourced services provider.

In previous IS Audit assignments, instances have been noticed where

- The RFP and tender for the information system did not have punitive clauses to levy penalties on and/ or terminate the contract with the incumbent software services provider, in cases of material breach of contractual obligations. This had resulted in continued dependence of the audited entity on the software services provider even in case of defaults in the performance of the contractual obligations and time and cost overruns. The incumbent software services provider had perverse incentives to maintain the status of the project as a going concern with no foreseeable project completion date, since the payments were based solely on the number of person-days committed to the project.
- The RFP and tender for the information system did not have clauses for Exit Management of the incumbent software services provider to transfer key documentation such as the source code, System Architecture, Data Flow Diagram and User Manual to the audited entity prior to end of contract period and for transfer of knowledge for a specified period to any successor software services provider (for operation and maintenance) after the end of the contract period. This had resulted in continued dependence of the audited entity on the software services provider (vendor lock-in), even after the end of the contract period.

- The only bidder who was well-informed and was able to submit the L1 bid for the subsequent phase of development, whose contract value was significantly higher than the first phase.

The outsourcing of functions can result in a vendor lock-in issue, since moving the data to a different service provider may require considerable resources and money. In addition, audited entities may become dependent on the software they are using with a specific cloud provider and would not be able to change the service provider.

2.2 Information Security Management

Audit Issue	Information Security Management
Checks to be exercised	1. Whether regular Internal Audits of the system have been carried out. 2. Whether periodic Security Audits by STQC and Vulnerability Assessment and Penetration Testing by CERT- IN empanelled vendors have been carried out. 3. Whether suitable action has been taken as follow-up from the identified issues arising from the Security Audits. 4. Whether system has user logs, an Application log and a Data Base Administrator log, for the purpose of Maintaining a trail for information security.

IS Auditors should examine whether Internal Audits have been carried out by the audited entity, whether the information system was required to be covered by Security Audits conducted by the Standardization Testing and Quality Council (STQC) and whether Vulnerability Assessment and Penetrating Testing was required to be carried out by vendors empanelled by the Indian Computer Emergency Response Team (CERT-IN), and comment on the periodicity of such reviews and actions taken by the audited entities on the risks identified and recommendations made.

Security Audit by STQC is carried out within the information system, with physical and logical access (usually with privileged Administrator access rights), to verify the system configuration and to scan for weaknesses and mis-configuration issues. So, it is a review of the system from the "inside-out" perspective. The Security Audit Report lists the identified weaknesses and mis-configuration issues along with associated risk levels and recommends actions to be taken for risk mitigation.

Vulnerability Assessment and Penetration Testing (VAPT) is carried out remotely from the public domain (the Internet), to detect exploitable vulnerabilities. So, it is a review of the system from the "outside-in" perspective. Based on the assessment of vulnerabilities identified and any sensitive information available in the public domain, a series of penetration tests are attempted- such as port scanning, system fingerprinting, service probing, password cracking etc.- using state-of-the-art software tools (commercial and open source) and techniques typically used by malicious hackers. The list of tools and techniques to be used during penetration tests are frequently updated by the CERT-IN, based on emergent cybersecurity threats and based on deep level of engagement with the ethical-hacker community. The VAPT should therefore be carried out by the vendors empanelled by CERT-IN, who have requisite expertise in the domains of cybersecurity. The objective of VAPT is to detect any material vulnerabilities in the cybersecurity and information security domains of the system and take remedial actions against penetration of the system by hostile and malicious State or non-State actors.

IS Auditors should mandatorily comment on the risks identified by these reviews against which mitigation measures have not yet been implemented, as well as recommendations made during these reviews against which action has not yet been taken for resolution. Such unaddressed risks and pending actions should be immediately highlighted by the IS Auditors to the Governance Committees, as they could potentially have material adverse impact on the functioning of the information system.

Deriving assurance on information security management with respect to the dimension of availability (i.e. to verify that access to view or modify data by authorized users is not restricted/ prevented due to lack of responsiveness on the part of the system) is the responsibility of the auditors who conduct the Security Audit and VAPT. This is because availability of the system is impacted through external attacks such as Distribute Denial of Service (DDoS), which are executed by malicious hackers. Identification of potential vulnerabilities in the system design and configuration which may be exploited to execute attacks affecting the availability of the system, is one of the key deliverables of these reviews.

Deriving assurance on the aspects of confidentiality and integrity of data when the system is subject to cyber-attacks from external actors is also the responsibility of the auditors conducting VAPT.

Deriving assurance on information security management with respect to the dimensions of confidentiality (i.e. to verify that user access to view data is restricted to only that data which they have been formally are authorized to view) and integrity (i.e. to verify that user access to modify data is restricted to only that data which they have been formally authorized to modify) for the registered users of the system is the responsibility of IS Auditors of the IAAD.

For this purpose, IS Auditors should examine the access rights (to view/ modify data) granted by the Administrator of the information system to individual users, and carefully verify that the access rights granted conform to the delegation of powers, to the organizational structure, and to the business processes which are required for that user. Access rights should be granted on a "need to know, need to function" basis, with no superfluous mapping of data access to users.

If the access rights have been granted in compliance with the business rules of the audited entity, the residual risk on the dimensions of confidentiality and integrity of data would only emanate from the users having privileged access rights. These include the System Administrator user for the front-end of the information system, i.e. the IT application and the Data Base Administrator user for the back-end of the information system, i.e. the database.

IS Auditors should carefully review the user logs (which maintain a trail of all user actions for individual registered users of the system), the Application log (which maintains a trail of all actions by System Administrator related to user access management for the front-end of the system) and the Data Base Administrator log (which maintains a trail of all actions by DBA related to modify data at the back-end of the system).

IS Auditors should mandatorily comment if user logs for individual registered users are missing for intervening periods of time, as it would be indicative of deletion of entries in the user logs through the back-end of the system. The risk in this scenario is that data in the information system could

An example from the Crime and Criminal Tracking and Networking System implemented by State Governments may illustrate this risk. A police user X acting with mala-fide intent to favour a person A, may irregularly record a fictitious entry in the General Diary for a complaint from person A against person B, which pre-dates a genuine entry in the General Diary for a complaint from person B to person A. This would make it seem like the genuine entry was only a reaction to the fictitious entry, and potentially impact the police investigation. At a later point of time, even if the police investigation concludes that a fictitious entry had been made, if the user log for X for that period is missing, it would be challenging to fix responsibility on that user.

have been modified by that individual user in such a manner that it results in an irregularity but wanted to evade fixing of responsibility for such irregular modification.

IS Auditors should mandatorily comment if Application log is missing/ incomplete for intervening periods of time, as it would be indicative of deletion of entries in the Application log through the back-end of the system. The risk in this scenario is that the System Administrator could have irregularly granted privileged access to view/ modify data to unauthorized users but wants to evade responsibility for such irregular grant of privileged access rights.

Another example from the Crime and Criminal Tracking and Networking System implemented by State Governments may illustrate this risk. A police user X acting with mala-fide intent to favour a person A, may persuade/ coerce the System Administrator to irregularly grant privileged access to user X to view the Charge Sheet under preparation in a case where user X is not involved at all, but in which has person A is the accused. This information from the Charge Sheet under preparation would be valuable to person A to potentially influence the witnesses and question the quality/ source of evidence. At a later point of time, if the Application log for that period is missing, it would be challenging to fix responsibility on the System Administrator and user X for such irregular leaking of the Charge Sheet under preparation.

IS Auditors should mandatorily comment if the DBA log is missing/ not furnished for audit scrutiny. As can be seen from the above description, the DBA log is the primary internal control which would have recorded the actions of the DBA in deleting data through the back-end of the system, either through execution of queries or scripts for that purpose. Absence of a DBA log is a material risk and should be immediately reported to the Governance Committees for remedial action and fixing of responsibility.

