OFFICE OF THE COMPTROLLER AND AUDITOR GENRAL OF INDIA,
NEW DELHI
(Professional Practices Group)

No. 94/17-PPG/2019

Date: 06.08.2020

STANDING ORDER

Subject: Auditing in an IT Environment

The enclosed Standing Order on Auditing in an Information Technology (IT) environment is applicable with immediate effect. This Standing Order replaces existing Chapter 22 of MSO (Audit) 2002 and also the Manual of Information Technology Audit issued in 2006.

Vidhu Sood

(Vidhu Sood)
Principal Director (PPG)

All DAIs and ADAIs
All DGs/PDs at HQ
All concerned State Audit offices
PD and Secretary to C&AG

Standing Order on “Auditing in an Information Technology (IT) Environment”

1 Auditing in an Information Technology (IT) Environment

1.1 Introduction

Audits, whether financial, compliance or performance audits, are conducted increasingly in an Information Technology (IT) environment today. Governments and other public sector entities have continuously adopted IT, in order to enhance efficiency and effectiveness in their functioning and delivery of various public services. IT has made it possible to capture, store, process, retrieve and deliver information electronically, and the delivery mode of public services is, in many cases, rapidly transitioning from physical to electronic.

This transition to computerised information systems and electronic processing by audited entities in the public sector has triggered a significant change in the environment in which auditors work. There is also a need to ensure that internal IT controls to maintain confidentiality, integrity, non-repudiability, and availability of data, and the systems that process, maintain and report this data have been adopted by public sector entities. For instance, the highly repetitive nature of many computer applications implies that even small errors remaining undetected may lead to large losses. An error in the calculation of income tax to be deducted from employees’ remuneration will not recur in each case in a manual system, but once this error is introduced in a computerised system, it will affect each case. The financial implications of such recurring or repetitive errors could, in the final analysis, be very substantial. Therefore, it becomes imperative for auditors to gain assurance through an audit of such IT systems[1] and utilise the information available on such systems for deriving appropriate audit conclusions.

1.2 Audit of IT Systems and IT-assisted audits

Audits in an IT environment cover either or both of the following:

(i) Audit of IT systems or ‘IT Audits’;

(ii) Financial, compliance or performance audits (or combined audits) using various IT tools for supporting the achievement of the audit objectives – also referred to as “IT-assisted audits”.

The broad principles of audit and requirement of access to data, information and documents as contained in the Regulations shall apply to auditing in an IT environment.

[1] For the purpose of audit, an IT system would include objects like mobile apps and even APIs (Application Programming Interfaces).

1.2.1 Audit of IT systems

Audit of IT systems is the process of deriving assurance on whether the development[2], implementation and maintenance of IT systems meets organizational goals, safeguards information assets and maintains data integrity. In other words, it is an examination of the implementation of IT systems and IT controls to ensure that the systems meet the organisation's business needs without compromising security, privacy, cost, and other critical business elements. It crucially also determines areas such as whether, and to what extent, the data can be relied upon as a single source of truth, for purposes of audit.

2 Frameworks and Approaches to IT Governance & Management

Note: In the absence of overarching frameworks prescribed by Government of India (GoI), this section is based largely on the CoBIT (Control Objectives for Information & Related Technology) framework version 4.1[3] and CoBIT version 5, prepared by ISACA (Information System Audit & Control Association), as well as ISO/ IEC 38500:2015. References are also made to the WGITA-IDI Handbook on IT Audit for SAIs (October 2013). With regard to information security management, references are also made to ISO/ IEC 27000 series: 2013.

2.1 IT Governance

IT Governance is the overall framework that guides IT operations in an organisation to ensure that it meets the needs of the enterprise today and that it incorporates plans for future needs and growth. It is an integral part of the enterprise governance, and comprises the organisational leadership, institutional structures and processes, and other mechanisms (reporting & feedback, enforcement, resources etc.) that ensure that IT systems sustain organisational goals and strategy while balancing risks and effectively managing resources. Thus, value creation through IT means **realising benefits** at an **optimal resource cost** while **optimising risk**.

ISO/ IEC 38500: 2013 sets out six principles for good governance of IT:

Responsibility	Individuals and groups understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
Strategy	The organization's business strategy takes into account the current and future capabilities of IT; the plans for use of IT satisfy the current and on-going needs of the organization's business strategy.
Acquisition	IT acquisitions are made for valid reasons, on the basis of appropriate and on-going analysis, with clear and transparent decision-making.

[2] This includes procurement, as the development, implementation and maintenance could be done through in-house or outsourced resources.

[3] Prepared by IT Governance Institute (ITGI), an arm of ISACA.

	There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
Performance	IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
Conformance	The use of IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
Human Behaviour	IT policies, practices and decisions demonstrate respect for human behaviour, including the current and evolving needs of all the 'people in the process'.

Further, ISO/ IEC 38500 recommends a three task model: (a) **Evaluate** (the current and future use of IT); (b) **Direct** preparation and implementation of strategies and policies to ensure that use of IT meets business objectives; and (c) **Monitor** conformance to policies, and performance against strategies.

2.2 Information Criteria

To satisfy business objectives, information needs to conform to certain control criteria or attributes:

Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Non-repudiability is the assurance that a party cannot later deny originating data and is based on provision of proof of the integrity and origin of the data that can be verified by a third party.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e. externally imposed business criteria as well as internal policies.

Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities[4].

2.3 IT Resources

IT resources or assets[5] can be categorized into:

- IT Applications –automated systems, as well as the associated manual procedures.
- Information – data (in all forms) input, processed and output by the IT systems
- Infrastructure –technology and facilities (hardware, system software, networking, environment etc.) that enables the processing of the IT applications
- People

2.4 Controls

Controls are the policies, procedures, practices and organisational structures designed to provide reasonable assurance that organisational/ business objectives will be achieved and undesired events will be prevented or detected and corrected. Controls may be either manual or programmed/ automated. IT Control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

Adequacy of controls (i.e. whether they are properly designed) and **effectiveness** of controls (i.e. whether they are functioning as planned) are both important. Such controls would also be commensurate with the risk assessed so as to reduce the impact of such risks to acceptable levels.

2.4.1 General and Application Controls

General Controls are controls which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. Application Controls are specific controls unique to each computerised application.

