

WGITA – IDI HANDBOOK ON IT AUDIT FOR SUPREME AUDIT INSTITUTIONS

Version 2022

**WGITA – IDI HANDBOOK ON IT AUDIT
FOR SUPREME AUDIT INSTITUTIONS
(2022 REVISION)**

INTOSAI Goal Chairs and IDI's joint paper on 'Quality assuring INTOSAI public goods that are developed and published outside due process' identifies three levels of quality assurance, as follows:

QUALITY ASSURING INTOSAI PUBLIC GOODS THAT ARE DEVELOPED AND PUBLISHED OUTSIDE DUE PROCESS – Levels of Quality Assurance

Level 1: Products that have been subjected to quality assurance processes equivalent to INTOSAI due process, including an extended period of transparent public exposure (90 days)

Level 2: Products that have been subjected to more limited quality assurance processes involving stakeholders from outside the body or working group responsible for the products' initial development. Quality assurance processes might, for example, include piloting, testing and inviting comments from key stakeholders, although not go as far as full 90-day public exposure

Level 3: Products that have been subjected to rigorous quality control measures within the body or working group responsible for their development

Different levels of Quality Assurance may be appropriate for different GPGs. This GPG has been developed according to quality assurance level 2

Quality Assurance Protocol: Version 2.0

IDI's Protocol for Quality Assurance (QA) of IDI's Global Public Goods defines measures to ensure quality based on the three levels of quality assurance above. For quality assurance level 2, these measures include: approval by the IDI Board to create the GPG; formation of a competent product development team; peer review by experts external to the development team; modification based on review; proofreading, editing and translation of the document by competent persons; public exposure with relevant stakeholders; and due approvals for the GPG version 1.

Updates to this GPG

To ensure that this GPG stays relevant, IDI and INTOSAI Working Group on IT Audit (WGITA) will conduct a light touch review of this handbook on a biennial basis. If there are substantial changes to be made, IDI-WGITA may decide to work on a revised version of the handbook. Such decisions will be taken on the basis of the biennial review. Major revisions will follow IDI's Protocol for Quality Assurance. Light touch reviews will not normally be subject to this Protocol.

This GPG is jointly owned by IDI (IDI's Relevant SAs work stream) and WGITA, which are responsible for maintenance of this GPG.

Quality Assurance Review Process

Shourjo Chatterjee (Strategic Support Unit, IDI) has undertaken a QA review of the process followed for the development of this GPG, against QA Protocol Version 2.0. The QA reviewer is familiar with IDI's protocol for QA of GPGs and was not involved in development of the GPG. This QA review process is designed to provide all stakeholders with assurance that the IDI has carried out the quality control measures stated above, designed to meet quality assurance level 2.

Results of the Quality Assurance Review

The QA review of the process followed in developing this GPG concluded that the Protocol has been followed as required for quality assurance level 2 in all respects.

Conclusion

Based on the QA review, IDI and WGITA assure the users of this Global Public Good (GPG) that this document has been subjected to a quality assurance process equivalent to Due Process for INTOSAI Framework of Professional Pronouncements (IFPP).


Einar Gørrissen
Einar Gørrissen (Dec 21, 2022 08:37 GMT+1)

Einar Gørrissen
Director General
INTOSAI Development Initiative
19 December 2022

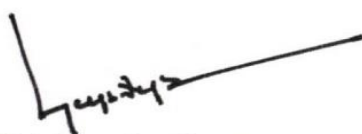

Girish Chandra Murmu
Chair,
INTOSAI Working Group on IT Audit

TABLE OF CONTENTS

PREFACE	1
LIST OF ABBREVIATIONS.....	2
INTRODUCTION.....	3
CHAPTER 1: IT AUDIT	6
I. What Is an IT Audit?	6
II. Step 1: Planning an IT Audit.....	9
III. Step 2: Designing an IT Audit.....	14
IV. Step 3: Conducting an IT Audit	18
V. Step 4: Reporting the Results of an IT Audit.....	23
VI. References and Further Reading	25
CHAPTER 2: IT GOVERNANCE AND MANAGEMENT	26
I. What Is IT Governance and Management?.....	26
II. Key Elements of IT Governance and Management	28
III. Risks to the Audited Organisation	32
IV. References and Further Reading	36
CHAPTER 3: IT DEVELOPMENT AND ACQUISITION	38
I. What Is IT Development and Acquisition?.....	38
II. Key Elements of IT Acquisition and Development	39
III. Risks to the Audited Organisation	42
IV. References and Further Reading	43
CHAPTER 4: IT OPERATIONS.....	45
I. What Are IT Operations?	45
II. Key Elements of IT Operations.....	45
III. Risks to the Audited Organisation	50
IV. References and Further Reading	51
CHAPTER 5: OUTSOURCING.....	52

I. What Is Outsourcing?	52
II. Key Elements of Outsourcing	54
III. Risks to the Audited Organisation	56
IV. References and Further Reading	58
CHAPTER 6: BUSINESS CONTINUITY MANAGEMENT	60
I. What Is Business Continuity Management?	60
II. Key Elements of Business Continuity Management.....	61
III. Risks to the Audited Organisation	67
IV. References and Further Reading	67
CHAPTER 7: INFORMATION SECURITY	69
I. What Is Information Security?.....	69
II. Key Elements of Information Security	72
III. Risks to the Audited Organisation	78
IV. References and Further Reading	79
CHAPTER 8: APPLICATION CONTROLS.....	81
I. What Are Application Controls.....	81
II. Key Elements of Application Controls	84
III. Interface and Data Management System Controls.....	88
IV. Risks to the Audited Organisation	89
IV. References and Further Reading	90

FIGURES

Figure 1: Common Phases of an IT Audit.....	9
Figure 2: Typical IT System Layout in an Organisation	12
Figure 3: Scope Considerations in an IT Audit	15
Figure 4: General and Application Controls	16
Figure 5: Audit Findings Matrix Template	19
Figure 6: Understanding IT Audit Documentation	22
Figure 7: Generic IT Governance Framework	27
Figure 8: Domains of IT Operations	45
Figure 9: Steps in Change Management	47
Figure 10: Application Review Cycle	82
Figure 11: Application Controls Example	84
Figure 12: Key Elements of Application Controls	84
Figure 13: Examples of Application Controls	85

PREFACE

The audit of information technology systems, controls, and processes, also referred to as an IT audit, has become one of the central themes of audits being conducted by Supreme Audit Institutions (SAIs) across the world. This is a natural response to the critical reliance on IT systems to support government and public sector organisations. The IT systems being used should protect the organisation's data and assets as well as support mission, financial, and other specific goals.

While the increasing use of IT has led to improved business efficiency and more effective service delivery, it has also brought with it risks and vulnerabilities associated with, for example, the digitalisation of services and the increased connectivity to other internal and external systems and networks. The role of IT audit in providing assurance that appropriate processes are in place to manage the relevant IT risks and vulnerabilities is essential if the SAI is to report meaningfully on the efficiency and effectiveness of government and public sector operations.

In 2014, the International Organization of Supreme Audit Institutions (INTOSAI) Working Group on IT Audit (WGITA) and the INTOSAI Development Initiative (IDI) jointly worked to produce the first Handbook on IT Audit with the goal to provide SAI auditors with standards and universally-recognised good practices on IT audit. This 2022 version of the handbook provides an update to the explanations of the major areas that IT auditors may be required to look into while conducting IT audits.

The WGITA/IDI handbook follows the general auditing principles as laid down under the International Standards for Supreme Audit Institutions (ISSAI).¹ The handbook also draws from the internationally recognised IT frameworks, including ISACA's COBIT framework, International Standards Organisation (ISO) standards, and IT guides and manuals of some of the SAIs, in an attempt to provide the users with essential information and key questions needed for the effective planning and performance of IT audits.

The project to update this handbook was led by the chair of WGITA, namely SAI India, SAI of the United States of America, and the IDI. WGITA and the IDI wish to thank the individual members of the team who worked relentlessly in developing this guidance. IT auditors from the SAIs of Australia, Brazil, Fiji, India, Kuwait, Philippines, Tanzania, and the United States of America have contributed valuably by providing IT audit report examples. Many thanks also go to the SAIs that provided their valuable feedback and comments on the handbook.