With reference to the above examples related to missing user log and Application log from the Crime and Criminal Tracking and Networking System implemented by State Governments, the risk associated with missing DBA log may be illustrated. If indeed the DBA had irregularly facilitated the deletion of entries from user log and Application through the back-end of the system, the DBA log would have entries to record the action by the DBA for deletion from the Application log (actions of the System Administrator to irregularly grant view access rights to user X) and to record the action by the DBA for deletion from the user log for X (actions of user X to view the Charge Sheet under preparation in a case that he wasn't involved with and to record a fictitious entry in the General Diary). If the DBA log is itself missing, then there would be no trail of evidence to fix responsibility for irregularities on the System Administrator or user X.

IS Auditors should therefore recommend that responsibility ought to be fixed on the DBA for the information system, in case DBA log is missing/ not maintained.

In previous IS Audit assignments, instances have been noticed where

- Information systems which are intended to cover critical public sector delivery processes have been implemented with the Community Edition of the open-source database instead of the Professional Edition. This in turn resulted in the absence of a .DBA log and had resulted in deletion of data at the back-end of the system, without the maintenance of a trail of irregular actions.
- The audited entity had not implemented the vital internal control of assigning the DBA role to its own personnel and instead relied on the software services provider to function as the DBA. This had resulted in the inability of the audited entity to fix responsibility for irregular deletions at the back-end, even when material irregularities- such as hard deletion of First Information Reports filed by police users- had been carried out by the DBA.

2.3 Disaster Recovery Management

Audit Issue	Disaster Recovery Management
Checks to be exercised	1. Whether Business Continuity and Disaster Recovery Plan has been documented 2. Whether Recovery Point Objective and Recovery Time Objective have been defined. 3. Whether Disaster Recovery Drills including restoration of backed up data have been conducted at prescribed intervals. 4. Whether RPO and RTO have been achieved in the DR Drills. 5. Whether suitable action has been taken as follow-up from identified issues arising from the DR Drills.

IS Auditors should examine whether Plans for Business Continuity and Disaster Recovery have been formulated, with provisions for the number of Near and Far Disaster Recovery Data Centres, frequency of data back-up (real time/ daily/ weekly etc.) and for replication of general controls (including physical controls such as perimeter security, guards, fire safety etc. and environmental controls such as Heating, Ventilation and Air Conditioning) applicable to the primary Data Centre at the DR Centres

IS Auditors should derive assurance that the two crucial controls for effective Business Continuity and Disaster Recovery- the definition of the Recovery Point Objective and the definition of the Recovery Time Objective- have been adopted by the audited entity. The RPO defines the point of time up to which the business data is required to be restored, in case of a disaster event. The RTO defines the point of time by which the business data is required to be restored, in case of a disaster event.

To illustrate, if an earthquake occurs at 3 PM on a particular date and the RPO has been defined as 4 hours and RTO has been defined as 2 hours, it would mean that the audited entity should have its information system restored for regular use by 5 PM (2 hours RTO), with all data up to 11 AM on that date (4 hours RPO) restored for use.

Depending on the criticality of the information system, the value of the data being stored in the information system and the costs for data back-up and restoration, audited entities should adopt appropriate RPO and RTO. sFor example, critical information system used by a Stock Exchange may define very low values for RPO and RTO to uphold investor confidence and prevent panic, while a less critical information system (such as one for processing applications for Vehicle Driver Licenses) may define higher values for RPO and RTO.

IS Auditors should also review whether Disaster Recovery Drills have been conducted at the prescribed frequencies and examine the DR Drill Reports to derive assurance that the identified risks and recommended mitigation measures have been implemented by the audited entity. IS Auditors should immediately report any unaddressed risks and pending actions to the Governance Committees, as they may have a material impact on the functions of the information system.

2.4 Access Management

Audit Issue	Access Management
Checks to be exercised	1. Whether there is a documented user registration and de-registration procedure for granting access, including mandatory fields for KYC. 2. Whether the access rights given to users is compliant with delegation of powers and extant Rules. 3. Whether password policy and Multi Factor Authentication of users is in place for login management. 4. Whether a system log is maintained to record details of the user who has completed verification of KYC and other details of registration of new users, before they can access the system.

Under Access Management, IS Auditors should examine the controls implemented for both categories of users- the personnel of the audited entity itself (Departmental users hereon) and other stakeholders including members of the public (external users hereon).

IS Auditors should derive assurance that every user registered in the system- Departmental and external- is unique and that there are clearly defined mandatory data fields in the system which function as the primary key to establish such uniqueness. For example, Departmental ID Number for Departmental users and Permanent Account Number (PAN)/ Aadhaar Number for external users could be used as the primary keys. In addition to the entry of the data into the concerned data fields to establish uniqueness, IS Auditors should examine whether the system has controls to

i. Prevent duplicate registration of users- For example, when Departmental ID Number or PAN/ Aadhaar Number which has already been entered by a previously registered user is attempted to be entered, the system should prevent the registration process from being completed.

ii. Verify the veracity of the data entered- For example, the system may have controls for mandatory upload of a scanned copy of the Departmental ID Card/ PAN Card/ Aadhaar Card by users during the registration process, in addition to keying in the Departmental ID Number and PAN/ Aadhaar Number as data. The system may permit access to the newly registered users only after an existing Departmental user has completed a workflow in the system, confirming that the data entered matches the information on the uploaded documents. A system log records the details of the existing Departmental user who completed the verification process.

Apart from the data fields which function as the primary key in the system, IS Auditors should review whether other data fields have been defined to fulfil Know Your Customer (KYC) norms. The concept of KYC norms is derived from the financial services industry and refers to information related to an entity (a unique user in this case) which is required for communication with the entity, executing transactions with the entity and generating aggregated MIS Reports for that entity. This KYC information does not establish the uniqueness of the entity and therefore should be mapped with the primary key for that entity. In case of information systems, the typical KYC data fields would be mobile number, email ID and bank account number for users, which should be mapped to the primary key. Since the primary key establishes the uniqueness of users, mapping of more than one mobile number/ email ID or bank account number to the same primary key (such as PAN/ Aadhaar Number) reflects the material risks such as potential misappropriation (in case of information systems intended to disburse scholarship amounts to multiple beneficiaries mapped to the same bank account number), potential cartelization (in case of e-procurement systems with multiple bidders mapped to the same mobile number or email ID or IP address) or potential evasion from law enforcement (in case of an information system which has the details of the accused individual in multiple phone fraud crimes recorded with different names/ aliases but with the same mobile number).

As described in the section of this Manual on Information Security Management, the main objective of examination of Access Management for Departmental users is to derive assurance that access rights (to view/ modify data) granted by the System Administrator conform to the delegation of

powers, to the organizational structure, and to the business processes which are required for that user. Access rights should be granted on a "need to know, need to function" basis, with no superfluous mapping of data access to users. This means that the access rights should be granted and modified as and when events occur in the Departmental users' service careers- grant of access rights during registration of new Departmental user at the time of recruitment, grant of additional access rights at the time of promotion, modification of access rights at the time of transfer and revocation of access rights during de-registration of Departmental users at the time of resignation/ retirement/ termination- in compliance with the business rules of the audited entity.

IS Auditors should examine whether standard controls related to adoption of a strong password, mandated change of password on first login, frequency for mandated change of password, multi factor authentication (One Time Password to mobile number/ email ID) have been adopted, to mitigate the risk of unauthorized users accessing the system with the login credentials which are weakly designed or protected.

2.5 Master Data Management

Audit Issue	**Master Data Management**
Checks to be exercised	1. Whether key and sensitive data fields which constitute master data (such as Bank Account Numbers) have been identified. 2. Whether there is a documented procedure for addition/ modification and deletion of master data, with specified roles for this purpose. 3. Whether segregation of duties has been ensured through maker-checker model for modifications to master data. 4. Whether master data management has been carried out in compliance with the delegation of powers for users. 5. Whether the system maintains a log for changes made to the master data, with user names and time stamps recorded.

IS Auditors should examine the controls implemented for Master Data Management in the information system.