Examples of general controls include:

- Development and implementation of an IT Strategy and an IT Security Policy, and setting up of an IT Steering Committee
- Organisation of IT Staff to separate conflicting duties
- Planning for disaster prevention and recovery
- Environment controls

[4] In many situations, reliability would also include the aspect of 'comparability' of data, where the information or data complies with accepted standards and guidelines, facilitating fair comparison with corresponding information in respect of other peer organizations.

[5] Includes in-house and outsourced resources

- Physical access controls over the data centre and logical access controls over infrastructure, applications and data
- System development life cycle controls
- Change management controls
- Computer operations controls

Application controls are usually categorized into:

- Controls over input (data origination and data entry);
- Controls over transaction processing;
- Controls over outputs (distribution of results)
- Controls over application security.

Examples of application controls include system edit checks of the format of entered data to help prevent possible invalid inputs, application enforced controls that prevent users from performing transactions that are not part of their normal duties, and the creation of detailed reports and transaction control totals that can be balanced by various units to the source data to ensure that all transactions have been posted completely and accurately.

Presence of controls in an IT system is significant from the audit point of view because the system may allow, in their absence, duplication of inputs or processing, or conceal or make invisible/ untraceable some of the processes. Controls also provide safeguards against data loss attributable to damage to or corruption of files, manipulation of data, power failures or fluctuations, viruses, computer abuses, etc. Absence of audit trails would also make it difficult to ensure the efficient and effective functioning of a computerised system for an auditor. Besides, in organisations where IT systems are operated, on contract, by outside agencies that employ their own standards and controls, absence of controls could also make the system vulnerable to remote and unauthorised access.

2.4.2 Manual and Programmed/ Automated Controls and Business Process Re-engineering

The exact design of application controls depends on the approach adopted for design of the IT system. If the IT solution is an end-to-end automated solution without significant offline manual documentation/ approvals, then the majority of application controls would be automated.

The aspect of Business Process Re-engineering (BPR) may also need to be considered, specifically in the context of Government entities in India moving from a manual/ paper-based environment to an automated environment. In order to achieve effectiveness through an IT system, it may be necessary to not just replicate manual processes but conduct a review of the existing manual processes and consider which manual processes are either not necessary or need to be amended in an automated environment. Such a BPR exercise helps to minimize automation of ineffective/ inefficient paper-based processes.

For example,

- Daily/ periodic totalling of manual registers may not be necessary in an automated environment, where such summarization is automated.
- Compilation and submission of periodic “returns”, summarizing the activities during the specified period, may not be necessary, if there is a real-time dashboard which provides such information.
- Reconciliation or “squaring off” of transactions for internal/ external consistency may be fully automated, doing away with the need for submission of reconciliation “returns”.

2.5 Requirements of IT security management systems

Note: These are drawn largely from ISO/ IEC 27000 series

An Information Security Management System (ISMS) consists of the policies, procedures, guidelines and associated resources and activities, collectively managed by an organization in the pursuit of protecting its information assets. As per ISO/ IEC 27001, the reference control objectives for an ISMS are categorised as follows:

- Information security policies
- Organization of information security – covering internal organization, use of mobile devices and security of teleworking
- Human resources security – prior to employment, during employment, and post-employment/ termination/ change of employment
- Asset management – covering identification of assets and defining protection responsibilities; information classification; media handling
- Asset control – covering the business requirements of access control; user access management; user responsibilities; system and application access control
- Cryptographic controls[6]
- Physical and environmental security
- Operations security – covering operational procedures and responsibilities; protection from malware; backup; logging and monitoring; control of operational software; technical vulnerability management; IS audit considerations (minimising impact on operational systems)

[6] A cryptographic key is a string of data that is used to lock (typically, by altering data so that it appears random) or unlock cryptographic functions, including authentication, authorization and encryption. Cryptographic controls are policies and procedures that are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

- Communications security – covering network security management; and information transfer
- Systems acquisition, development and maintenance – covering security requirements of information systems; security in development and support processes; protection of test data
- Supplier relationships – covering information security in relationships with suppliers to ensure protection of the organization's assets that is accessible by such suppliers; supplier service delivery management to maintain an agreed level of information security and service delivery
- Information security incident management
- Information security aspects of business continuity management
- Compliance with legal and contractual requirements and information security reviews

2.6 End-to-end processes for management of enterprise IT

End-to-end processes for IT Management[7] cover planning, organizing, acquisition, implementation, delivery, support, monitoring and evaluation of information systems and services. These could be categorized into the following IT domains:

- **Plan & Organize** – This covers aspects such as the IT strategic plan; architecture and technological direction; IT processes, organisation and relationships; IT investment; IT human resources; quality management; risk assessment and management; project management etc.
- **Acquire & Implement** – This covers aspects such as identifying IT solutions (including requirements specification, feasibility studies and decision); procuring IT resources; acquiring and maintaining IT applications and technology infrastructure; managing changes; testing and roll-out etc.
- **Deliver & Support** – This covers aspects such as managing operations, performance & capacity; managing service levels and third party services; ensuring security; managing service desk, incidents and problem resolution; managing configuration; manage data etc.
- **Monitor & Evaluate** – This covers aspects such as monitoring and evaluating IT performance & internal controls; ensuring compliance with external requirements

[7] CoBIT Version 5.0 makes a clear distinction between IT Governance (the responsibility of the Board of Directors or equivalent) and IT Management (the responsibility of the executive management under the CEO or equivalent).

3 Audit of IT Systems – Principles and Considerations

Important principles and considerations with regard to audit of IT Systems at different stages of the IT Systems Lifecycle[8] are as follows:

3.1 Audit of Planning and Organization for IT

Aspects to be covered could include:

- **Defining a Strategic IT Plan**, which represents the mutual alignment between IT strategy and business strategic objectives. It should consider the current and future needs of the business, the requirement of resources, the current capacity of IT to deliver services, as well as the existing IT infrastructure and architecture, investments, delivery model, resourcing (including staffing) and then lay out an IT Strategy to support the business objectives.

- **Defining the Information Architecture**, by focusing on the establishment of an enterprise data model that incorporates a data classification scheme to ensure the integrity and consistency of all data.

- **Determining the Technological Direction**, by defining and implementing a technological infrastructure plan, architecture and standards that recognise and leverage technology opportunities.

- **Defining the IT organisation, relationships, policies and processes,** by establishing transparent, flexible and responsive IT organisational structures (e.g. IT Steering Committee, CIO) and defining and implementing IT policies/ processes (e.g. HR, documentation, outsourcing, IT Security) with owners, roles and responsibilities.