IDI and WGITA will conduct a light touch review of this handbook on a biennial basis. If there are substantial changes to be made, IDI-WGITA may decide to work on a revised version of the handbook. Such decisions will be taken on the basis of the biennial review.

¹www.issai.org.

LIST OF ABBREVIATIONS

BCP	business continuity plan
CMMI	Capability Maturity Model® Integration
DRP	disaster recovery plan
FISCAM	Federal Information Systems Controls Audit Manual
GAO	Government Accountability Office, United States of America
GUID	INTOSAI Guidance
IDI	INTOSAI Development Initiative
IEC	International Electrotechnical Commission
INTOSAI	International Organization of Supreme Audit Institutions
ISCP	information system contingency plan
ISO	International Organization for Standardization
ISSAI	International Standards for Supreme Audit Institutions (in older documents sometimes referred also as INTOSAI Standards)
ITIL	Information Technology Infrastructure Library
KPI	key performance indicator
NIST	National Institute of Standards and Technology, US Department of Commerce
OLA	operational level agreement
SAI	Supreme Audit Institution
SDLC	system development life cycle
SLA	service level agreement
WGITA	Working Group on IT Audit

INTRODUCTION

The universal nature of IT has changed the way we all work in many ways, and the audit profession is no exception. As technology has advanced, governments and other public sector organisations have continuously adopted IT innovations into their information systems with the goal of increasing efficiency and enhancing the delivery of various public services.² The delivery mode of public services has also rapidly transitioned from physical to electronic. This shift has resulted in government organisations having to function as digital platforms to provide services to the public, as well as infrastructure providers for their supporting IT systems. The ongoing digitisation of information, or the changing of records and data from an analogue format to a digital one, has also increased the overall dependency on IT systems.

The pace at which technology is advancing is faster than ever, which also has implications for IT audits. IT systems are increasingly complex, technologically diverse, and geographically dispersed. These systems are interconnected with other internal and external systems and networks, including the internet, thus increasing their complexity. Government organisations are also storing more of their information on cloud-based systems,³ with the goals of buying services more quickly and reducing costs. The trend toward ubiquitous computing and easier access to information will undoubtedly continue.

Advances in technology, however, have also brought increased risks and vulnerabilities. Notably, the growth of web-based IT systems and networks has increased the security risks facing government organisations. These organisations collect and process extensive amounts of personally identifiable information,⁴ which can pose challenges to ensuring the privacy of such information. The COVID-19 pandemic also generated unprecedented challenges for government organisations that needed to continue to carry out their missions while also ensuring that their employees were able to perform their work safely and effectively.

These trends, combined with the increasing sophistication of hackers and others with malicious intent, increase the risk of sensitive data being compromised. The ineffective protection of an organisation's systems and networks can also impair delivery of vital services. As such, each new vulnerability needs to be identified, risk assessed for likelihood and impact, mitigated according to an organisation's risk appetite, and controlled as appropriate.

With an increase in investment and dependence on IT systems by audited organisations, it is imperative for the IT auditor to adopt an appropriate methodology and approach. This can help to ensure that the audit can definitively identify risks to data integrity, availability, validity, abuse, and privacy, and also provide assurance that mitigating controls are in place. In an IT audit environment, controls are the processes, tools, and other oversight mechanisms in place to manage IT functions and to avoid risks and vulnerabilities.

In a typical IT system, especially when implemented in an environment of inadequate controls, the audited organisation faces many risks that an IT auditor should be able to identify. Even when the audited

²Information systems can be defined as a combination of strategic, managerial, and operational activities involved in gathering, processing, storing, distributing, and using information and its related technologies, while IT comprises the hardware, software, communication, and other facilities used to input, store, process, transmit, and output data.

³Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources (e.g., networks, servers, storage applications, and services) that can be rapidly provisioned and released.

⁴Personally identifiable information is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

organisation has implemented some risk reduction measures, an independent audit is required to provide assurance that adequate information system controls are in place. Such audits should include determining whether general IT controls⁵ and application controls⁶ have been designed to minimise the exposure to various risks and are operating efficiently and effectively.

In summary, the transition to IT systems and digital processing by audited organisations in the public sector has triggered a need for audit organisations to develop appropriate capacity to conduct a thorough examination of controls related to IT systems to fulfil their overall audit mandates. In particular, there is a need to ensure that internal IT controls related to the confidentiality, integrity, validity and availability of data have been adopted by government organisations.

Content and Structure of the Handbook

This handbook is intended to provide IT auditors with descriptive guidance on different domains in IT auditing and was developed following the requirements of IDI's Protocol for Quality Assurance of its Global Public Goods V2.0.⁷

In chapter 1 of this guide, readers will find an overview of IT audit definition, SAls' mandates, and the scope and objectives of IT audits. It also provides an explanation of general IT controls and applications controls, and the relationship between the two. These control domains are further elaborated on in subsequent chapters. Chapter 1 also describes the IT audit process and methodology of risk-based assessment for selecting IT audits. The description of the IT audit process is a generic one, based on standard audit methods⁸ followed when auditing IT systems. The tables and charts that accompany the description of the audit process are meant to provide illustrative examples and should be adapted to individual audit engagements. The users of the handbook should consider the audit process in the context of related information in the ISSAIs and other international frameworks and standards, as well as refer to the manuals and audit procedure guidelines at their respective SAls for planning and conducting specific audits.

Chapters 2-8 provide a detailed description of different IT domains that will assist IT auditors in identifying potential auditable areas. Organisational-level risks related to the IT domain have been listed at the end of each chapter, which will assist IT auditors in identifying the high-risk auditable areas. The guidance provided on each domain will help IT auditors in planning, either on a specific domain or a combination of domains depending on the scope and objective of the IT audit (e.g., performance audit or financial). For example, the guidance for the audit of IT governance can be used to plan an audit of an organisation's IT governance mechanism, or for planning the audit of the general controls environment of which IT governance is an important part.

Appendix I of this handbook includes an overview of emerging areas in IT auditing and provides references to further reading for the interested user. Appendix II includes links to audit reports identified by SAls around the world, which can provide valuable examples of the wide range of IT audit areas discussed in chapters 2-8 of this handbook.

⁵General IT 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, information system security, business continuity, and access and change management.

⁶Application 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.

⁷The protocol is available at <http://www.idi.no/en/idi-library/global-public-goods>.

⁸See, for example, International Organization of Supreme Audit Institutions, *International Standards of Supreme Audit Institutions (ISSAI) 100: Fundamental Principles of Public Sector Auditing* (2019) and ISSAI 5100 *Guidance on Audit of Information Systems* (2019).

The 2014 Handbook on IT Audit included a set of additional appendices with step-by-step guidance on developing an audit matrix. These audit matrix appendices listed key audit issues, criteria, information required, and analysis methods. For the 2014 Handbook on IT Audit and the audit matrix appendices, please visit: <https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-english-version.pdf>

Technical guidance on the use of Computer Assisted Audit Techniques is also beyond the scope of this handbook. The SAIs are encouraged to organise separate training in Computer Assisted Audit Techniques for their staff. The SAIs may also consider nominating their staff in the IDI capacity development programme on IT audit.

Please visit both the WGITA and IDI websites for more information on resources and upcoming training programmes.

WGITA: <https://www.intosaicommunity.net/wgita/>

IDI: <http://www.idi.no>

We hope that the SAIs and their IT audit staff will find this handbook to be a useful tool in enhancing their knowledge and understanding of IT audit issues, and that it will assist them in planning and conducting IT audits.

The readers of this handbook may also like to refer to other IDI global products, which complement this handbook. These include the *IDI Performance Audit ISSAI Implementation Handbook*,⁹ the *Financial Audit ISSAI Implementation Handbook*,¹⁰ and the *Compliance Audit ISSAI Implementation Handbook*.¹¹

⁹International Organization of Supreme Audit Institutions Development Initiative, *IDI Performance Audit ISSAI Implementation Handbook*, version 1 (August 2021), <https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook>.

¹⁰International Organization of Supreme Audit Institutions Development Initiative, *Financial Audit ISSAI Implementation Handbook*, version 1 (Dec. 8, 2020), <https://www.idi.no/news/professional-sais/financial-audit-issai-implementation-handbook-version-1-english-light-touch-review-2020>.