Depending on the business processes covered by the information system, the audited entity should have identified key and sensitive data fields which constitute the master data for the system. These are the data fields whose modification without following due process may result in financial/ reputation loss for the audited entity. For example, for the Integrated Financial Management System implemented by State Governments, the key and sensitive master data could include the list of Heads of Accounts, the list of Departments, the list of DDOs, the list of DTOs, the list of Personal Deposit Account Administrators and the list of Bank Account Numbers for payment beneficiaries. Modifications to these data fields by individual users on their own- either through gross negligence leading to error or mala-fide intent leading to irregular acts- could result in significant loss of budgetary control, inability to incur expenditure and even misappropriation of public funds.

It may be noted that Master Data Management is a general control distinct from Access Management. This is because it is required even when there is assurance that all the users in the system are registered and authorized users and that each user has been granted access rights in conformity with the delegation of powers and other business rules applicable to the audited entity. Master Data Management is required to be implemented in the information system to enforce the principle of segregation of duties for key user roles who have been entrusted with the responsibility to make modifications to key data fields in the information system.

IS Auditors should review whether segregation of duties (SOD) has been enforced in the system in the form of SOD matrix in the user access table (listing access rights which carry potential conflicts of interest and therefore cannot be assigned to the same user) or in the form of system workflows for business process to modify master data which require a second user to approve the proposed modification by the first user (maker-checker model).

IS Auditors should also review whether a system log to record the details of the modification to key and sensitive master data fields is being maintained in the information system, so that responsibility may be fixed by the audited entity in cases where the maker-checker have colluded among themselves.

2.6 Change Management

Audit Issue	Change Management
Checks to be exercised	1. Whether there are any pending Change Requests/ Change control Notes which have not yet been implemented. 2. Whether User Acceptance Tests have been conducted before introducing any changes to the production environment.

IS Auditors should examine the controls implemented for Change Management in the information system. The organizational structure for initiating and completing Change Management should have been defined by the audited entity in its Change Management Policy. Typically, either one of the Governance Committees or a dedicated Change Management Committee is entrusted with the responsibility of collecting Change Requests from Departmental users and external users of the information system.

IS Auditors should examine whether the organizational structure for Change Management has listed, categorized the Change Requests and prioritized the Change Requests that have to be implemented, along with the sequence (some Change Requests may be sequentially dependent on others).

IS Auditors should examine whether the status of pending Change Requests (along with associated risks if not implemented and potential benefits to the audited entity if implemented) has been reported to the Governance Committees. IS Auditors should include a specific comment on pending Change Requests which have been approved for implementation but not yet implemented as on the date of audit, with age-analysis and analysis of causes for delays noticed. Approved Change Requests are typically communicated to the software services provider as Change Control Notes, which are part of the key documentation to be examined during IS Audit.

IS Auditors should examine whether User Acceptance Tests with relevant business process owners and users have been conducted and documented for the changes to be implemented and checked for edge/ corner cases, before their introduction into the production environment for the information system.

2.7 Incident Response Management

Audit Issue	Incident Response Management
Checks to be exercised	1. Whether issues reported by Help Desks and as incidents have been categorized by type and analysed. 2. Whether there are any major issues identified by Help Desks and/ or incidents reported, which have not yet been acted upon. 3. Whether the system experienced any downtime/ outage during the audit period and whether root cause analysis was carried out and mitigation measures have been taken to prevent recurrence.

IS Auditors should review the Policy for Incident Response Management adopted by the audited entity. The organizational structure for Incident Response Management in large organizations typically includes provisions for distributed (geographic location-wise or organizational unit-wise) Help Desks as tier 1 support, a central Technical Support Team deployed by the software services provider as tier 2 support and the core Developer Team of the software services provider as tier 3 support. Each tier responds based on the criticality of the incidents reported, with clear criteria (nature of incident/ lapse of period for resolution of incident) for escalation to the higher tier.

IS Auditors should review whether the incidents reported to the different tiers have been categorised by type, analysed by the PMU and reported to the Governance Committees at regular intervals. IS Auditors should examine whether reported incidents which require changes to be implemented to the system have been reported to the Change Management Committee for their conversion into formal Change Requests and inclusion in the list of Change Requests that have to be implemented, along with the sequence (resolution of some incidents/ Change Requests may be sequentially dependent on others). IS auditors should also test check the tickets raised by the system users and the action taken against the same, and whether the action was taken timely and satisfactorily.

IS Auditors should include a specific comment on major incidents reported which have not been resolved despite the lapse of the prescribed time criteria for resolution and include a comment on the age-analysis for escalation across tiers and analysis of causes for delays noticed.

2.8 Maintenance Management

Audit Issue	Maintenance Management
Checks to be exercised	1. Whether any identified hardware and software procurement/ upgrade requirements have not yet been acted upon. 2. Whether inventory of hardware and software assets has been prepared and kept updated. 3. Whether any maintenance issues identified and communicated by the software services provider have not yet been acted upon.

IS Auditors should the above aspects related to Maintenance Management. IS Auditors should review whether the audited entity has adopted policies to define the period of useful life for major hardware assets, to determine replacement timelines and initiate timely procurement.

IS Auditors should examine the correspondence/ communication with the software services provider to identify whether any hardware or software assets carry the risk of obsolescence in the absence of immediate upgrades, and whether the PMU for the information system has reported such maintenance requirements to the Governance Committees at regular intervals.

IS Auditors should include a specific comment on major hardware and software upgrades and additional procurement which have been identified but have not been acted upon, with age-analysis and analysis of causes for delays noticed. Continued use of obsolescent assets carries the material risk that these assets which are beyond the normal support period by their manufacturers/ developers may fail and have a material adverse impact on the functions of the information system.

IS Auditors should examine whether an Asset Register (using a software tool or otherwise) has been maintained for the hardware and software assets for the information system. The Asset Register should have relevant data fields to function as controls. For example, hardware assets should have data such as book value, warranty period, physical location, ID of Departmental personnel designated as owner of the asset, useful life, depreciation, current value etc., to enable the audited entity to transfer, sell, dispose and replace the hardware asset. Similarly, software assets should have data such as license number, cost of license, license renewal date, ID of Departmental personnel to whom the license has been assigned, free technical support period etc., to enable the audited entity to renew licenses on time (to avoid penalties) and to regulate payments to software product owners.

2.9 Consultant Management

Audit Issue	Consultant Management
Checks to be exercised	1. Whether KPIs for monitoring the performance of the consultant have been defined. 2. Whether payments to the consultant have been made after review of the services delivered and after review of requirement to continue the engagement of consultancy services.

IS Auditors should review the procurement process to hire the services of the project management consultant engaged for the information system.

The **Project Management Consultant** is typically engaged to assist the audited entity in the following processes-

- Preparation of RFP
- Evaluation of proposals received in response to RFP
- Preparation of tender and definition of technical bid evaluation criteria
- Technical bid evaluation
- Project Monitoring during the implementaion phase
- Service Level Monitoring during the operations and maintenance phase

IS Auditors should examine whether Key Performance Indicators for the project management consultant have been defined in the contract signed with the audited entity, with clear definitions of role and responsibility, timelines for work deliverables, format for work deliverables (documents) and the specific metrics to be measured to determine amounts payable by the audited entity. IS Auditors should comment in case of lack of clarity/ definitions for these aspects in the contracts.

The key risk associated with the audited entity engaging a project management consultant is that the latter may develop a vested interest in extending the contract as a going concern, with no foreseeable time horizon for termination. This risk typically arises due to excessive dependence on the project management consultant for the functions of project monitoring and service level monitoring.

The excessive dependence may be evidenced through

i. Absence of documentation on the work done by the consultant in the form of deliverables and absence of minutes of meetings held by the consultant.

ii. Communications taking place only between the consultant and the audited entity on the one hand, and between with the consultant and the software services provider on the other.

iii. Repeated extensions of contract despite absence of documentation required by the contract, engagement of retired personnel as consultant, and retention of the same individual as consultant despite that individual having changed his/ her employer.