- **Managing the IT Investment,** through effective and efficient IT investment decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions with appropriate frameworks (e.g. Cost-benefit analysis among competing solutions for selecting the optimum solution).

- **Communicating Management Aims & Direction to personnel,** by providing accurate, understandable and approved policies, procedures, guidelines etc. and enforcing them (i.e. monitoring and ensuring compliance).

- **Managing IT Human Resources**, through hiring and training personnel, assigning roles corresponding with skills and creating job descriptions, establishing performance review processes, managing dependency on individuals, and managing job change and termination.

[8] The four stages adopted here – Plan & Organize; Acquire & Implement; Deliver & Support; and Monitor & Evaluate correspond to the four domains used in CoBIT Version 4.1 framework.

- **Managing Quality**, by establishing and maintaining a Quality Management System, ongoing performance monitoring against pre-determined objectives, and implementing a programme for continuous improvement of IT services.
- **Assessing and Managing IT Risks,** by developing and implementing a risk management framework (on an ongoing, continuous basis), which covers risk identification and assessment and risk response (avoidance, reduction, sharing or acceptance) and acceptance of residual risk *(this is usually covered as part of audit of IT security).*
- **Managing IT Projects,** by establishing and implementing a programme and project management framework for IT Projects which enables stakeholder participation/ monitoring of project risks and progress.

Typical risks for the audited entity could include:

- Ineffective, inefficient or user-unfriendly IT systems
- Project failures
- Direction-less IT function not serving the business needs
- Business growth constrained by IT
- Ineffective resource management
- Inadequate decision making due to poor reporting structures
- Third party (vendor) dependency
- Lack of transparency and accountability
- Non-compliance with legal and regulatory requirements
- Exposure to information security risks

In practice, audit of planning and organization for IT is generally not taken up independently, but together with audit of acquisition of a new IT solution or the delivery and support of an existing IT solution.

3.2 Audit of Acquisition and Implementation of IT Systems

Aspects to be covered could include:

- **Identifying automated solutions,** by defining, finalizing (and maintaining) business functional and technical requirements; developing a feasibility study (and alternative courses of action) and finalizing feasibility study reports.
- **Acquiring and maintaining IT applications,** by translating business requirements into a high-level design specification for software acquisition; adhering to development standards for all modifications; and separating development, testing and operational activities.

- The acquisition and maintenance of an IT solution may be done through an in-house team (or through a Government provider like NIC) or through a formal tendering and contracting project from an external service provider (using the business requirements and the high level-design specification). Irrespective of the mode of development/ acquisition and maintenance, the overall audit objective remains the same – ascertaining that procedures are adequate to ensure the development and implementation of a well-documented IT system incorporating adequate controls and meeting the user requirements in an efficient manner.

- The IT solution could be based on Commercial Off the Shelf (COTS) software or a 'bespoke' developed or a combination thereof. The underlying product(s) (comprising the "technology stack") used for the IT solution could be either "open source" (i.e. where the source code is freely available to users") or proprietary. Further, the IT solution could be based on "open standards"[9] or following an "open architecture"[10]

- Also, the application development could follow the waterfall model (which is a linear, sequential approach) or an Agile / Rapid Application Development (RAD) methodology (which is an iterative approach) – or a hybrid approach.

- Quality assurance and testing, which is to be clearly segregated from development, is intended to ensure that the developed/ acquired solution meets the business requirements, meets the acceptance criteria, and has undergone testing with the user and stakeholder involvement.

- Configuration management ensures that the integrity of documents, software and other descriptive or support materials that are part of the system is maintained; changes to these products are managed, and baselines are established so that reverting back to the known and tested version, when needed, is feasible. Configuration management is generally implemented through establishing a repository of configuration items and maintaining a baseline for configuration items; establishing configuration procedures for managing and logging all changes to the configuration repository; periodically reviewing configuration data verify and confirming integrity of the current and historical configuration. (Note: configuration management is also covered as part of "delivery & support" of IT systems).

- Data transfer and migration from legacy systems or paper-based records/ files is an important aspect for audit examination. Adoption of inappropriate or inadequate data transfer procedures may result in the relevant records being transferred inaccurately and incompletely from an existing system to a new one. Further, under-estimation of the effort and resources required for data transfer and migration should be avoided;

[9] i.e. compliance to a set of accepted standards, which ensure enhanced integration and inter-operability, minimises vendor lock-in and is easier to migrate.

[10] i.e. following a layered, hierarchical structure, where the functionality and access of each layer can be controlled; this enables each layer to be implemented without affecting other layers and makes adding, upgrading and swapping components easier.

there should also be clarity in terms of responsibilities for data transfer and migration between the third party vendor/ service provider, if any, and the audited entity.

- **Acquiring and maintaining technology infrastructure**, by producing a technological infrastructure acquisition plan, implement controls for infrastructure resource protection and availability, and planning infrastructure maintenance.
- **Providing effective user and operation manuals and training materials** for knowledge transfer for successful system operation and use.
- **Procuring IT resources,** by defining / applying procurement standards and procedures, obtaining professional legal and contractual advice and procuring hardware, software and services in line with defined procedures.
- **Managing changes,** by defining change procedures (including emergency changes); assessing, prioritising, authorising and documenting changes; and tracking status and reporting on changes.
- **Installing and testing solutions and changes,** by establishing a testing methodology, undertaking release planning, evaluating and approving test results (by business management) and performing post-implementation reviews.

Typical risks for the audited entity, especially for external development, could include:

- Lack of adequate involvement of users in the specification of requirements
- Lack of effective management of the vendor, getting periodic reports of status on costs, schedule and scope (as per key milestones specified in the contract) and corrective action thereon
- Lack of effective quality assurance and testing;
- Lack of training or ineffective training.

3.3 Audit of Delivery & Support of IT Systems

Aspects to be covered could include:

- **Defining and managing service levels,** by identifying service requirements and agreeing on service levels, and monitoring the achievement of service levels.
- **Managing third-party services,** by identifying supplier services and supplier relationship management, identifying and mitigating supplier risk, and monitoring and measuring supplier performance (Note: this is covered in detail under Audit of IT Outsourcing).
- **Managing performance and capacity,** by planning and providing system capacity and availability; monitoring and reporting system performance; and modelling and forecasting system performance.