¹¹International Organization of Supreme Audit Institutions Development Initiative, *Compliance Audit ISSAI Implementation Handbook*, draft version 0 (Jan. 8, 2018), <https://www.idi.no/elibrary/professional-sais/issai-implementation-handbooks/handbooks-english/803-compliance-audit-issai-implementation-handbook-version-0-english>.

CHAPTER 1: IT AUDIT

As mentioned previously, government organisations' transition to IT systems and digital processing has triggered a need for audit organisations to develop the appropriate capacity to conduct a thorough examination of controls related to information systems to fulfil their overall audit mandates. In particular, audit organisations need to ensure that internal IT controls related to the confidentiality, integrity, validity and availability of data have been adopted by government organisations.

This chapter provides an overview of the process for auditing IT systems, also known as an IT audit. This chapter serves both as an introduction and summary to chapters 2-8. As such, this chapter differs from all the other chapters in terms of the design and detail.

As stated earlier, the description of the IT audit process depicted in this chapter is generic, based on standard audit methods, and is a reflection of audit methodology followed by SAIs. As such, users should consider the audit process described in this chapter in the context of related information in the ISSAIs and other international standards.

I. What Is an IT Audit?

a. Requirement to Conduct IT Audits

The mandate of a Supreme Audit Institution (SAI) to conduct an audit of IT systems is contained in ISSAI 1—Lima Declaration.¹² By extension, the mandate of an SAI to audit IT systems is derived from the overall mandate for SAIs to conduct performance, financial, and compliance audits or a combination of these.¹³

- A **performance audit** focuses on whether interventions, programmes, and institutions are performing in accordance with the principles of economy, efficiency, and effectiveness, and whether there is room for improvement.
 - **Auditing economy** focuses the audit on how the audited organisations succeeded in minimising the cost of resources, taking into account the appropriate quality of these resources.
 - **Auditing efficiency** means asking whether the inputs have been put to optimal or satisfactory use, or whether the same or similar outputs could have been achieved with fewer resources.
 - **Auditing effectiveness** deals with results. When assessing effectiveness, SAIs consider whether and how a government policy, programme, or activity is meeting its goals.

In performance audits, an organisation's performance is examined against relevant criteria that identify the required or desired state with respect to an audit topic as well as representing reasonable and attainable standards of performance. The causes of deviations from those criteria or other problems are also analysed. Performance audits typically test whether a government is making good use of resources to deliver its policy goals. Such audits often examine the implementation of a policy or policies.

- A **financial audit** focuses on determining whether an organisation's financial information is presented in accordance with an applicable financial reporting and regulatory framework and determining the accuracy of financial reporting. The purpose of a financial audit is to enhance the confidence that intended users can have in financial statements. This is achieved by the expression of the auditor's opinion on whether the financial statements were prepared, in all material respects, in accordance with an applicable financial reporting framework. A financial audit can involve detailed, substantive testing

¹²International Organization of Supreme Audit Institutions, *Lima Declaration*, Part VII Section 22.

¹³International Organization of Supreme Audit Institutions, *International Standards of Supreme Audit Institutions (ISSAI) 100: Fundamental Principles of Public Sector Auditing*.

of financial information.

- A **compliance audit** is an independent assessment of whether a given subject matter follows applicable authorities identified as criteria. A compliance auditor assesses whether activities, financial transactions, and information are, in all material respects, in compliance with the authorities which govern the audited organisation. Compliance audits add value by providing independent assurance of compliance by the audited organisation based on independent professional judgment and sound and robust analysis.
- An **integrated audit** combines different types of audits to evaluate the interplay between financial, operational and technology processes on the achievement of control objectives.¹⁴ For example, an integrated audit of an entity's financial statements may include an analysis of deficiencies in information systems controls.¹⁵

IT audits are frequently a subject area within the context of a broader audit (i.e., performance, financial, or compliance). An IT audit can be conducted that is not part of a performance, financial, or compliance audit; however, the general principles, procedures, standards, and expectations applicable to financial, performance and compliance audits are also applicable to IT audits.

b. Definition of IT Audit

IT audits are an examination of aspects of an organisation's use of IT, including IT infrastructure, policies and procedures, applications, and use of data. IT audits regularly incorporate analysis of systems and controls to ensure that they meet the organisation's business needs without compromising security, privacy, cost, and other critical business elements. IT audits also often involve deriving assurance on whether the development, implementation, and maintenance of IT systems meets business goals, safeguards information assets, and maintains data integrity. IT audits often involve the identification of instances of deviation from criteria, which have in turn been identified based on the type of audit engagement (e.g., a performance, financial, or compliance audit).

IT audits vary based on the types of audits within which they are performed. For example:

- In the context of a financial audit, an example IT audit could be an examination of general controls that ensure the operation of the information systems that underlie an entity's financial processes, as depicted through its financial statements.¹⁶
- In the context of a performance audit, an example IT audit could be a determination of the extent to which agency adoption of new technology has produced measurable government-wide benefits and cost savings.¹⁷

¹⁴Harvard University, "What Is an Integrated Audit?," <https://rmas.fad.harvard.edu/faq/what-integrated-audit>.

¹⁵For example, see: U.S. Government Accountability Office, *Management Report: Improvements Are Needed in the Bureau of the Fiscal Service's Information Systems Controls*, GAO-14-693R, (July 18, 2014), <https://www.gao.gov/products/GAO-14-693R>.

¹⁶For example, see: U.S. Government Accountability Office, *Management Report: Improvements Needed in the Bureau of the Fiscal Service's Information System Controls Related to the Schedule of Federal Debt*, GAO-22-105569, (Mar. 17, 2022), <https://www.gao.gov/products/GAO-22-105569>.

¹⁷For example, see: U.S. Government Accountability Office, *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked*, GAO-19-58, (Apr 4, 2019.), <https://www.gao.gov/products/gao-19-58>.

- In the context of a compliance audit, an example IT audit could be an examination of the efficacy of information systems that produce compliance reports, enabling employees to run and control an entity's operations.¹⁸

IT audits may deal with a variety of diverse areas, such as IT governance, IT investments in areas such as telecommunications, whether sufficient controls exist to protect data for entities such as local governments, analysis of the application of new technologies such as artificial intelligence, or the development, acquisition and operation of IT systems. IT audits also deal with aspects of both information security and cybersecurity, which are closely related.

- **Information security** can be defined as the ability of an IT environment¹⁹ to protect information and system resources, whether digital or analogue, with respect to confidentiality, availability, and integrity.²⁰ Information security includes those measures necessary to govern, prevent, detect, document, and counter such threats. Information security allows an organisation to protect its information system infrastructure from unauthorised users.
- **Cybersecurity** is the process of protecting digital information by preventing, detecting, and responding to cyberattacks.²¹ Cybersecurity involves strategy, policy, and standards regarding the security of, and operations in, cyberspace. It encompasses, among other things, threat and vulnerability reduction, incident response, resiliency and recovery, and information assurance.²²

A key difference between information security and cybersecurity is that cybersecurity focuses more precisely on the protection of digital information, while information security focuses more broadly on protection of all information system resources. Among these two areas, this handbook focuses primarily on information security, although many of the key elements of information security are also applicable to cybersecurity. A separate audit guidance document on cybersecurity and data protection is in development as part of another INTOSAI WGITA project.

c. Phases of an IT Audit

The primary phases of an IT audit include scoping, planning, designing, conducting, and reporting the results of the audit. Each of these phases is described in more detail below. Section II focuses on audit planning, section III on audit design, section IV on conducting the audit, and section V on reporting the results of the audit.

¹⁸For example, see U.S. Government Accountability Office, *Improper Payments: Additional Guidance Needed to Improve Oversight of Agencies with Noncompliant Programs*, GAO-19-14, (Dec. 7, 2018), <https://www.gao.gov/products/gao-19-14>.

¹⁹The IT environment consists of the IT applications, supporting infrastructure, and processes that an entity uses to support business operations and achieve business strategies.

²⁰National Institute of Standards and Technology, *Glossary*, (2021), <https://csrc.nist.gov/glossary>.

²¹National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1* (2018).

²²National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Glossary*, (Gaithersburg, MD: March 10, 2022), <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary>.

Figure 1: Common Phases of an IT Audit



Source: Unknown.

Note: This figure is intended to provide an illustrative example and should be adapted to individual audit engagements.