The absence of documentation of the deliverables is a red flag, usually indicative of the consultant keeping all key information to himself and not sharing the same with the audited entity.

IS Auditors should comment on the absence of a clear plan and timelines to take over the functions of the consultant through knowledge transfer to Departmental personnel.

3. Application Controls

IS Auditors shall examine the Audit Issues under the Audit *Objective 3* as per the ADM, exercise the checks listed below against each Audit Issue and suitably comment on the deficiencies noticed.

The examples of how ADMs specific to the mapping of business rules and implementation of application controls to enforce the business rules are included in *Annexure-III*. The audit of application controls is therefore very specific to the information system in question. This section of the Manual therefore only contains a description of the different types of application controls that are implemented in most information systems, and general guidance on how they may be tested by IS Auditors.

3.1 Input and Validation Controls

Input controls are implemented to ensure completeness of data required to be entered by users for the workflows which correspond to the business processes covered by the information system. Validation controls are implemented to ensure that only permissible values/ range of values/ data types/ data available in the master tables are entered into the system by users.

IS Auditors should exercise the following checks-

i. Obtain functional description for each class of input and design information for data entries for each workflow proposed to be examined.

ii. Inspect the functionality and design for the presence of timely checks and error messages for users.

iii. Assess whether validation criteria and parameters on input data match the business rules and enforce rejection of unmatched input types.

iv. In case of online processing systems, verify that invalid data is rejected or edited on entry and test the logic checks/ calculation checks performed. Database operatives (such as *, =, or, select) should be disallowed as valid input, as they can be used to disrupt or retrieve information from the database.

v. Determine which interfaces exist with other IT applications. These interfaces could be in the form of real-time data transmission or periodic transmission of data files via batch processes. Review the system flow diagrams to obtain information on interfaces and validation controls for data imported into the information system.

3.2 Processing Controls

Processing controls are essential for ensuring correct computations, conversion, enhancement and transformation of data in the information system, through the entire transaction processing cycle in the system workflows.

IS Auditors should exercise the following checks-

i. Assess the processing logic from a study of the data flow chart and the defined and established business process rules.

ii. For critical transactions, process a representative sample outside the system to verify that the processing controls have been implemented correctly. For example, pension calculations for a sample of cases may be carried out using other software tools and results compared with the system generated results.

iii. Inspect the functionality and design for the presence of sequence and duplication errors, referential integrity checks, control, and hash totals.

iv. Inspect reconciliations and other documents to verify whether input counts are coherent with output counts to ensure completeness of data processing.

v. Trace transactions through the process to verify that reconciliations effectively determine whether file totals match or the out-of-balance conditions are reported.

vi. Enquire whether control files are used to record transaction counts and monetary values, and that the values are compared after posting.

vii. Verify that reports are generated identifying out-of-balance conditions and that the reports are reviewed, approved and distributed to the appropriate personnel.

viii. Verify that the application correctly identifies transactional errors, and that data integrity is maintained even during unexpected interruptions to transaction processing. This requires appropriate functionality for handling processing errors, review of suspense files and subsequent clearance.

3.3 Output Controls

Output controls are essential to ensure that output information is presented in complete and accurate form for users. Output controls include not only individual application controls to present the output data but also functionalities for system generated alerts and exception reports, which have been illustrated in the two examples at *Annexure-III*.

IS Auditors should exercise the following checks-

i. Procedures have been designed to ensure that the completeness and accuracy of application output are validated prior to the output being used for subsequent processing, including use in end-user processing.

ii. Examine the balancing and reconciliation of output as established by documented methods.

iii. Select a representative sample of electronic output, and trace selected documents through the process to ensure that completeness and accuracy are verified before other operations are performed.

iv. Examine if each output product contains processing program name or number, title or description, processing period covered, user ID and location, date and time prepared, and security classification.

v. Select a representative sample of output reports and verify that potential errors are reported and centrally logged.

3.4 Application Security Controls

Application Security controls are essential for security in application transactions through maintenance of log trails.

IS Auditors should exercise the following checks-

i. Obtain documentation and assess the design, implementation, access and review of audit trails.

ii. Inspect the audit trail structure and other documents to identify user roles who can disable or delete the audit trails.

iii. Inspect the audit trail to verify that adjustments, overrides and high-value transactions are designed to be reviewed in detail.

iv. Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to verify that periodic review and maintenance of the audit trail results in detection of unusual activity and supervisor reviews are effective.

v. Inquire how the access to the audit trail is restricted. Examine access rights and access logs to the audit trail files. Verify whether only restricted and authorised personnel have access to the audit trail. Assess if the audit trail is protected against privileged modifications.

VI. Reporting of IS Audit assignments

IS Audit products reflect the auditors' overall assessment of the governance mechanism adopted, and the general controls and application controls implemented for the information system.

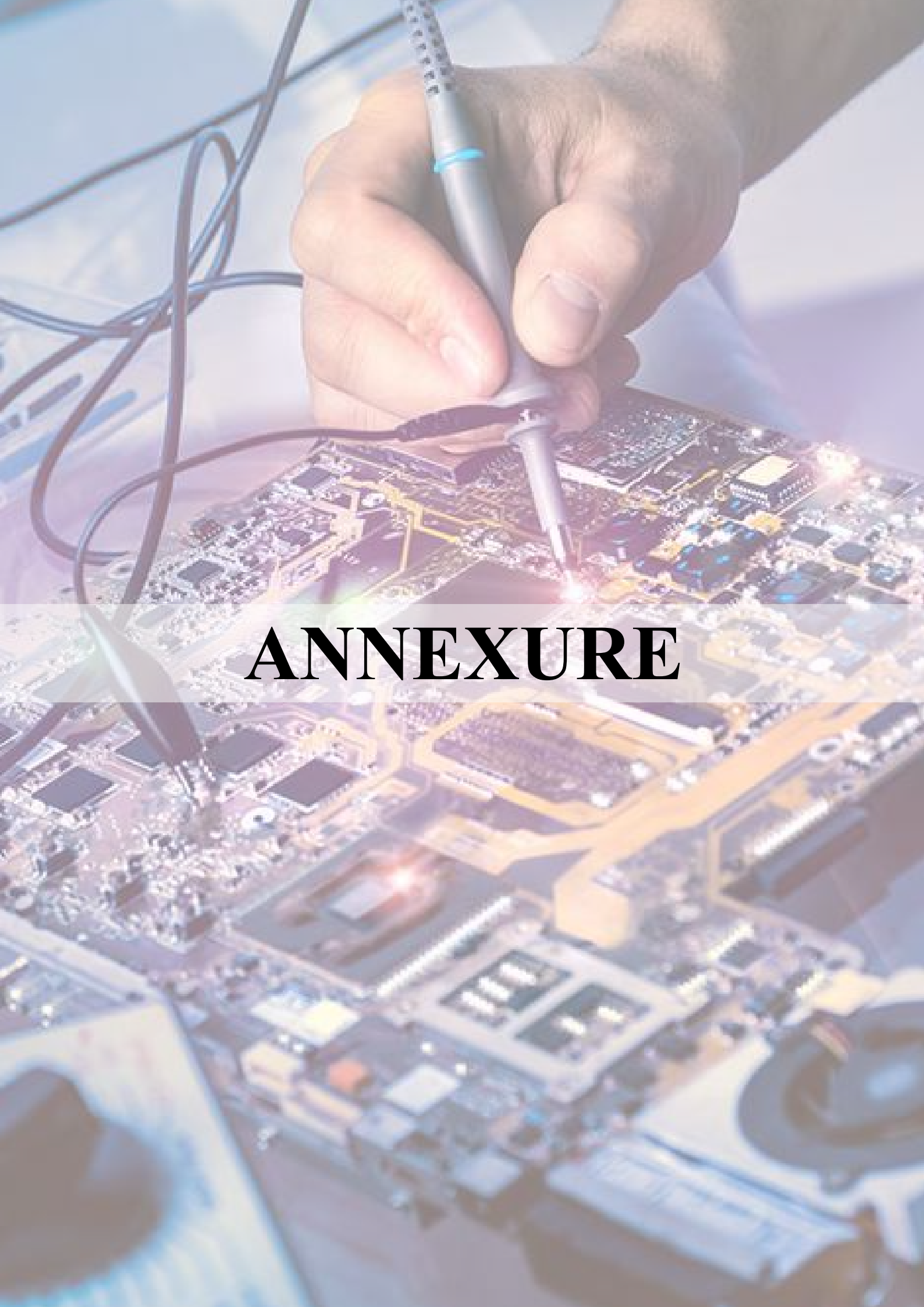
The provisions in the Compliance Audit Guidelines 2016 which are related to Audit Reporting shall be applicable to IS Audit assignments.