- **Ensure continuous service,** (also referred to as Disaster Recovery Planning (DRP)/ Business Continuity Planning (BCP)[11]) by
  - ❖ Developing a framework for IT continuity to support enterprise-wide business continuity management;
  - ❖ Developing IT continuity plans, based on risk understanding of potential business impacts (Business Impact Assessment and Risk Management), to reduce the impact of a major disruption;
  - ❖ Establish necessary preventive controls, including environment controls; focus attention on critical IT resources and establish priorities in recovery time; consider resilience, response and recovery requirements for different tiers.
  - ❖ Ensuring that the IT Continuity Plan is kept up-to-date continuously to reflect actual business requirements;
  - ❖ Establishing a business continuity management team; Defining an appropriate distribution strategy for the IT Continuity Plan (accessibility under all disaster scenarios); Ensuring security through BCP/ DRP implementation.
  - ❖ Testing the IT Continuity Plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant; provide all concerned parties with IT Continuity Plan training.
  - ❖ Ensuring offsite backup storage for all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans; alternate site arrangements
  - ❖ Embedding information security continuity in the organization's business and IT continuity Plans.
  - ❖ Planning the actions to be taken for the period when IT is recovering and resuming services.
  - ❖ Managing and monitoring back-up and disaster recovery for outsourced services.
- **Ensuring Systems Security**, by defining and implementing IT security policies, plans and procedures, identity and user access management, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents (described in greater depth in Audit of IT Security).
- **Education and training of users,** with a clear understanding of IT training needs, execution of an effective training strategy and measurement of results.

[11] E.g. a distinction is often drawn between Business Continuity Planning – which is the process for planning and testing the recovery of business processes after disruption, and Disaster Recovery Planning (or IT Continuity Planning), which is the process of planning and testing for recovery of IT systems after a disaster.

- **Configuration management** *(Note: Configuration management is covered under the Acquisition and Implementation domain)*;
- **Managing problems,** by implementing processes for recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems;
- **Managing service desks and incidents,** by creating a service deck function with quick response, defining clear escalation criteria and procedures, and reporting on resolution and trend analysis; (*Note: information security incident management is covered under Audit of IT Security*)
- **Managing data**, by backing up data and testing restoration; managing onsite and offsite storage of data; and securely disposing of data and equipment (*Note: this is usually covered under Audit of IT Security).*
- **Managing the physical environment,** by providing and maintaining a suitable physical environment to protect IT assets from physical access, damage or theft *(Note: this is usually covered under Audit of IT Security).*
- **Managing IT operations,** by defining, implementing and maintaining procedures for IT operations; organising the efficient scheduling of jobs; defining and implementing procedures to maintain IT infrastructure and events *(Note: audit of IT operations management usually also covers service level management; and management of third party/ outsourced service providers).*

3.4 Audit of Monitoring and Evaluation for IT

This could cover aspects such as:

- **Monitoring and evaluating IT performance**, by monitoring and reporting process metrics and identifying and implementing performance improvement actions;
- **Monitoring and evaluating internal compliance** and ensuring **compliance with External requirements**, by:
  - ❖ Defining a system of internal controls embedded in the IT processes framework; monitoring and reporting on the effectiveness of such controls; and reporting control exceptions to management for action;
  - ❖ Identifying applicable legislation, regulation, contractual and other external requirements (including requirements relating to intellectual property rights, and privacy and protection of personally identifiable information); review and adjust IT policies and procedures to ensure compliance; monitor and report on compliance; and protect records from loss, destruction, falsification, unauthorized access, unauthorized release in accordance with requirements; technical compliance review *(Note: this is often covered as part of Audit of IT Security).*

4 Cross-cutting/ Special Focus Areas

4.1 Audit of Application Controls

The steps involved in carrying out a review of application controls in a specific IT system would broadly be as follows:

- Understanding the business processes/ requirements (laws and regulations, business rules, flows, actors, roles and related compliance requirements);
- Studying the IT application and its environment – this could involve:
  - ❖ Review of application documentation (including the functional requirements, the detailed design/ system requirement specifications – to establish the responsibility of an external service provider) as well as documentation on technical infrastructure;
  - ❖ Study key functions of the application at work by observing and interacting with operating personnel at work, performing a walkthrough of the business process and IT application from source entry to output and reconciliation mechanisms; Discussions with managers, operators and developers;
- Identify risks associated with the business activity/ function and see how these risks are handled by the application;
- Assessing controls, including substantive testing as appropriate (covered separately)

4.1.1 Input Controls

The objective of input controls is to ensure that the procedures and controls reasonably guarantee that (i) the data received for processing are genuine, complete, not previously processed, accurate and properly authorized; and (ii) the data has been entered accurately and without duplication. Input control is extremely important because the most important source of error or fraud in computerised systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

With regard to input controls, some common control elements include:

- Data entry checks (e.g. validity, completeness, duplicate; range checks) – this is generally the most important set of controls;
- Source documents management (e.g. preparation, logging, traceability (e.g. numbering) and retention procedures);
- Error handling mechanisms (e.g. error messages, subsequent correction measures, prompts enabling re-input, use of suspense data);
- Data entry authorisation rules (e.g. segregation of duties; manual procedures/ supervisory level authorisation of data on data entry form).

4.1.2 Processing Controls

The objectives of processing controls are to ensure that (i) the processing of transactions is accurate and complete; (ii) the transactions are unique without any duplication; (iii) all transactions are valid; and (iv) the computer processes are susceptible to audit.

This is achieved by providing controls for:

(i) adequately validating input and generated data;

(ii) processing the correct files/ data elements;

(iii) detecting and rejecting errors during processing and referring them back to the originators for re-processing;

(iv) proper transfer of data from one processing stage to another; and

(v) verifying, during or after processing, the control totals established prior to processing.

With regard to processing controls, some common control elements include:

- Proper mapping of business rules (e.g. requirements of law, rules and regulations);
- Checking for sequence and duplication errors; transaction/ record counts; control and has totals; Input reconciliations
- Referential integrity checks

4.1.3 Output Controls

Output controls ensure that all output is:

(i) produced and distributed on time;

(ii) fully reconciled with pre-input control parameters;

(iii) physically controlled at all times, depending on the confidentiality of the document; and

(iii) errors and exceptions are properly investigated and acted upon.