II. Step 1: Planning an IT Audit

Planning is a key part of any audit, including an IT audit. In most SAIs, planning for audits is carried out at three levels: strategic planning; macro, or annual planning; and micro, or organisation-level planning. Planning should be considered a continuous process throughout the audit, as additional information is discovered which may impact upon the original plan. An audit that follows from the results of a previous audit as part of a continuous audit approach requires similar planning. However, under a continuous audit approach, some steps, such as understanding the organisation, should be lessened as a result of information already gathered.

a. Strategic Planning

A strategic plan of the SAI is a long-term (3-5 years) forecast of audit targets and objectives, including those of IT systems and respective organisations under jurisdiction of an SAI. In some SAIs, only a list of new and emerging IT areas to audit may be included in their strategic plans. These could include looking at new methods of system development (e.g., agile programming), acquisition or cloud computing in the public sector, or the adoption of new technologies, such as artificial intelligence or blockchain. The strategic planning process and the SAI's strategic plan provides the tone and direction of the SAI's IT audit goals for the future. For example, as discussed in chapter 3 on IT development and acquisition, an organisation that is planning to adjust system development lifecycle methodologies might forecast an audit to check on the status and progress of the switch.

b. Macro Planning and a Risk-based Approach

The macro level of audit planning is usually done on an annual cycle basis at the SAI level for selection of the audit areas and, depending on the SAI, formulation of a process for deciding what areas will be audited annually.²³ With the rapid proliferation of modern IT systems across governments and the limitation of resources available to SAIs, a **risk-based approach** to prioritise and select suitable topics would be appropriate. In addition to considerations for selecting IT systems to audit, when deciding on audit topics,

²³The organisation of SAIs across the world will have different structures. The stage one here refers to a typical headquarters-field formation of an SAI, where the planning at global level is carried out or approved at headquarters and the actual audit is carried out at the field level.

organisations must also consider information such as overall IT expenditures, connectivity with other external entities, and the maturity of IT processes and governance. Furthermore, the SAI will additionally have to incorporate obligatory audits, like those demanded by law or requested by a parliament, congress, or other oversight organisations.

SAIs usually audit numerous organisations that use different information systems. There may be different applications for different functions and activities and there may be a number of computer installations at different geographical locations.

Considerations of how and which information systems to audit are partially based on an understanding of an organisation's inherent risk. **Inherent risk** consists of the probability that certain features of the IT systems of an audited organisation, by their very nature, may result in an adverse impact on the delivery of the function mandated to be carried out by the organisation. For example, an IT system that is required to make available information for all members of the public carries the inherent performance risk that beyond an anticipated peak user limit, the information system may fail to respond and the information would not be available to any user. While the organisation may adopt controls to mitigate inherent risks, in many cases, it may have to simply tolerate their existence within an acceptable risk level.

While there are risks inherent to information systems, these risks impact different systems in different ways. For example, the risk of non-availability even for an hour can be serious for a billing system at a busy retail store, and the risk of unauthorised modification can be a source of fraud and potential losses to an online banking system. The technical environments in which the systems run also may affect the risk associated with the systems.²⁴ A risk-based approach in selecting IT systems for an audit assists the auditor in deciding the priority of audits.

To use a risk assessment framework, an SAI needs to have some minimum information across agencies, usually gathered through a survey or control self-assessments. An example process for how to assess risks to determine potential IT systems for audit are listed in the “steps in a risk-based approach” box, at right.²⁵ For organisations with broader mandates, it will be necessary to narrow down potential audit scope, for example, to particular organisations or IT topics, before performing these steps.

For carrying out risk-based assessments of IT driven systems, SAIs may select a methodology which is appropriate for their purpose. Such methodologies may range from simple classifications of the risk profile of the IT environment as high, medium, and low to more complex and numeric calculations which quantify the risk rating based on objective data gathered from the audited organisation. The classification will be based on the SAI's understanding of the organisation and its environment and professional judgement of the IT audit team of a SAI. For

Example: steps in a risk-based approach

1. Identify the audit universe that would comprise the listing of all auditable organisations or units falling under the jurisdiction of an SAI.
2. List the information systems in use at the auditable organisation/units.
3. Identify factors that impact the criticality of the system for the organisation to carry out its functions and deliver service.
4. Assign weight to the critical factors. This could be carried out in consultation with the audited organisation.
5. Compile information for all the systems across all organisations, and—based on cumulative scores—place the systems/organisations in order of priority for audit.
6. Prepare an annual audit plan that outlines the priority, approach, and schedule of IT audits. This exercise could be done at annual intervals and thus could be a recurring plan.

²⁴S. Anantha Sayana, ISACA.

²⁵A further example of a risk assessment methodology for information systems, and a guide for auditors on how to assess risks when planning audit work, can be found at: Internal Audit Community of Practice, *Risk Assessment in Audit Planning* (April 2014), https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf.

example, as discussed more in chapter 4, an SAI deciding on which IT systems to audit may choose them based on which have implemented the most significant changes and add change management criteria to its list of potential risk areas.

While a risk assessment process is one way to select the audited organisation for IT audit, the SAIs also select auditable organisations on a cyclical basis, using mandated audits or on account of specific requests from oversight bodies (i.e., a congress, parliament, or legislature).

c. Micro Planning

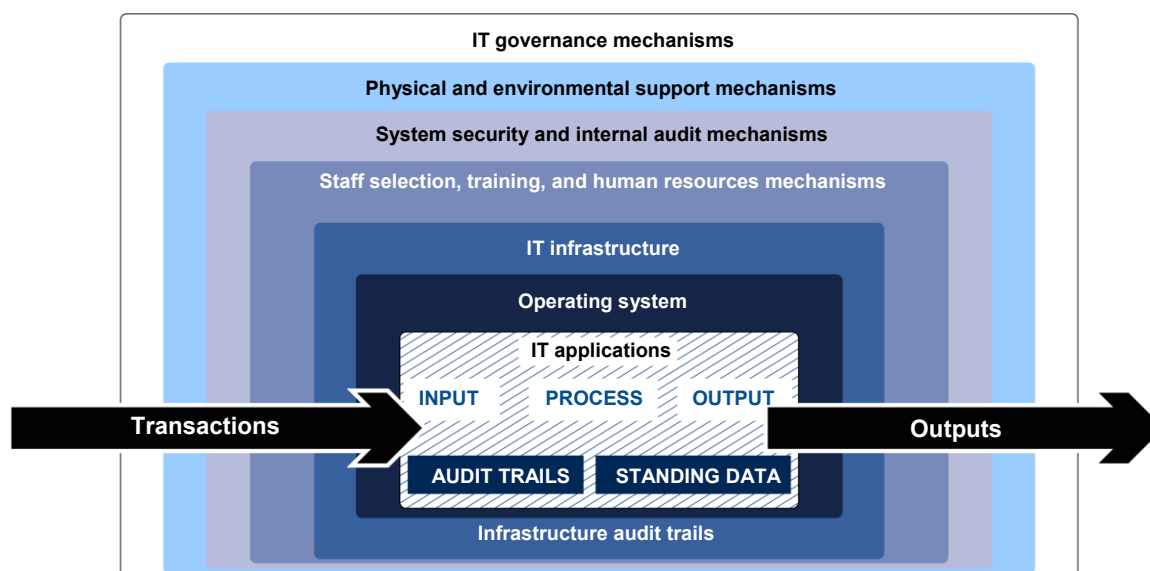
Micro planning involves the development of a detailed audit plan of the selected audit organisation, beginning with outlining the audit objectives. The audit plan will assist auditors in preparing an IT audit programme. The prerequisite step in developing the audit programme will be to have a clear understanding of the organisation and its IT systems. This handbook aims to assist the auditor once a plan has been created to populate the audit matrix with specific objectives for each area (e.g., governance and information security) that will be investigated. Micro-level planning requires an understanding of the organisation, some preliminary assessment of controls to facilitate detailed audit planning, and considerations of resource and staff allocation to ensure that the audit team is composed of members that collectively have the competence to conduct IT audit engagements to achieve the intended objectives. For example, as discussed in chapter 6 on business continuity management, an organisation may plan to audit additional criteria in the area of disaster recovery planning for systems that are vital to organisation-wide operations.

i. Understanding the organisation

The extent of knowledge of the organisation and its processes required by the IT auditor is largely determined by the nature of the organisation and level of detail in which audit work is being performed. IT audits will differ, for example, based on the scope of what is being audited—from an individual IT system to a single institution, area of government, or even a whole country. Knowledge of the organisation should include the business, financial, and inherent risks facing the organisation and its IT systems. It should also include the extent to which the organisation relies on outsourcing to meet its objectives and to what extent the organisation's business processes have been mapped in an IT environment.²⁶ The auditor should use this information in identifying potential problems, formulating the objectives and scope of work, performing the work, and considering actions of management for which the IT auditor should be alert. Figure 2 shows a typical layout of an IT system in an organisation.