The IS Audit product may be processed as either a stand-alone Report or as a Subject Specific Compliance Audit which is part of a longer Compliance or Performance Audit Report.

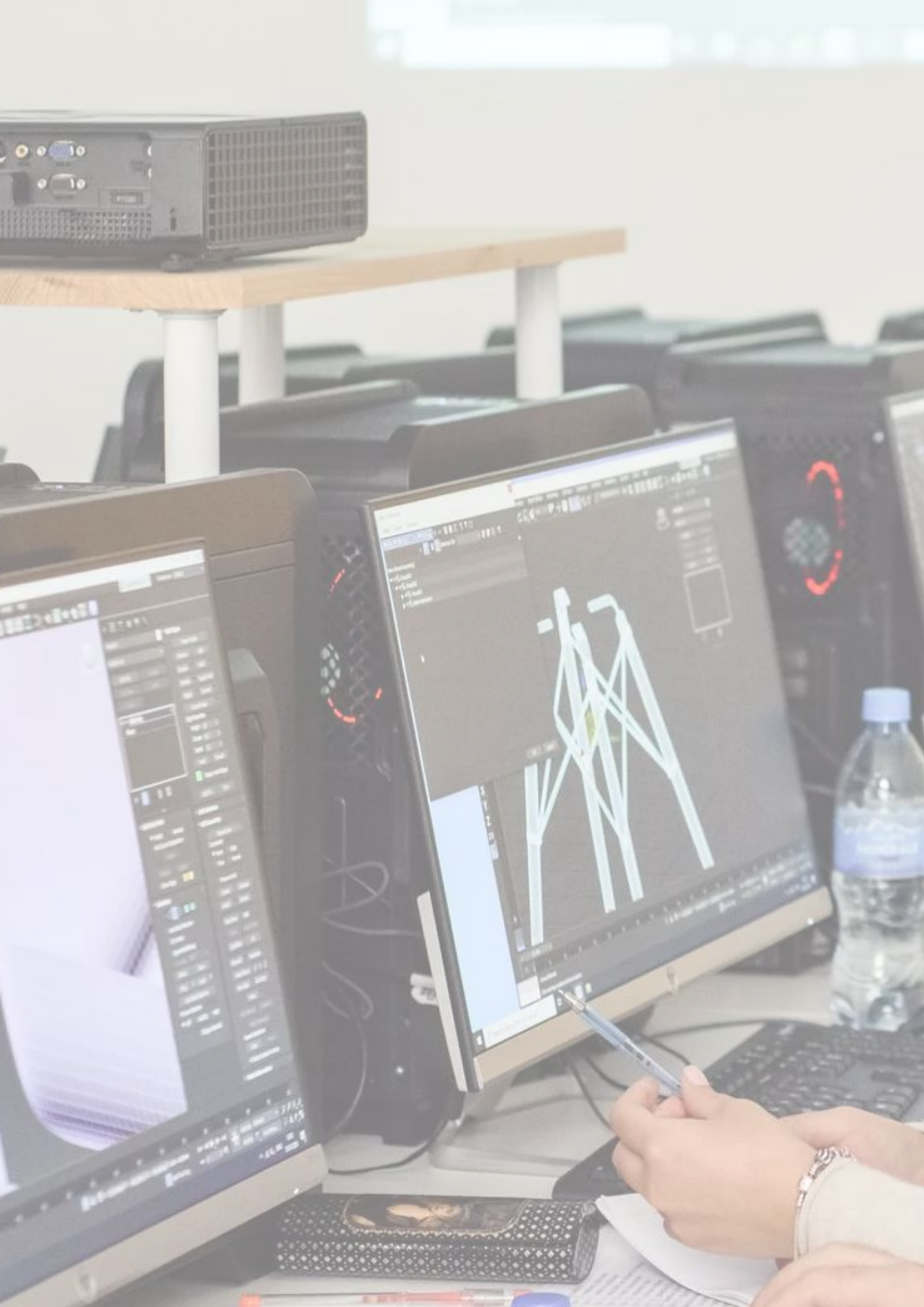
VII. Follow-up of previous IS Audits

The objective of Follow-up Audit is to verify whether recommendations from the previous IS Audit assignments have been implemented by the audited entities.

The provisions in the Compliance Audit Guidelines 2016 which are related to Follow-up Audits shall be applicable to IS Audit assignments.



ANNEXURE



Annexure I- Indicative list of documents for IS Audit

1. Minutes of meetings of Governance Committees
2. Functional Requirements Specification/ User Requirements Specification
3. System Requirements Specification/ Technical Blueprint Document
4. Request for Proposal
5. Technical Bid Evaluation
6. Financial Bid Evaluation
7. Contract/ Agreement/ MoU with software services provider
8. Service Level Agreement
9. List of Invoices presented by software services provider
10. Contract/ Agreement with project management consultant
11. KPIs for monitoring performance of project management consultant
12. List of Invoices presented by project management consultant
13. License Agreements
14. IS Project Scheduled Timelines and Actual Progress Monitoring
15. IS Project Costing, Budgeting and Actual Expenditure Monitoring
16. Hardware and Software Assets Inventory
17. Change Control Notes
18. Unit Test Reports, Product Integration Test Reports, User Acceptance Reports
19. User Training Courses (Scheduled Sessions or Self Learning)
20. Go-Live/ Deployment Communication
21. System Architecture, Data Flow Document, User Manual and other descriptive documents
22. Certification on taking possession of source code and Intellectual Property from software services provider
23. MIS for Incidents Response Management
24. Benefits Realization (if defined) Document
25. Security Audit Reports by STQC
26. Vulnerability Assessment and Penetration Test Reports by CERT-IN empanelled vendors
27. Business Continuity and Disaster Recovery Plan
28. Disaster Recovery Drill Reports

Annexure II- Indicative Checklist of Issues for IS Audit Design Matrix

I. Audit Objective 1: Whether governance mechanism had been adopted to ensure that the information system has been implemented in compliance with the approved functionalities, timelines and costs.

Sub-Objectives

1. Whether Steering Committee/ Implementation Committee/ Technical Committee has been constituted
    i. Whether these Committees have met at prescribed frequency of meetings
    ii. Whether these Committees have documented and discussed key risks to the IS project and have recommended mitigation measures
    iii. Whether the decisions taken by these Committees in their meetings have been followed up in subsequent meetings and actions taken have been reviewed
2. Whether documentation related to the IT project has been maintained for record
    i. Whether user/ functional requirements have been compiled and documented
    ii. Whether Detailed Project Report has been prepared and updated regularly
    iii. Whether contract/ MoU/ Work Orders (including Service Level Agreement) have been issued to the software services provider, with clear definition of work, timelines and deliverables
    iv. Whether processing of payments against invoices raised by the software services provider has been carried out with supporting documentation to assess correctness of amounts payable
    v. Whether the contract with the software services provider includes clauses related to punitive actions for non-performance of obligations and for exit management (transfer of documentation to the audited entity prior to end of contract period and transfer of knowledge for a specified period to any successor software services provider after the end of the contract period).
3. Whether monitoring of progress of implementation against approved timelines and costs has been carried out
    i. Whether task level details have been defined for the IT project, and sequential

dependencies have been identified to determine the Critical Path for the project

ii. Whether analysis has been carried out on the list of functionalities/ Modules not yet implemented (along with reasons)

iii. Whether analysis of time and cost overruns (if any) has been carried out.