With regard to output controls, some common control elements include:

- Proper definition of outputs and desired reports at the system design and development stage;
- Proper documentation of report extraction logic;
- Output review and tracking
- Completeness and accuracy validations, reconciliation
- Review and follow-up of application generated exception reports
- Output labelling, handling, retention and distribution procedures

4.1.4 Application Security Controls

With regard to application security controls, the design of the application (e.g. whether through individual user IDs/ passwords or through single sign on mechanisms; the extent to which application rules are embedded in each application layer; the approach to role-based permissions for different application objects). Some common control elements include (*Note: several of these elements are generally applicable for IT Security, not just for security of specific applications)*:

- Traceability of transactions: transaction logging; use of unique user IDs; logs reporting and monitoring; ideally the audit log should record what records or fields were added/ amended/ deleted when they were added/ amended/ deletion, from what to what, and who made the addition/ amendment/ deletion;
- User accounts, permissions and password management: use of guest and test accounts; privileged and administrator accounts use and compensatory controls for such accounts; procedures for granting and revoking access; job termination procedures and access removal; IT/development team access to production databases; formal procedures for approving and granting access; use of strong passwords; periodic changes enforcement; password encryption etc.
- Masterfile and standing (semi-permanent) data protection: controls to ensure that amendments to standing data are authorised; users are held accountable for any changes made; the standing data is up-to-date and accurate; and the integrity of the master files is maintained;
- Conflicting duties and segregation of duties adoption: different user roles; access rights available for each user profile; segregation of duties rules.

4.2 Substantive testing, as part of detailed testing of application controls

Substantive testing of IT controls is often used to support assessment of controls through other means (review of documentation; questionnaires; walk-throughs; use of test data using the User Interface etc.). The objectives of such substantive testing, as part of an audit of IT systems, include:

- Confirming that the implementation of business functional requirements in the IT solution is actually working effectively, as evidenced through data analysis;
- Deriving assurance (or lack of such assurance) about the adequacy and effectiveness of IT controls (e.g. application controls relating to input validation and processing; security controls relating to access, logging).

However, where the data analysis/ analytics is carried out, not as part of a comprehensive audit scope to assess the adequacy and effectiveness of IT (and non-IT) controls, but related to other aspects of a financial, compliance or performance audit, this should be treated as an “IT-assisted audit”, which is covered in Section 6.

Substantive testing is usually carried out using IT tools for inquiry, extraction and data analysis[12], but often also includes detailed scrutiny of supporting documentation (e.g. manual/ offline workflows/ approvals; manual/ offline records, or unstructured electronic records – e.g. PDF or scanned documents, images etc.) for a sample of cases, as also tracing a sample of these transactions through different processes across the system.

A commonly adopted approach to testing of application controls is use of CAATs (Computer Assisted Audit Techniques). For example, either test data or CAATs may be used to test a control designed to ensure that payments exceeding a certain value are not made. CAATs can be used in this context to interrogate the entire payments file to identify payments in excess of the specified value. If the interrogation is applied to the entire year's transactions, it achieves the main audit objective in verifying that no excess payments will have been made in the period.

CAATs are often employed for:

(i) independent verification of ledger balances and control totals;

(ii) re-calculation of critical computerised calculations to verify their correctness;

(iii) range checks to verify the efficient functioning of IT controls and test for exception conditions;

(iv) testing the validity of data stored in the master file; etc.

Some of the CAATs commonly used in IA&AD currently are IDEA, MS Access, MS Excel, SQL Querying of RDBMS data etc. Detailed guidance on use of CAATs is covered separately, and not as part of this Standing Order.

Where the IT system with or used by the auditable entity is an end-to-end automated solution without significant offline/ manual documentation/ approvals, and controls for ensuring the integrity and non-repudiability of IT data is assessed by Audit to be adequate and effective, a significant proportion of audit may be conducted off-site; except with regard to outputs and outcomes, or as may be determined by Audit to be necessary for certain substantive checks in audit.

However, in the case of most IT systems implemented in the Indian public sector, the end-to-end automation is usually incomplete or has gaps, which necessitates detailed scrutiny of supporting documentation for a sample of cases. Such detailed scrutiny helps to validate the findings of inquiry, and data extraction and analysis; for example, in situations such as the following:

- Where there are concerns about the quality of data entered (integrity and non-repudiability) or maintenance of data quality in the IT solution;
- Where there are significant manual or offline approvals or other manual interventions;

[12] Computer Assisted Audit Techniques (CAATs) as well as specialised tools for data analytics

- Where the supporting documentation is either not fully captured electronically, or there are concerns about data integrity and non-repudiability;
- Where the solution does not cover the process chain in an end-to-end manner[13].

4.3 Audit of IT Security

Information Security can be defined as the ability to protect information and system resources with regard to **Confidentiality; Integrity; Non-repudiability**; and **Availability**. As the potential, complexity and role of information technologies grow, information security becomes an increasingly important topic of IT audits. It is a critical factor of organisation's activities, because information security weaknesses may lead to severe damage (legal, reputational/ credibility, financial, productivity, exposure to further intrusions). Such damage may be caused by security breaches (detected and undetected), unauthorised external connections to remote sites, exposure of information (disclosure of corporate assets and sensitive information to unauthorised parties).

Aspects to be covered in audit of IT security could include the following:

- **Formation of an Information Security culture**, by creating security awareness; seeking management commitment, and building co-ordination through setting up cross-functional teams, and thereby ensuring alignment of information security and business objectives.
- **Defining and implementing a risk management framework,** by
  - ❖ Establishing an IT risk management framework aligned to the organization's risk management framework;
  - ❖ Identifying and recording risks/ potential events (important realistic threats that could exploit a significant applicable vulnerability) and affect the confidentiality/ integrity/ non-repudiability/ availability of information systems or data;
  - ❖ Conduct risk assessment (i.e. assess the likelihood and potential impact of identified risks);
  - ❖ Develop and implement risk responses/ countermeasures that mitigate, in a cost-effective manner, exposure to risks. These counter-measures may avoid/ reduce the likelihood and/or potential impact; share or transfer the risk with/ to/ another party. The risk may also be accepted (either the entire risk, or the residual risk after countermeasures). Maintaining and monitoring of a risk action plan would be essential.
- **Developing and maintaining an IT Security policy** and associated procedures, which regulate how an organisation manages, protects and distributes resources to achieve security objectives; they will identify criteria for according individuals authority, and may

[13] E.g. in an e-procurement solution where the final approval of the purchase order takes place offline in the purchasing entity's files, or payment to the service provider does not take place through the e-procurement solution

specify conditions under which individuals are permitted to exercise their authority and should also provide individuals with a reasonable ability to determine whether their actions violate or comply with the Policy/ procedures. Policies for use of mobile devices and teleworking, where necessary, may also be adopted.