²⁶Organisations changing over from a manual to an electronic environment would normally conduct a business process reengineering exercise. It may be possible that some of the business processes are being carried out manually along with the IT systems or that an organisation has developed automated processes that are inefficient or ineffective by replicating its manual processes. These particular scenarios would present specific interest areas for IT auditors.

Figure 2: Typical IT System Layout in an Organisation



Source: Unknown.

A typical application forming the core of an IT system in an organisation will have in place a technology stack—a combination of programming languages, frameworks, and tools that developers build upon to create the application. The technology stack can include a database management system with specific databases, software(s) mapping the business rules in the system through specific modules, and front end user interface(s) supported by network application software if there is a networked environment. The databases and applications software reside on servers, which are essentially high capacity hardware or software capable of hosting large and multiple databases and applications. The servers could be specific to different user requirements, such as data servers, application servers, internet servers, and proxy servers.

Prior to initiating the assessment of controls in an information system, the auditors should develop an understanding of the system architecture, and the underlying data and its sources in order to identify the required audit tools and techniques. Based on the IT auditors' understanding of the information system and the audited organisation, they may decide on their approach for an IT audit.

Other audit activities that could be useful in understanding the audited organisation include

- mapping out business operations of the auditee entity,
- mapping out the interaction of the entity with its peers or the outside environment,
- listing out business activities that are critical to the goals and targets of the auditee organisation, and
- listing out all the IT solutions that are being used by the entity.

ii. Materiality

The materiality, or relevance and significance, of IT audit issues should be determined under the SAI's overall framework for deciding materiality policy of an audit report. The perspective of materiality may vary depending on the nature of the IT audit engagement.²⁷ The auditor should consider the materiality of the matter in the context of, for example, the financial statements or the nature of the organisation or activity. Materiality in an IT context may also be defined in non-financial terms.

²⁷ISSAI 100 paragraph 41 states that "materiality is often considered in terms of value, but it also has other quantitative as well as qualitative aspects. The inherent characteristics of an item or group of items may render a matter material by its very nature. A matter may also be material because of the context in which it occurs."

The IT auditor should determine whether any IT deficiency could potentially become material. The significance of deficient general IT controls should be evaluated in relation to their effect on application controls (i.e., whether the associated application controls are also ineffective). If the application deficiency is caused by the general IT control, then they are material. For example, if an application-based tax calculation is materially wrong and was caused by poor change controls to tax tables, a management decision not to correct a general IT control deficiency and its associated reflection on the control environment could become material when aggregated with other control deficiencies affecting the control environment.²⁸

iii. Allocation of resources and audit team composition

IT audit requires specific allocation of resources, especially personnel who are well acquainted with typical IT systems, processes, and mechanisms that govern a successful IT implementation. In addition to suitable staff resources,²⁹ appropriate budget, infrastructure, and any other requirements identified should also be provided for. The timeline for an audit should be decided, if possible, in consultation with the audited organisation.

SAIs may ensure that the audit team is composed of members that collectively have the competence to conduct IT audit engagements to achieve the intended objectives. The necessary knowledge, skills, and competence may be acquired through a combination of capacity building, such as training or increased on-the-job experience; recruitment; and engagement of external resources, per the strategic plan of the SAI.

SAIs may consider different options to allocate human resources for IT audit engagements, such as the following:

- Establish a central group with IT specialists who assist other audit teams in the SAI to conduct these audits or deploying IT specialists.
- Establish a dedicated IT audit group or function that is entrusted with the responsibility of conducting all IT audit engagements for the SAI that interacts with other teams who have legacy knowledge of the audited organisation.
- Use a mix of generalist auditors with broad IT knowledge and specialised auditors with more focused expertise on one or a few specific areas of IT.
- Include other insourced staff resources as temporary members of IT audit team.

SAIs may engage external resources, such as IT consultants, contractors, specialists, and experts to conduct IT audits if internal resource constraints exist, or if external resources are deemed to be more convenient or cost effective. SAIs should ensure that such external resources are adequately trained and sensitised to the guidelines for professional conduct, as well as for processes and products of IT audit applicable to the SAI. This work should be adequately monitored through a documented contract, a service-level agreement, or a non-disclosure agreement. Special care may be needed with regard to the maintenance of confidentiality, especially with regard to auditee information, by the external resources.

When auditing IT systems, SAIs may ensure that IT audit teams collectively have the capacity to do the following:

- Understand the technical elements of an IT system, including all relevant instances of the application in use, so as to be able to access and use the IT infrastructure for the audit process.
- Understand the mapping of business processes into the programming logic of the IT system.

²⁸*Materiality Concepts for Auditing Information*, ISACA Guidelines (G6).

²⁹Suitable staff resources means personnel who have an understanding of the information systems and could carry out data extraction and analysis if required, as IT audits invariably require use of IT skills for carrying out the audits. The SAI should refer to ISSAI 100 paragraph 39 on providing the necessary competence to its staff before undertaking an IT audit.

- Understand the audit methodology, including relevant auditing standards and guidelines applicable to the SAI.
- Understand IT techniques to collect the audit evidence from automated systems.
- Understand IT audit tools to collect, analyse, and reproduce the results of such analysis or re-perform the audited functions.
- Understand how to evaluate and compare the costs, such as effort and resources, and the benefits derived from implementation of an IT system.
- Determine advantages, disadvantages and business risk of IT acquisition and outsourcing practices and strategies.
- Determine whether the objectives of the IT project were achieved with due regard to quality and scope, and within the budgeted timelines and costs.
- Understand services, requirements, and specifications to ensure reliable and cost-effective vendor selection and to verify that essential contents of vendor contracts are in place.

In addition, for financial audits, SAIs may also ensure that audit teams have sufficient experience generally in conducting financial statement audits and understanding financial statements.

III. Step 2: Designing an IT Audit

a. IT Audit Objectives

IT audit objectives can vary based on a variety of factors, such as the overall audit type (i.e., performance, financial, or compliance), the organisation or organisations under audit, type of IT operations under audit, the key risks to the organisation or organisations, and other factors.

Some examples of audit objectives are

- for performance audits, to ensure that IT resources allow organisational goals to be achieved efficiently and effectively, and that the relevant controls are effective in prevention, detection, and correction of instances of excess, as well as extravagance and inefficiency in the use and management of information systems;
- for financial audits, to evaluate the relevant controls which have an impact on reliability of data from information systems, which in turn have an impact on the financial statements of the audited organisation; or to evaluate the processes involved in the operations of a given area, such as a payroll system or financial accounting system; and
- for compliance audits, to ensure compliance of the processes of the information systems with the laws, policies, and standards applicable to the audited organisation.

The scope of IT audits may cover specific areas of IT implementation, such as

- acquisition, development, and implementation of IT systems,
- operations and maintenance,
- change management,
- access management,
- information security and business continuity,
- value for money delivered through IT systems, and
- enterprise resource planning or other complex/ specialised IT systems.
- enterprise resource planning or other complex/ specialised IT systems.

If an IT audit is a part of an audit engagement, the SAI should ensure that the audit team as a whole works in an integrated manner to achieve the overall audit objective. For example, to achieve effective integration,

SAls may consider

- comprehensively documenting the work to be performed by the IT auditors,
- formulating a protocol for sharing of information between the IT auditors and other auditors, and
- identifying which information systems and control objectives are within scope of the audit.

After developing audit objective(s) and approach, IT auditors often formulate specific audit questions that will guide the audit work. Audit questions should flow from the overall audit objective(s), and typically are more specific in that they address the topics you will describe or evaluate during the audit. The aim is for the audit questions to cover all aspects of the audit objective(s). Audit questions are either **descriptive** (meaning they describe a condition) or **evaluative** (meaning they evaluate a condition against criteria and can be normative or analytical).

b. Scope and Methodology of IT Audit

IT auditors have many options when determining the scope of an audit. Typical scope questions to consider are listed in figure 3.