4. Whether formal policies have been adopted and/ or documented processes have been followed for major processes

i. Access Management

ii. Change Management

iii. Incident Response Management

iv. Information Security

v. Business Continuity and Disaster Recovery

5. Whether measures have been taken to facilitate adoption of the use of the IT system as intended

i. Whether adequate training has been imparted

ii. Whether User Manual has been published for registered suppliers as well as Departmental users

iii. Whether extent of adoption and use by Departments has been analyzed

iv. Whether there is any continued parallel use of offline work processes (if any) even after implementation of the system (along with reasons).

II. Audit Objective 2: Whether general controls related to the operations of the information system have been implemented, in compliance with executive instructions.

Sub-Objectives

1. Whether compliance with procurement requirements has been achieved.

i. Whether engagement of project management consultant has been carried out in compliance with the applicable Rules and executive instructions.

ii. Whether engagement of the system integrator/ software services provider has been carried out in compliance with the applicable Rules and executive instructions.

iii. Whether hardware and software has been procured in compliance with requirements identified and approved by the competent authority.

iv. Whether engagement of service providers for outsourcing of functions of the information system has been carried out in compliance with the applicable Rules and

executive instructions.

2. Whether compliance with information security requirements has been achieved.
    i. Whether regular Internal Audits of the system have been carried out.
    ii. Whether periodic Security Audits by STQC and Vulnerability Assessments and Penetration Tests by CERT-IN empanelled vendors have been carried out.
    iii. Whether suitable action has been taken as follow-up from the identified issues arising from the Security Audits and VAPTs.
    iv. Whether the system has user logs, application log and Data Base Administrator log for the purpose of maintaining a trail for information security.
3. Whether compliance with Business Continuity and Disaster Recovery requirements has been achieved.
    i. Whether Business Continuity and Disaster Recovery Plan has been documented
    ii. Whether Recovery Point Objective and Recovery Time Objective have been defined.
    iii. Whether Disaster Recovery Drills including restoration of backed up data have been conducted at prescribed intervals.
    iv. Whether RPO and RTO have been achieved in the DR Drills.
    v. Whether suitable action has been taken as follow-up from identified issues arising from the DR Drills.
4. Whether compliance with Access Management requirements has been achieved
    i. Whether there is a documented user registration and de-registration procedure for granting access, including mandatory fields for KYC.
    ii. Whether the access rights given to users is compliant with delegation of powers and extant Rules.
    iii. Whether password policy and Multi Factor Authentication of users is in place for login management.
    iv. Whether a log is maintained to record details of the user who has completed verification of KYC and other details of registration of new users, before they can access the system.
5. Whether compliance with Master Data Management requirements has been achieved
    i. Whether key and sensitive data fields which constitute master data (such as Bank

Account Numbers) have been identified.

ii. Whether there is a documented procedure for addition/ modification and deletion of master data, with specified roles for this purpose.

iii. Whether segregation of duties has been ensured through maker-checker model for modifications to master data.

iv. Whether master data management has been carried out in compliance with the delegation of powers for users.

v. Whether the system maintains a log for changes made to the master data, with usernames and timestamps recorded.

6. Whether compliance with Change Management requirements have been achieved.

   i. Whether there are any pending Change Requests/ Change Control Notes which have not yet been implemented.

   ii. Whether User Acceptance Tests have been conducted before introducing any changes to the production environment.

7. Whether compliance with Incident Response Management requirements have been achieved.

   i. Whether issues reported by Help Desks and as incidents have been categorized by type and analysed.

   ii. Whether there are any major issues identified by Help Desks and/ or incidents reported, which have not yet been acted upon.

   iii. Whether the system experienced any downtime/ outage during the audit period and whether root cause analysis was carried out and mitigation measures have been taken to prevent recurrence.

8. Whether compliance with Maintenance requirements have been achieved

   i. Whether any identified hardware and software procurement/ upgrade requirements have not yet been acted upon.

   ii. Whether inventory of hardware and software assets has been prepared and kept updated.

   iii. Whether any maintenance issues identified and communicated by the software services provider have not yet been acted upon.

9. Whether Consultant Management was compliant with contractual provisions.
    i. Whether KPIs for monitoring the performance of the consultant have been defined.
    ii. Whether payments to the consultant have been made after review of the services delivered and after review of requirement to continue the engagement of consultancy services.

III. Audit Objective 3: Whether business rules have been correctly mapped and application controls have been implemented in the information system, to ensure compliance with executive instructions.

Sub-Objectives (for each Module to be examined as part of the Audit Scope, as well as any integration required with other IT applications)

1. Whether the business rules have been correctly mapped and application controls have been implemented in _____ (Module 1).
    i. Whether Business Rule 1 and associated application controls for Business Rule 1 have been implemented (list for each business rule and associated application controls to be examined under Module 1).
    ii. Business Rule 2…
    iii. Business Rule 3… and so on.
2. Whether the business rules have been correctly mapped and application controls have been implemented in _____ (Module 2).
    i. Whether Business Rule 1 and associated application controls for Business Rule 1 have been implemented (list for each business rule and associated application controls to be examined under Module 1).
    ii. Business Rule 2…
    iii. Business Rule 3… and so on.
3. Module 3…
4. Module 4… and so on.

Annexure III-Examples of Audit Design Matrix under Audit Objective 3

I. Example 1: ADM under Audit Objective 3, for e-Procurement Systems implemented by State Governments

Sub-Objectives

1. Tender Publication: Whether the published tender documents are published in defined formats and accessible to all registered suppliers and system alerts are generated for them, upon publication of the tender documents.

i. Whether new e-tenders have been published with key details (including bid evaluation criteria and provisions of contract to be awarded) for publication, as approved by the competent authority.

ii. Whether provisions in the contract to be awarded after bid evaluation have been mandatorily made part of the e-tender, by requiring the draft contract to be uploaded as a separate document or to be entered as per standard data templates.

iii. Whether the new e-tenders are in the approved format and languages.

iv. Whether email and SMS alerts are generated for all registered suppliers when a new e-tender is published.

v. Whether functionality and application controls are in place to issue clarifications/ modifications to the original e-tender through the system only (and not through offline modes) along with system generated alerts to registered suppliers regarding the modifications.

vi. Whether all the data fields which are mandatory to be entered during bid submission (BOQ, technical bid and financial bid data) have been clearly defined, even if standard e-tender data templates have not been used.

2. **Bid Submission: Whether application controls for submission of bid data and documents have been implemented, to ensure compliance with Rules.**

   i. Whether the system has application controls to enforce the prescribed minimum time for receiving responses from bidders, for each e-tender.

   ii. Whether validation controls have been implemented to ensure workflow for bid submission cannot proceed without entering the mandatory data fields as per the defined and valid data type.

   iii. Whether there are validation controls to ensure that each document uploaded has to be accompanied by data entry to specify the document identifier (for e.g. upload of GST Registration Certificate should be accompanied by data entry of the Certificate Number).

   iv. Whether application controls have been implemented for collection of all the prescribed fees which are required to accompany the bids.

   v. Whether functionality and application controls are in place to call for additional/ missing documents in the bids through the system only (and not through offline modes) along with system generated alerts to registered suppliers regarding the documents sought.

   vi. Whether application controls are in place to prevent submission of bids using free-text data fields and upload of voluminous documents containing potentially irrelevant content.