- **Organising of IT security** for implementing the IT security policy, including information security roles and responsibilities; segregation of conflicting duties;
- **Human Resources Security** at different stages – prior to employment (background verification checks, terms and conditions of employment relating to information security); during employment (management requiring compliance with information security policies and procedures; information security awareness, education and training; and disciplinary process against employees who have committed an information security breach); post-employment, termination and change of employment/ position (protection of organization's interests through revoking access/ enforcing access as per new responsibilities).
- **Asset management and control**, including inventory of assets associated with information and information processing, rules for acceptable use of assets, return of assets (by employees/ external users on conclusion of their employment/ agreement etc.), and disposal of assets, as well as information classification. Management of removable media, disposal of media, and protection during transportation are also important.
- **Authentication, Authorization and Access control:**
  - ❖ **Identity Management and Authentication** – enabling and managing user identities (including user account management); defining and implementing authentication mechanisms; hold users accountable for safeguarding their authentication information;
  - ❖ **Cryptographic controls** – Develop and implement a policy on the use of cryptographic controls; and develop and implement policies/ procedures for cryptographic key management;
  - ❖ **Authorization and Access Control** – Establish, document and review an access control policy, based on business and information security requirements, and implement access control to systems, applications and networks; Manage privileged access rights; Periodic review of user access rights and removal or adjustment upon termination/ change
- **Physical and environmental security** (covered in **Managing the physical environment** under "Delivery and Support");

- **Network security and cyber security management**[14];
- **Maintaining security of information transfer** within the organization and to an external entity
- **Security testing, surveillance and monitoring**;
- **Security requirements as part of system acquisition, development and maintenance**;
- **Operations security**:
  - ❖ Operating procedures and responsibilities (documented operated procedures; controlling changes to the organization, business processes etc.; capacity management; separation of development, testing and operational environments; control of operational software);
  - ❖ Protection from malware through detection, prevention and recovery controls, combined with user awareness;
  - ❖ Data backup (covered under **Managing data** as part of "Delivery and Support")
  - ❖ Logging and monitoring (event logging and protection; protection and review of administrator/ operator logs; clock synchronization)
- **Information security in supplier relationships**;
- **Information security incident management**, including
  - ❖ Establishing responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents;
  - ❖ Monitoring and detection of security events and reporting information security events through appropriate management channels as soon as possible;
  - ❖ Requiring employees and contractors to report observed or suspected information security weaknesses;
  - ❖ Assessing information security events and deciding if they are to be classified as information security incidents; responding to incidents in accordance with documented procedures; and learning from incidents to reduce the likelihood or impact of future incidents;
- **Compliance** (covered under **Monitoring and evaluating internal compliance** and ensuring **compliance with External requirements** under "Monitoring and Evaluation"

Typical risks for the audited entity could include:

- Unauthorised disclosure of information;

[14] Cyber security is the act of protecting internet-connected systems and networks from digital attacks. Network security, on the other hand, is the act of protecting files and directories in a network of computers against misuse, hacking, and unauthorized access to the system.

- Unauthorised modification or destruction of information;
- Vulnerability of information systems to attack
- Destruction of IT infrastructure
- Disruption of access to or use of information or an IT system
- Disruption of an IT system
- Information or data stolen or destroyed/ lost

Note: The Guidelines for Indian Government Websites require that websites/ web-hosted applications must undergo an (external) third party security audit from an empanelled agency, and successfully clear the same, prior to hosting and after addition of new modules; this also applies to mobile apps and APIs (Application Programming Interfaces). Also, government agencies/ contracted service providers internally conduct Vulnerability Assessment/ Penetration Testing (VT) of web applications and web hosting infrastructure. There are other guidelines which require successful third party audits[15].

IAAD Audit Teams do not conduct such security audits or VA/PT. However, we review the scope and coverage of these security audits to verify that it is adequate and also up-to-date; and also the content of the security audit reports to verify follow-up action, if any, required to be taken.

4.4 Audit of IT Outsourcing

4.4.1 Overview

Outsourcing is the process of contracting an existing business process that an organisation previously performed internally or a new business function to a third party. The contracted party is responsible for providing the contractually required services for an agreed fee. An entity may choose to outsource selected parts or all of its IT infrastructure, services or processes. Some areas of outsourcing could include:

- Operating infrastructure that may include data centre and related processes;
- Cloud computing with multiple options: Infrastructure as a Service (IAAS); Platform as a Service (PAAS); Software as a Service (SAAS) [16];
- Processing of in-house applications by a service provider
- Systems development or maintenance of applications

[15] E.g. the Guidelines for Compliance to Quality Requirements of e-Procurement Systems mandate successful audit from the STQC Directorate of MEITY (Ministry of Electronics & Information Technology)

[16] IAAS - A vendor provides clients pay-as-you-go access to storage, networking, servers and other computing resources in the cloud.

PAAS - A service provider offers access to a cloud-based environment in which users can build and deliver applications; provider supplies underlying infrastructure.

SAAS - A service provider delivers software and applications through the internet. Users subscribe to the software and access it via the web or vendor APIs.

- Installing, maintaining, and managing the desktop computing and associated networks.

4.4.2 Key Elements of Outsourcing

- **Outsourcing policy** – Organisations need to have some policy or vision on what aspects or the business functions (typically IT, but could be others) can be outsourced, and what functions must remain in-house.
- **Tendering for the outsourced service provider** – A transparent and objective process, based on criteria appropriate for the system or services being acquired; determination of outsourcing requirements prior to vendor selection.
- **Service Level Agreement (SLA)** – This is the most critical element of outsourcing and is a legally binding agreement which enables effective management of vendors. Typical areas would include:
  - ❖ Types of services that will be performed by the vendor; allocation of responsibilities between the organisation and the vendor
  - ❖ The services that will be measured, measurement period, duration, location, and reporting timelines (uptime; defect/ error rates, response time, help desk staffing hours, etc.)
  - ❖ Frequency of back-up, data and service recovery parameters e.g. Recovery Time Objective (RTO) and Recovery Point Objective
  - ❖ Time to implement new functionalities
  - ❖ Penalty (and incentive) clauses
  - ❖ Termination/ 'material breach' clauses
  - ❖ Data privacy and confidentiality;
  - ❖ Escrow clauses for source code;
- **Vendor/ contract management** – The audited entity should have processes to ensure periodic follow-up of the status of the project, quality of service, witnessing testing prior to introduction into the production environment; access to vendor's internal QA process (to ensure vendor personnel compliance with contractually approved policy and plans for all their work). SLA compliance monitoring and action for failure to meet SLA parameters are also very important.
- **Benefit realization** – If the justification for the outsourcing is realisation of cost savings, then the entity should try and determine, on a periodic basis, if the projected savings are achieved. The methodology for determining projected savings should be reviewed during audit.
- **Security** – The audited entity must evaluate whether vendors have sufficiently robust security practices and can meet the security requirements internally. The risk of security

breaches, intellectual property violations, or data privacy breaches must be addressed. While the outsourced service provider would be responsible for information security management, the audited entity remains accountable to its stakeholders for information security.