Figure 3: Scope Considerations in an IT Audit

What?	<ul style="list-style-type: none">▪ What specific questions or hypotheses are being examined?▪ What are the key processes relevant to your audit?▪ What is the subject matter that will be assessed and reported on?▪ What resources are available to complete the audit?
Who?	<ul style="list-style-type: none">▪ Which agencies and organizations have responsibilities or perspectives relevant to the audit?▪ Who within relevant agencies and organizations is best positioned to provide appropriate and sufficient evidence to answer the audit questions?▪ Who is responsible for assuring the reliability of information and data that are relevant to your audit?
Where?	<ul style="list-style-type: none">▪ What are the locations to be covered?▪ Where are the documents and records that need to be examined?
When?	<ul style="list-style-type: none">▪ What is the timeframe to be covered?

Source: Performance Audit Subcommittee Development Team.

Note: This figure is intended to provide an illustrative example and should be adapted to individual audit engagements.

The IT auditor is very often required to assess the policies and procedures that guide the overall IT environment of the audited organisation, ensuring that the corresponding controls and enforcement mechanisms are in place. The scoping of the IT audit involves deciding the extent of audit scrutiny; the coverage of IT systems and their functionalities; IT processes to be audited; locations of IT systems to be covered including at third parties, such as cloud or outsourced providers, whose own control environments form part of the audited entity's control environment; and the time period to be covered by the audit.³⁰

SAls may select the time period for audit analysis (e.g., 1 year or 3 years) in defining the scope of the IT audit engagement. An audit could also be required to conclude on a specific date. A time period should be selected that is relevant to the aims defined for the audit engagement.

Once an audit's scope has been set, IT audit teams further define the methodology or specific steps they plan to take to perform the audit's objectives according to the scope. By defining methodology details, audit

³⁰Location includes the back-end servers (application or data), user locations, and networks in a generic manner, and also determines the physical locations to be covered in a distributed network across buildings, cities or countries, if applicable.

teams better ensure that the steps they plan to take are possible with respect to the data they plan to collect, that they do not perform extraneous audit steps, and that the results of the audit steps taken will allow the team to speak to the audit's objectives.

The audited organisation should be briefed about the scope, objectives, and the assessment criteria of the audit should be discussed with them as necessary. The SAI may, if necessary, write the engagement letter to the audited organisation where it may also set out the terms of such engagements.

c. General IT and Application Controls

As previously stated, IT audits are defined as the examination of controls related to IT systems, in order to identify instances of deviation from criteria. **Controls** are the processes, tools, and other oversight mechanisms in place to manage IT functions and to avoid risks and vulnerabilities. The controls evaluated in an IT audit will be determined by the objective and the scope of the audit.

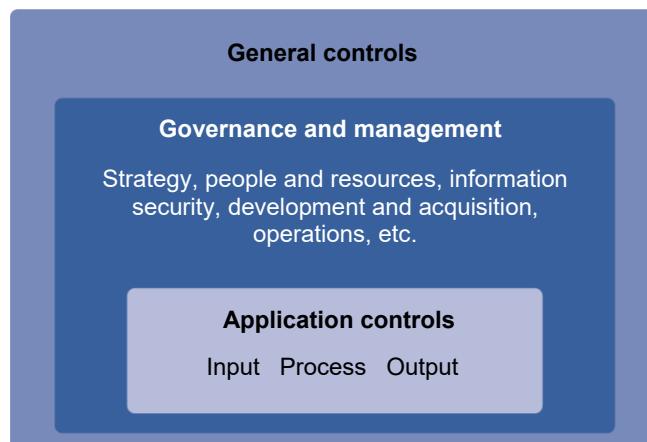
Controls are used to mitigate risks to the organisation. In particular, there are several types of risks relevant to IT audit controls:

- **Control risk** consists of the probability that IT controls that have been adopted by the audited organisation may fail to mitigate the adverse impact that they were designed in response to. For example, an information system which is required to ensure that access to confidential data is restricted to authorised personnel may adopt the control of requiring the presentation of a username and password by personnel attempting to gain access. The control risk in this situation is that the username and password are not adequately secure and can be guessed by unauthorised personnel through repeated attempts, resulting in loss of confidentiality and potential adverse impact on the organisation. An organisation that insists on use of secure, non-trivial passwords which have a combination of alphabetical, numerical, and special symbols and ensures that the information system prevents access to the username beyond a certain number of failed attempts to gain access would have a lower control risk than one that does not have these features. Use of multi-factor authentication could also be used to lower control risk in such a situation.
- **Detection risk** consists of the probability that the absence, failure, or inadequacy of IT controls adopted by an organisation, which may have a potentially adverse impact on the organisation, are not detected by the auditor.
- **Residual risk** is the remaining level of risk after controls have been applied, can be further reduced by identifying those areas in which more control is required. An acceptable level of risk target can be established by management (risk appetite).

In an IT context, controls are divided into two categories, which are shown in figure 4: general controls and application controls. The categories depend upon a control's span of influence and whether it is linked to any particular application.

General IT controls are the foundation of the IT control structure. These are concerned with the general environment in which the IT systems are developed, operated, managed, and maintained. General controls are manual or automated procedures which aim to ensure confidentiality, integrity, and availability of information in the physical environment within which information systems are developed, maintained, and operated. General controls establish a framework of overall control for the IT activities and provide assurance that the overall control objectives are satisfied.

Figure 4: General and Application Controls



Source: Unknown.

General controls are implemented using a number of tools such as policy, guidance, and procedures as well as implementing an appropriate management structure, including that for management of the organisation's IT systems. Examples of general controls include the development and implementation of an IT strategy and an IT security policy, setting up of an IT steering committee, organising IT staff to separate conflicting duties, setting up of system roles and privileges appropriate to a person's role, and planning for disaster prevention and recovery.

General IT controls are not specific to individual transaction streams or particular accounting packages or financial applications. The objective of general IT controls is to ensure the appropriate development and implementation of applications, programme and data files, and computer operations.

Application controls are specific controls unique to the information systems in each application. Application controls are IT dependent manual or automated procedures within an information system that affect the processing of transactions and may relate to validation of input data, accurate processing of data, delivery of output data, and controls related to integrity of master data. They apply to application segments and relate to the transactions and existing data. For example, in an online payment application, one input control could be that the credit card expiry date should fall beyond the date of transaction, and details entered should be encrypted.

The design and implementation of general IT controls may have a significant impact on the effectiveness of the application controls. General controls provide the applications with the resources they need to operate and ensure that unauthorised inquiries and changes cannot be made to either the applications (i.e., they are protected from reprogramming) or underlying data (e.g., the large collection of transaction data).

Critical element areas for application-level general controls are³¹

- security management,
- access control / segregation of user access,
- configuration management / change management,
- operations management, and
- contingency planning.

The application controls operate on individual or groups of transactions and ensure that the transactions are correctly input, processed, and output. The design and operating effectiveness of general IT controls greatly influence the extent to which the application controls can be relied upon by the management to manage risks.

d. Why Are IT Controls Important for the IT Auditor?

Generally, the IT auditor is called upon to test technology-related controls. As more and more organisations rely on IT to automate their operations, the line dividing the role of an IT and a non-IT auditor is also fast reducing. As a minimum, all auditors are required to understand the control environment of the audited organisation so as to deliver assurance on internal controls operating in an organisation. As per ISSAI Fundamental Principles of Public Sector Auditing, "auditors should obtain an understanding of the nature of the entity/programme to be audited."³² This includes an understanding of internal controls, as well as objectives, operations, regulatory environment, systems, and business processes involved.

Every control area is based on a set of control objectives that an organisation puts in place in order to mitigate a control risk, including technical requirements in place for an organisation's systems. The role of the auditor is to understand the potential business and IT risks facing the audited organisation, and in turn

³¹U.S. Government Accountability Office, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, (Feb. 2, 2009), <https://www.gao.gov/products/gao-09-232g>.