3. **Bid Submission: Whether the confidentiality and integrity of the data in the draft and frozen bids submitted are maintained.**

   i. Whether application controls for encryption of data at rest and in transit are in place, to ensure confidentiality of the draft bids and frozen bids submitted by the suppliers.

   ii. Whether application controls for opening of the bids only by authorized users and only by using a secure decryption key have been implemented.

   iii. Whether all the bids received against a particular e-tender are decrypted as a single batch process or sequentially with no prescribed time limits in the system.

   iv. Whether Database Administration/ System Administrator/ any other Power User has been granted access rights to view or modify the draft bids and frozen bid data, prior to the formal opening of the bids.

v. Whether a system log maintains a trail of users who attempted to view/ modify the draft and frozen bid data along with timestamps, irrespective of before or after the opening of the bids.

vi. Whether a documented procedure is in place to handle incidents such as inability to decrypt some of the technical or financial bids received in compliance with the Rules and whether the competent authority has reviewed the extent of occurrence of such incidents.

4. Bid Evaluation: Whether the application controls for bid evaluation ensure compliance with the provisions in the GFR for procurement of goods and services.

i. Whether application controls have been implemented for analysis of bidders' registration and data (Email, Mobile Number, IP address, PAN, GSTIN etc.) to generate exception reports on e-tenders having high risk of cartelisation, for review by the competent authority.

ii. Whether application controls have been implemented to ensure that technical evaluation of bids has to be completed through system workflow, even if the Bid Evaluation Committee conducts its proceedings in offline mode and the proceedings are uploaded as a document.

iii. Whether application controls have been implemented to ensure that bids can only be opened by the bid openers designated by the competent authority.

iv. Whether financial bid data remains encrypted and not available for viewing until technical evaluation of bids has been completed.

v. Whether application controls have been implemented to ensure that based on specified data fields for technical bid criteria, the user has to specify qualified/ not qualified status at the end of the technical evaluation.

vi. Whether the results of the evaluation of technical bids and results of qualified/ not qualified are communicated by the system to all the participating bidders, before financial bids are evaluated.

vii. Whether the provision in the Rules (if any) for opportunity to appeal against the decision of the technical bid evaluation has been mapped into the system as a mandatory workflow requirement.

viii. Whether application controls have been implemented to ensure that financial evaluation of bids has to be completed through system workflow, even if the Bid Evaluation Committee conducts its proceedings in offline mode.

ix. Whether application controls have been implemented to ensure that based on specified data fields for financial bid criteria, the system computes L1, L2 etc., and is not left to the users to determine.

x. Whether the results of the evaluation of financial bids (L1, L2 etc. computed by the system along with decision made by the financial bid evaluation committee) are communicated by the system to all the participating bidders, before award of contract.

xi. Whether the provision in the Rules (if any) for opportunity to appeal against the decision of the financial bid evaluation has been mapped into the system as a mandatory workflow requirement.

5. Award of Contract: Whether application controls have been implemented to ensure that award of contract has to be completed through system workflow.

i. Whether generation of Award of Contract on manual basis has been dispensed with and executive instructions have been issued for mandatory generation of Award of Contract through the system workflow.

ii. Whether application controls have been implemented for automation of refund of EMD and other dues to unsuccessful bidders.

6. Generation of Exception Reports: Whether the system generates exception Reports for review by senior Officers

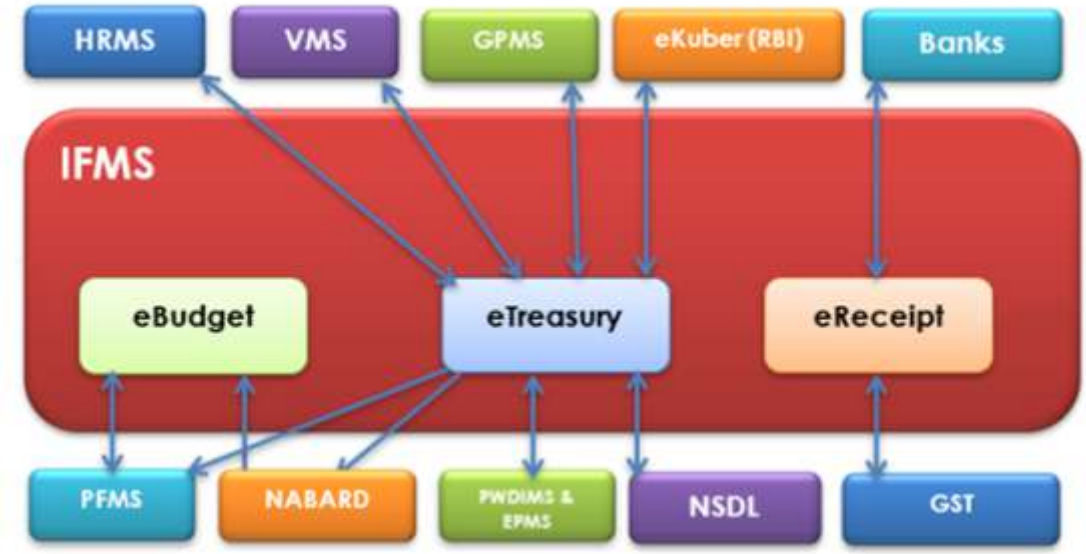
i. Whether application controls have been implemented for generation of exception reports for amounts collected as various fees but not yet refunded to registered suppliers, with communication of system generated alerts on the status of pending refunds (with age analysis) to the competent authority by email/ SMS.

ii. Whether application controls have been implemented for generation of exception reports for e-tenders against which bid processing has not been completed within prescribed timelines, with communication of system generated alerts on the status of pending e-tenders (with age analysis) to the competent authority by email/ SMS.

iii. Whether application controls have been implemented for black-listing of suppliers for prescribed periods and for prevention of their participation in bidding using the same identification details (ID, PAN, GSTIN etc.)

iv. Whether application controls have been implemented for analysis of e-tenders to generate exception reports on e-tenders having high risk of splitting of tenders, for review by the competent authority.

I. Example 2: ADM under Audit Objective 3, for Integrated Financial Management Systems implemented by State Governments



Sub-Objectives

1. Whether the business rules have been correctly mapped and application controls have been implemented for Budget Preparation, Budget Review and Budget Distribution.

i. Whether budget estimates are prepared and submitted by all Departments on IFMS, with the required data fields (such as Department Name, DDO Code, Head of Account, Scheme Code, Amount, Justification/ Remarks).

ii. Whether budget estimates of all Departments are reviewed by Finance/ Planning Department on IFMS, with inclusion/ exclusion of line items and increase/ decrease of amount in each line item recorded.

iii. Whether there is any manual intervention necessary for loading the opening budget allotment for Departments, after approval by the Legislative Assembly for a new financial year (to check whether it is manually or through file transfer or through an interface with any other application used for the budget review and approval processes).

iv. Whether there is mapping in place to prevent loading of allotment of budget estimates under different Heads of Account to unrelated Departments (for example, budget allotment under MH 2202-01-111 Sarva Siksha Abhiyan should not be erroneously permitted to be loaded to Industries Department).

v. Whether re-appropriations are processed on IFMS in compliance with business rules (as per delegation of powers and only across the permitted Heads of Account).

vi. Whether surrenders are processed on IFMS in compliance with business rules (surrender amount cannot exceed available budget amount).

vii. Whether there are any cases of excess expenditure over budget (along with reasons).

viii. Whether budget allotment by CCO to DDO can be made in excess of the budget available under a particular Head of Account.