4.4.3 Vendor Lock-in/ Vendor Dependence

Vendor lock-in makes a customer dependent on a vendor for products and services, unable to use another vendor without substantial switching costs (financial, time, and effort involved). Vendor lock-in may be to the System Integrator (SI); the provider of data services (e.g. cloud service provider); OEM suppliers of products forming part of the technology stack; lock-in with a specific technology; or a combination thereof.[17]

Vendor lock-in (and how to minimise it) is one of the most critical aspects of outsourcing in the Indian public sector. Some of the major aspects of vendor lock-in include the following:

- ❖ Time consuming and effort-intensive acquisition process for a new product, or engagement with a new service provider;
- ❖ Loss of data, or inabilities/ difficulties in migrating data from the existing solution to a new solution;
- ❖ Difficulties in migrating some or all of the functionalities from the existing solution to a new solution;
- ❖ Lack of long term IT vision of the audited entity – not "building for change", and assuming that today's functionalities will not change and that the existing IT solution has an indefinite life.
- ❖ Inadequacies in tendering and contract award (e.g. clauses unduly unfavourable to the entity – e.g. highly onerous requirements for establishing material breach by the vendor) and contract award (e.g. inadequate attention to preparation and review of exit management plan and updates thereto; inadequate monitoring of SLA compliance);
- ❖ Lack of access to upto-date source code, and other solution documentation (application documentation – including detailed documentation of business processes/ functional requirements, system design and development; O&M documentation; documented SoPs etc.), which makes switching to another solution difficult;
- ❖ Lack of use of open standards/ open architecture while developing the solution, resulting in undue dependence on the vendor for frequent and continuous change management and difficulties in addition of/ changes to modules, integrability with future systems, and switching components of the technology stack;

[17] OEM: Original Equipment Manufacturer

- Discontinuing (immediate or in the short to medium term time horizon) of support for the existing solution or parts of the existing technology stack;
- Effort involved in upgrading elements of the existing technology stack to the current versions;
- High costs involved in upgrading elements of the existing technology stack (especially COTS/ proprietary software); need for enterprise support of existing technology stack at high costs;
- Lack of adequate institutional knowledge within the audited entity's staff (residing largely with the outsourced vendor's development/ O&M team) and undue dependence on key vendor personnel and/or on an external consultant;
- Ownership (or claim to ownership) by the vendor on intellectual property relating to the IT solution.

4.4.4 Other Risks to the Audited Entity

Typical risks to the audited entity, other than vendor lock-in, and associated aspects which have been covered in the previous section, include:

- **Vendor failure to deliver** (delivery on time, to scope/ quality, and to cost) – This could arise due to an imperfect tendering process, flawed contractual clauses, and inadequate management/ monitoring of vendor performance. Lack of, or ineffective, contingency plans for addressing such events may compound the problem.
- **Scope creep –** While a certain amount of scope change during the development cycle (typically of the order of 10-15%), substantial increases in scope (and costs) could occur due to various factors e.g. inadequate – or not detailed enough – requirement specifications; inadequate or poor user involvement/ sign-off during design and development (e.g. sign-off of SRS etc. with only a cursory review); inadequate user involvement in User Acceptance Testing; poor contractual clauses. At the same time, the tendency to make contractual clauses unduly strict (e.g. requiring the vendor to take on risks over which it has little or no control) could sometimes make things worse (e.g. forcing vendors to over-bid). The use of fixed cost pricing, when the requirements are fluid or ill-defined, also contributes to claims for change management costs.
- **Turnover of/ change in key vendor personnel,** potentially affecting delivery to time and cost.

5 Processes for Audit of IT Systems

5.1 "Auditability" and Information on IT Systems of Audited Entities

According to the Regulations:

- Audit may examine IT systems at various stages of the IT systems lifecycle for various validations, such as planning and feasibility study; requirements specification;

procurement and contracting; design and development; testing and implementation; operations & maintenance etc. This may also include audit of an IT system which is under development or implementation.

- An auditable entity is required to maintain complete documentation related to all stages (planning, acquisition, design, development and implementation, delivery and support, monitoring and evaluation) of an IT system. It is also required to document all changes made in its IT systems. Their absence in part or full, is to be reported by audit, along with the implications.
- The auditable entity is required to ensure that all requirements for the purpose of facilitation of audit are incorporated in the IT system, and audit of IT systems should comment on the absence/shortcomings in this regard, if any.
- Audit may, at periodic intervals, call for information from the auditable entity about various IT systems or platforms (including mobile apps etc.) in use or being developed and the auditable entity shall provide the requisite details.
- Depending on Audit's risk assessment and prioritization, Audit of IT system(s) would be necessary, when it is a newly implemented system or it has been subject to significant changes since the last audit so as to establish the integrity, non-repudiability and reliability of data.

In the context of rapid automation of audited entities, Audit's engagement with the audited entity at an early stage of definition and development of the IT systems is important. The ultimate responsibility for incorporating internal controls and an adequate trail into IT systems must rest with the audited entity. It is, therefore, not necessary for the auditor to provide, as a matter of policy, any consultancy advice on developing systems. Nonetheless, Audit should be aware of all developments that are likely to have a significant impact on the audit processes. At an early stage in the definition and design of a new system, the auditor should consider providing the auditee organisation specific comments on:

(i) internal controls in the light of weaknesses identified in the existing system;

(ii) audit needs such as data retention or retrieval facilities and audit trail requirements; and

(iii) any other requirement to facilitate audit or improve its efficiency and effectiveness.

5.2 Applicability to financial, compliance and performance audits

In general, audit of IT systems is important to derive assurance about the integrity, non-repudiability and reliability of data which is input, processed and output for these systems.