³²International Organization of Supreme Audit Institutions, *ISSAI 100*, paragraph 45.

to assess whether the deployed controls are adequate to meet the control objective. In the case of General IT controls, it is important for the auditor to understand the broad categories and extent of general controls in operation, evaluate the management oversight and staff awareness in the organisation for the same, and find out how effective the controls are in order to deliver assurance. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications.

In subsequent chapters, such as chapter 8 on application controls, some of the key areas of general IT controls and applications controls are discussed in detail.

IV. Step 3: Conducting an IT Audit

Conducting of an IT audit includes key steps such as gathering audit evidence that is sufficient, appropriate, relevant, and reliable; conducting a preliminary assessment of controls, such as policies and procedures, to assess their reliability; and detailed substantive testing of priority areas to ascertain the degree to which a control is working properly.

a. Gathering Audit Evidence

i. Evidence

Audit findings must be supported by evidence, so the quantity and quality of the evidence obtained is important. This means an IT auditor will need to continuously consider and evaluate the evidence they are planning to obtain, or have obtained, for sufficiency and appropriateness. Sufficiency refers to the quantity of evidence collected. Appropriateness refers to the quality of the evidence, and whether it is reliable and relevant. Auditors can evaluate whether evidence is relevant and reliable by considering, among other things, the nature of the source of the evidence and the source's reputation; controls operated by the audited entity, the presence of contradictory or confirmatory evidence, and the methods, models, and assumptions used in preparing the information in the evidence.

One useful tool for assessing audit evidence and developing conclusions and recommendations is an audit findings matrix. This tool allows auditors to determine whether findings and recommendations, if applicable, are based on sufficient and appropriate evidence. Figure 5 provides an example of an audit findings matrix template.³³

³³An illustration of a completed audit findings matrix can be found on page 174 of International Organization of Supreme Audit Institutions Development Initiative, *Performance Audit ISSAI Implementation Handbook*, version 1 (August 2021), <https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook>.

Figure 5: Audit Findings Matrix Template

Audit objective: Clearly and objectively express what the audit is about.

Audit question (the same stated in the audit design matrix): For each audit question (or sub-question), repeat each of the items mentioned in the table.

Finding	Finding statement (situation found)	Most relevant occurrences identified in the fieldwork.
	Criteria	Information used to determine if the expected performance of the audited object is satisfactory, exceeds expectations, or is unsatisfactory.
	Evidence and analysis	Result of applying data analysis methods or assessing your evidence. The techniques used to handle the information collected during fieldwork and the results achieved can be indicated.
	Causes	Reasons for the situation found. May be related to operation or design of the audit object. May be out of the control of the manager. Any recommendations should be related to the causes.
	Effects	Consequences related to causes and to corresponding evidence. These may be a measure of the findings' relevance.
Is the evidence sufficient (Y/N) and, if not, what remaining work is necessary to address any gaps in the evidence?		Consider the evidence you have for each element of the finding and whether it is sufficient and appropriate. If your current evidence is not sufficient for each element, what remaining work is necessary to address any gaps in the evidence?
Good practices		Actions identified that lead to good performance. May support the recommendations.
Recommendations		Proposals to address the causes (or deficiencies) identified.

Source: Adapted from U.S. GAO and SAI Brazil.

Note: This figure is intended to provide an illustrative example and should be adapted to individual audit engagements.

ii. Phase 1 - preliminary assessment of IT controls

The IT auditor should conduct a preliminary assessment of IT controls—both general and application controls—in the system to derive an understanding of assurance that they are reliable and sufficient to achieve the audit's objective.

The scope of the assessment of IT controls may include assessing whether

- IT policy has been defined, adopted, and communicated;
- IT governance structure is in place and is functional;
- controls accurately reflect technical requirements for underlying information systems;
- inventory of information system assets has been periodically carried out and requirements for augmentation, replacement, and removal have been identified;
- processes for sharing infrastructure and common services for information systems with other public organisations are in place and functional;
- processes for development, acquisition, and maintenance of IT have been defined, adopted, and

communicated (including that of change management);

- processes for IT operations (insourcing, outsourcing, and service agreements) have been defined, adopted, and communicated;
- measures to ensure physical security and intended physical working conditions have been adopted;
- measures for training and sensitisation of human resources to ensure confidentiality, integrity, and availability of information as well as compliance with the IT policy and governance structure requirements have been adopted;
- measures to ensure confidentiality, integrity, and availability of various communication modes and channels have been adopted;
- measures for statutory compliance management have been adopted;
- measures for business continuity management and disaster recovery management have been adopted;
- measures to ensure the completeness, accuracy, validity, and confidentiality of transactions and data performed as a part of business processes have been adopted; and
- measures to ensure the timely, accurate, and complete processing of information between system components, such as between applications have been adopted.

Depending upon the objective of the audit, auditors may be concerned with the design, implementation, and operating effectiveness of controls. If an auditor is concerned with the design of the control, an interview or inspection of documented business rules may be sufficient. If an auditor is concerned with the implementation of controls, inquiry may not be sufficient, and it may be necessary to conduct a walk through—an audit technique to confirm the understanding of controls—or perform data analysis to substantiate that the control has been implemented. Finally, an auditor who has concerns with the operating effectiveness of the control may be required to plan a sample test of transactions to demonstrate that the control has operated effectively throughout the relevant period.

Auditors may also consider how the evidence about the general controls impacts the nature, timing, and extent of procedures and evidence required to obtain assurance about the operation of application controls. For example, auditors should also consider evidence that supports the logical access of personnel to IT systems and change management within the production environment. If auditors have obtained sufficient and appropriate audit evidence regarding the effectiveness of the general controls, they may be able to conclude on the operating effectiveness of automated application control procedures. This can be done by testing a smaller sample of transactions because the effectiveness of the general IT environment provides evidence to the auditors on the effectiveness of the application control in the relevant period. In case of manual application control procedures, auditors may have to test a sample size appropriate to the confidence level selected.

iii. Phase 2 - substantive testing

Based on the assessment of IT controls, auditors may identify priority areas for taking up substantive testing, which involves detailed testing of the IT controls by employing various techniques for enquiry, extraction, and analysis of data. In substantive testing, the tests are designed to substantiate the assertions as per audit objectives.

Among the techniques used by IT auditors for data analysis are exception reporting, where deviations from expected performance are documented; file comparison; stratification, the sorting of data elements into distinct groupings; sampling; and duplicate checks. Another option for testing a system solution is the “thread and knots” approach, which progresses one business process at a time to identify significant activity points and whether relevant and adequate IT controls are present at each activity point. IT auditors should be cognisant of these options and use the appropriate tools for analysis. Auditors can use generalised or specialised audit software to carry out the information analysis.

When conducting substantive testing, IT auditors should ensure that the electronic evidence collected and

documented is sufficient, reliable, and accurate to sustain the audit observations. Such electronic evidence may consist of data files, user logs, analytical models, and management information systems reports and should be appropriately gathered and stored in a manner such that they are available for drawing assurance on the accuracy and validity of the audit process.

The IT auditor should also select an appropriate risk assessment and use sampling techniques to derive suitable conclusions based on statistically sufficient checks on limited data. Generally, it is good practice to recruit the aid of an expert or statistician within the organisation to select and determine the sampling method.

Where data volume and transfer, storage, and processing capacity permit, a high quality risk assessment can also be performed over the entire population to identify trends correlated to the auditor's understanding of the business. For example, an auditor could obtain a list of all users and their last system logon dates and compare it to a list of official departure dates to obtain a 100 percent analysis. This would enable an auditor to identify anomalous transactions or data points to form part of the sample in a more risk-targeted manner.

b. Engagement with the Audited Organisation

The ISSAIs recommend that the auditors establish effective communication throughout the audit process and keep the audited organisation informed of all matters relating to the audit.³⁴ For an IT audit, auditors may solicit due cooperation and support of the audited organisation in completing the audit, including access to records and information. Auditors may identify the mode of access to electronic data in the format necessary to allow analysis, in consultation with the audited organisation. The mode of access to data would be SAI specific.

c. Documenting an IT Audit

Information systems' audit documentation is the record of the audit work performed and the evidence supporting findings and conclusions. Preservation of the results and evidence is to be ensured by IT auditors such that they conform to the requirements of reliability, completeness, sufficiency, and correctness. It is also important for IT auditors to ensure that the audit process is preserved to enable subsequent verification of the analysis procedures. This involves suitable documentation techniques.