2. Whether the business rules have been correctly mapped and application controls have been implemented for generation of Sanction Orders.

i. Whether IFMS has provision for generation of all the types of Sanction Orders specified in the Treasury Rules (please list if any are missing) with all the key data fields to be entered for each type of Sanction Order.

ii. Whether Sanction Order can be generated by a user only as per delegation of powers (based on sanctioned amount and type of expenditure).

iii. Whether Sanction Order has to mandatorily be generated through IFMS, even if initially a manual Sanction Order has been issued (by entering the details from the manual Sanction Order into IFMS to generate a unique Sanction Order Number, to ensure completeness of Sanction Orders in a financial year).

iv. Whether mapping is in place to ensure that Sanction Order types can only be generated under the permissible Heads of Account for those types of Sanction Orders (for example, Sanction Order of type Grants in Aid should not be permitted under Capital Section Heads of Account, as it would violate Indian Government Accounting Standard 2).

v. Whether Sanction Order can be generated under a Head of Account under which budget allotment for that user is not available?

vi. Whether Sanction Order can be generated under a Head of Account where sanctioned amount exceeds available budget amount (i.e. the system should keep track of available budget amount for a new Sanction Order, after deducting previous sanctioned amounts under that Head of Account).

vii. Whether Sanction Order can be cancelled even after a Bill has been passed using that Sanction Order as the underlying basis for drawal of funds.

viii. Whether IFMS has provision for recording terms and conditions for each type of Sanction Order (such as date for submission of UCs, names and codes of DDO(s) authorized to draw the sanctioned amount(s), specific conditions from Scheme guidelines/ conditional grants in aid).

ix. Whether payment beneficiary for the funds to be drawn can be specified in Sanction Order, without previously entering their details into the master data for IFMS, through the defined process for master data management.

x. Whether bank account details of payment beneficiary can be modified in the Sanction Order, instead of modifying the same in the master data for IFMS through the defined process for master data management.

3. Whether the business rules have been correctly mapped and application controls have been implemented for generation and passing of Bills by DDOs.

i. Whether IFMS has provision for generation of all the types of Bills specified in the Treasury Rules (please list if any are missing) with all the key data fields to be entered for each type of Bill.

ii. Whether IFMS has provision for mapping and restricting the permissible combinations of Sanction Order types and Bill types in the system (for example, Contingent Expenditure Bill cannot be passed by linking to a Grants in Aid Sanction Order).

iii. Whether linking to an underlying and valid Sanction Order in IFMS is mandatory, for generation and passing of Bills

i. Whether Bills can be generated and passed without linking to a Sanction Order Number in the system.

ii. Whether Bills can be generated and passed by linking to impermissible type of Sanction Order for that Bill type.

iii. Whether Bills can be generated and passed by a DDO by linking to a Sanction Order which does not specify that DDO as the designated Drawing and Disbursing Officer.

iv. Whether Bills can be passed by linking to Sanction Orders from previous years.

v. Whether Bills can be passed by linking to a Sanction Order against which Bills have been previously drawn for the entire sanctioned amount.

iv. Whether Bills can be generated and passed with Bill amount exceeding the available balance of the sanctioned amount in the linked Sanction Order (i.e. the system should keep track of available sanctioned amount for a new Bill, after deducting previous Bills passed which were linked to that Sanction Order).

v. Whether key data fields from the linked Sanction Order are auto-populated by IFMS at the time of generation of Bills (such as Head of Account and payment beneficiary, if any).

vi. Whether the master data for payment beneficiaries has been reviewed to ensure that there is a clear trail of details of Departmental users who have verified the name of payment beneficiary, bank account number, IFSC with an uploaded copy of the bank pass book.

vii. Whether the master data for payment beneficiaries has been reviewed to ensure that impermissible payment beneficiaries are not included in the master data (such as Bank Account Number of the Department/ DDO itself, to facilitate parking of funds outside Government Account).

viii. Whether payment beneficiaries can be specified in Bills, without previously entering their details into the master data through the defined process for master data management (payment beneficiaries can only be selected from the list from master data).

ix. Whether bank account details of payment beneficiary can be modified in the Bill, instead of modifying the same in the master data for IFMS through the defined process for master data management.

x. Whether there are any specific Bill types (for Scheme expenditure or Grants in Aid) which account for significant share of overall expenditure of the State Government, and whether these Bill types have all the required data field validation and processing controls corresponding to the checks to be exercised by the DDO and DTO as per the Treasury Code.

xi. Whether Bill types for Pay and Allowances for serving State Government employees and Pension for retired employees have the required validation and processing controls in place.

4. Whether functionality and application controls for Utilization Certificates, adjustment of Abstract Contingent Bills and Personal Deposit Accounts have been implemented.

i. Whether the UC Module has been implemented in IFMS.

i. If not implemented, whether the fact has been reported to the governance Committees along with reasons for the same.

ii. If implemented, whether the application controls for submission of UCs on time and Sanction Order-wise have been implemented (UCs should not be submitted Scheme-wise or Head of Account-wise, they have be submitted Sanction Order-wise by each entity responsible for end utilization of funds).

iii. Whether the system is able to generate MIS Reports on correct status of outstanding UCs and prevent further release of Grants in Aid in such a scenario, in compliance with the extant Rules.

ii. Whether functionality for submission of Detailed Contingent Bills for adjustment of Abstract Contingent Bills previously drawn has been implemented in IFMS.

i. If not implemented, whether the fact has been reported to the governance Committees along with reasons for the same.

ii. If implemented, whether the application controls for submission of DC Bills against each AC Bill has been implemented (DC Bills should not be submitted Scheme-wise or Head of Account-wise, they have be submitted AC Bill-wise by each entity responsible for end utilization of funds).

iii. Whether the system is able to generate MIS Reports on correct status of unadjusted AC Bills and prevent further drawal of AC Bills in such a scenario, in compliance with the extant Rules.

iii. Whether functionality for accounting receipts into and payments out of Personal Deposit Accounts has been implemented in IFMS.

i. If not implemented, whether the fact has been reported to the governance Committees along with reasons for the same.

ii. If implemented, whether there are application controls in place to ensure compliance with Rule provisions regarding refund of inoperative PD Account balances.

iii. Whether the system is able to track the status of PD Account balances and generate timely alerts on inoperative PD Accounts whose balances are to be refunded at the end of the financial year.

5. Whether the business rules have been correctly mapped and application controls have been implemented in the Centralized Treasury Module of IFMS.

i. Whether there is any manual processing of Bills by Treasuries due to non-implementation of certain Bill types in IFMS.

ii. Whether linking to an underlying and valid Sanction Order in IFMS is mandatory, for passing of Bills by Treasuries.

i. Whether Bills can be passed and payment made without linking to a Sanction Order Number in the system.

ii. Whether Bills can be passed and payment made by linking to impermissible type of Sanction Order for that Bill type.

iii. Whether DDO-DTO mapping has been implemented correctly, to ensure that DTOs only process Bills related to DDOs in their jurisdiction.

iv. Whether Bills can be passed by linking to Sanction Orders from previous years.

v. Whether Bills can be passed by linking to a Sanction Order against which Bills have been previously drawn for the entire sanctioned amount.

iii. Whether Bills can be passed and payment made with Bill amount exceeding the available balance of the sanctioned amount in the linked Sanction Order (i.e. the system should keep track of available sanctioned amount for a new Bill, after deducting previous Bills passed which were linked to that Sanction Order).

iv. Whether the master data for payment beneficiaries has been reviewed to ensure that impermissible payment beneficiaries are not included in the master data (such as Bank Account Number of the Department/ DDO itself, to facilitate parking of funds outside Government Account).

v. Whether payment beneficiaries can be specified in Bills, without previously entering their details into the master data through the defined process for master data management (payment beneficiaries can only be selected from the list from master data).

vi. Whether bank account details of payment beneficiary can be modified in the Bill, instead of modifying the same in the master data for IFMS through the defined process for master data management.

6. Whether integration of IFMS with the Works Accounting System and HRMS in the State Government has been implemented.

i. Whether master data for contractors is shared between Works Accounting System and IFMS for payment of Works Bills.

ii. BUSINESS RULE 2/ APPLICATION CONTROLS FOR INTEGRATION WITH WORKS ACCOUNTING SYSTEM.

iii. And so on…

iv. Whether master data for contractors is shared between HRMS and IFMS for payment of salaries and pensions.

v. BUSINESS RULE 2/ APPLICATION CONTROLS FOR INTEGRATION WITH HRMS.

vi. And so on…

Comptroller and
Auditor General of India
http://www.cag.gov.in