For financial audits, the adequacy and effectiveness of controls relating to the IT systems used to capture, process and output data for the preparation of financial systems is important. This could be considered either along with the audit of the financial statements or separately.

For compliance audits, the adequacy and effectiveness of controls for ensuring compliance with the stipulated authorities and criteria (e.g. laws, rules, regulations, procedures, best practices etc.) is important.

For performance audits (e.g. of schemes, activities, organizations etc.) the audit scope could include audit of the underlying IT-based transaction processing system/ MIS/ reporting system.

5.3 Risk-based approach to planning

According to the Regulations, depending on Audit's risk assessment and prioritization, Audit of IT system(s) would be necessary, when it is a newly implemented system or it has been subject to significant changes since the last audit, so as to establish the integrity, non-repudiability and reliability of data.

- A risk-based approach to planning of audits of IT systems is to be adopted. For this purpose, a listing of significant IT systems in use or in development in the auditable entities falling within the audit universe is to be maintained and kept up-to-date.
- The prioritization of audits of IT systems will depend, inter alia, on the criticality of the IT system to the functioning of the audited entity. For this purpose, a risk assessment exercise will need to be carried out periodically, in line with the detailed Standard Operating Procedure (SoP) issued by Headquarters Office. The results of this risk assessment exercise will be reflected in the form of the specific assignments for audit of IT systems to be included in the annual audit plans of the audit offices, along with the audit scope and high-level audit objectives.
- Detailed planning for the assignments for audit of IT Systems will involve preparation and finalization of Audit Guidelines, in line with the detailed SoP issued by Headquarters Office. These guidelines will spell out the detailed audit objectives, the audit scope and period of coverage, sampling approach etc. and also specify the audit techniques proposed (including where necessary, substantive testing through inquiry, extraction and data analysis supplemented, as appropriate, by detailed review of offline documentation etc.) In the case of assignments where external resources/ services may be required and/or novel IT or other approaches are being considered, this should also be covered in the Audit Guidelines.

5.4 Requirement for access to auditee data

The requirement for access to auditee data for substantive testing of IT controls (as also for IT-assisted audit), linked to the audit scope, audit objectives and period of coverage, should be determined at a sufficiently early stage **(typically at the time of identification of audit assignments, rather than later)** considering the delays that are often faced routinely in (a) getting such access from the audited entity and (b) restoring or transforming such data into a form suitable for data analysis by Audit.

In case of receiving data dumps from the audited entity, Audit needs to ensure the integrity and non-repudiability of the data dump. It is important to ensure this before commencing inquiry, extraction and data analysis, in order to ensure that there is sufficient and appropriate evidence to support the resulting findings, conclusions and recommendations.

This could be ensured through a forwarding letter from the audited entity, which specifies:

- The source (through reference to time stamp of generation of the data dump/ hash number for the data dump) of the data for the purposes of ensuring integrity of data, authentication and non-repudiation
- The parameters of extraction used to create the data dump, i.e. queries used/ reports run.
- If such a forwarding letter from the audited entity is not received, internal documents may be generated by the Auditors noting important information such as the date on which the data was handed over, from what file the data dump was created, and whether the data was from the production environment or from some other environment, etc.

5.5 Audit Execution

Audit execution may be carried out through a combination of techniques e.g. document review, questionnaire, observation, walkthrough, flow charts, data capture and analysis, verification, re-computation, re-processing, third party confirmation etc., as defined during the audit planning and design stage.

5.6 Audit Reporting

The objective of the assignment for audit of IT systems is to provide assurance[18] with regard to the entirety of audit objectives and audit scope. **Hence, a Management Letter should be issued, either by or with the approval of the Head of Department, to the Government.** The Management Letter should describe the audit findings, conclusions and recommendations vis-à-vis the audit scope and entire set of audit objectives (at an appropriate level of granularity). Audit objectives in respect of which instances of non-compliance were NOT found, should also be suitably reflected in the Management Letter. **The objective of the Management Letter should be to provide assurance with regard to what was covered in audit,** and not merely a list of deficiencies.

Depending on the nature of the audit assignment and resulting findings, conclusions and recommendations, potential material for inclusion in the CAG's Audit Report may be processed as per the guidelines and practices for the Audit Report.

6 IT-assisted audits

This section is primarily intended to distinguish between audit of IT systems (IT audits) and IT-assisted audits; it does not cover detailed guidance on use of data analytics/ analysis.

[18] In accordance with the CAG's Auditing Standards and subordinate audit guidance

IT assisted audits involve the use of various IT tools including, but not limited to, traditional data analysis tools (also referred to as Computer Assisted Audit Techniques (CAATs)) and data analytics/ big data analytics for supporting the achievement of the audit objectives. Such analysis or analytics is applied on data provided by the auditable entity, which may be available in a variety of structures and formats, as well as external or third party data.

Data analysis or data analytics may be used for the purpose of substantive testing of IT controls (to assess their adequacy and effectiveness), as part of an audit of IT System, as described in Section 4.2. This section relates to cases **where the objective of use of IT tools is** primarily **NOT to derive assurance with regard to the IT system through assessing the adequacy and effectiveness of IT and non-IT controls**; hence, IT-assisted audits are treated differently from audit of IT systems.

Traditional data inquiry and analysis tools (typical CAATs) usually involve exception-based queries. Going beyond such exception-based queries, data analytics is the application of data science approaches to gain insights from data. It involves a sequence of steps starting from collection of data, preparing the data and then applying various data analytic techniques to obtain relevant insights. The insights include, but are not limited to, trends, patterns, deviations, inconsistencies, and relationships among data elements identified through analysis, modelling or visualization, which can be used while planning and conducting audits

Data analytics or big data analytics, in the context of audit, could also involve creating a risk score for individual transactions (based on static or dynamic parameters and with or without use of Machine Learning or Deep Learning).

Audit of the concerned IT system(s), so as to establish the integrity, non-repudiability and reliability of such data through adequate and effective IT and non-IT controls, may be necessary, when it is a newly implemented system or it has been subject to significant changes since the last audit. A third party audit may be sufficient, if it provides an appropriate degree of assurance about the adequacy and effectiveness of controls and thus the integrity, non-repudiability and reliability of data in such IT systems.

Depending on the gaps in automation, the level of offline documentation, and the adequacy and effectiveness of controls, the reliability of findings through data analysis/ analytics may need to be validated through field examination and verification of a sample of cases.