Documentation includes a record of

- the planning and preparation of the audit scope and objectives;
- the audit programmes;
- the evidence collected on the basis of which conclusions are arrived at;
- all work papers, including general files pertaining to the organisation and system;
- points discussed in interviews clearly stating the topic of discussion, person interviewed, position and designation, time, and place;
- observations as the auditor observed the performance of work:
 - The observations should include at least the place and time, the reason for the observation, and the people involved;
- reports and data obtained from the system directly by the auditor or provided by the audited staff:
 - The IT auditor should ensure that these reports carry the source of the report, the date and time, and the conditions covered;
 - One option for capturing these details is to use a screen capture; and
- any comments and clarifications added by auditors at various points in the documentation regarding

³⁴International Organization of Supreme Audit Institutions, *ISSAI 100*.

concerns, doubts, and need for additional information:

- The auditor should return to these comments later and add remarks and references on how and where these were resolved.

The evidence gathered during an IT audit may have necessary timestamps and details containing steps of data analysis carried out so that there is clarity on when the evidence was created, stored, and last modified, to mitigate the risk of subsequent changes. Figure 6 provides examples of what an IT auditor should expect to be able to understand from audit documentation.

Figure 6: Understanding IT Audit Documentation

What should an experienced auditor be able to understand from audit documentation?	
✓ The nature, time and extent of the work conducted.	✓ The conclusions reached as a result of the aforementioned significant matters.
✓ The findings of the audit work and the evidence obtained.	✓ Significant or key decisions made in reaching those conclusions.
✓ Significant matters that arose during the audit (for example, changes in the scope or approach of the audit, decisions regarding a new risk factor identified during the audit, actions taken as a result of disagreement between the audited entity and the team, etc.).	

Source: /Performance Audit Subcommittee Development Team.

Note: This figure is intended to provide an illustrative example and should be adapted to individual audit engagements.

As with all audit documentation, IT audit documentation should be retained and protected from any modification and unauthorised deletion. SAIs may evolve new standards for retention of IT audit documentation or adapt existing standards to meet the requirements of retention of IT audit related documentation. The period of retention should be a function of the mandate of the individual SAI and the statute(s) governing its activities. Special attention may be paid to media, the format, the life expectancy, and the storage requirements for these data, to ensure that the data are readable within the time frame defined in each SAI's data retention and archiving policy. This may necessitate converting data from one format to another to keep up with technological advances and obsolescence.

In case of examination of technical reports prepared by third party auditors on technology specific subject matters, auditors may adopt appropriate procedures to ensure the reliability of certain performance, financial, or compliance aspects. If, as a result of such procedures, reliance is placed on the contents of such reports, the fact of reliance should be suitably disclosed.

For preserving electronic data, the SAIs should provide for a back-up of data received from the audited organisation and the results of queries and analysis. The audit documentation should be kept confidential and should be retained for a period as decided by the SAI or imposed by law. The draft and final reports of the audit should also form part of the audit documentation. Where the audit work is reviewed by a peer or a superior, the remarks arising out of the review should also be recorded in the documentation.

d. Supervisory Review

The work of audit staff should be properly supervised during the audit, and documented work should be reviewed by a senior member of the audit staff.³⁵ The senior member of the audit staff should also provide necessary guidance, training, and a mentoring role during the audit.

³⁵International Organization of Supreme Audit Institutions, *ISSAI 100*, paragraphs 38, 39, and 50.

V. Step 4: Reporting the Results of an IT Audit

An IT audit report should follow the general layout of the reporting system followed by the SAI. IT audit reports should measure the technicalities reported based on the level of detail required by the audience of the report.

The IT auditor should report on the findings in a timely manner, and the findings should be constructive and useful to the audited organisation as well as meaningful to other stakeholders. The report could be submitted to appropriate authorities as per the mandate of the SAI and the IT audit.

Auditors should be aware of the need to limit the use of technical jargon and of the sensitivity of the information presented (e.g., passwords, usernames, and personal information) in the report. Despite the technical nature of an IT audit, auditors should ensure that the report is fully understandable by senior management of the audited organisation, stakeholders, and the general public. As part of this process, IT auditors should be aware that their audience is both other IT experts and the general public, and that they will need to interpret technical content for the latter.

Auditors should consider the potential negative impact of the report once an IT audit report is published. For example, if the IT audit report detects some security risks in the information system of an audited organisation and the same are reported before necessary controls to mitigate the risks have been adopted, the vulnerability of the information system may be exposed to the public. In such a scenario, auditors may consider options—such as reporting only after the necessary controls have been adopted, not reporting the exact security risk in full to avoid potential adverse impact on the audited organisation, or providing a separate/annexed confidential report that is not intended for wider circulation.

See appendix II for links to audit reports identified by SAIs around the world related to the chapters of this handbook. These audit reports can provide valuable examples of the wide range of IT audit areas discussed in this handbook.

a. Stages of Reporting

IT audit reporting depends on the traditions of SAIs and their legal environments. Reporting throughout the audit process often consists of stages such as:

i. Draft report

The reporting process begins with the discussion of the first draft of a report. This draft, after having been agreed to and approved internally within an SAI, is sent to the audited organisation's management prior to the closing meeting. The draft is then included as a matter for discussion in the closing meeting. This allows any inflammatory wording, factual errors, and/or inconsistencies to be identified, corrected, or eliminated at an early stage. Once the audited organisation and the auditor have discussed the contents of the draft, the auditor makes the necessary amendments and sends the audited organisation a formal draft.

ii. Management letter

The management letter is the formal draft given to the audited organisation so that it can respond to the observations raised. This allows management to concentrate on the findings, conclusions, and recommendations in the formal draft that they receive. At this point, it is the duty of management to formally write comments/responses to the auditor and address all the findings.

iii. Final audit report

When the audited organisation's comments are received, the auditor then prepares a response indicating the audit position. This is achieved by putting together the auditor's comments and the organisation's response in one report, which is the audit report (the final audit report).

In reporting on irregularities or instances of non-compliance with laws or regulations, the auditors should be mindful of placing their findings in the proper perspective. Reports on irregularities may be prepared irrespective of a qualification of the auditor's opinion.

By their nature, the audit reports tend to contain significant criticisms, but in order to be constructive, they should also address future remedial action by incorporating statements from the audited organisation or the auditor, including conclusions or recommendations.³⁶ Depending upon the SAI, the ultimate recipient of the management report may be those responsible for managing the organisation's operations or those responsible for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity.

In audits that involve IT audit work, the result of the IT audit may, in some cases, be communicated to the organisation through the means of a separate letter. In these cases, it may be important to explain how the result of the audit work relates to other communications which are part of the same performance, financial, or compliance audit and how the results of the IT audit work may be relevant for the resulting SAI audit report.

iv. Formulation of conclusions and recommendations

Audit findings, conclusions, and recommendations must be based on evidence. In formulating the conclusions, the IT auditor should have regard to the materiality of the matter in the context of the nature of the audit or audited organisation.³⁷ For balanced reporting, noteworthy accomplishments that fall within the SAI's mandate should also be reported.

IT auditors should frame conclusions on the findings based on the objectives. The conclusions should be relevant, logical, and unbiased. Sweeping conclusions regarding the absence of controls and risks should be avoided, when they are not supported by substantive testing such as control testing.

IT auditors should report recommendations when the potential for significant improvement in operations and performance is substantiated by the findings. Auditors should also report the status of uncorrected significant findings and recommendations from prior audits that affect the objectives of the current audit. Constructive recommendations can encourage improvements. Recommendations are most constructive when they are directed at resolving the cause of identified problems, action oriented and specific, addressed to parties that have the authority to act, feasible, and cost effective.

v. Limitations and constraints to IT audit

Limitations to the IT audit should also be pointed out in the report. The typical limitations are inadequate access to data and information, lack of adequate documentation of the IT process, and leading the IT auditor to devise his or her own methods of investigation and analysis to derive conclusions. Any other limitation or constraint faced by the IT auditor that affects the audit scope or execution should be pointed out in the report appropriately.

vi. Management response

In the case of IT audit reports, it is extremely important to get a response to the audit observations. The IT auditors should have meetings with the agency management at the highest level and document their response. If these efforts fail, adequate evidence about efforts made should be kept on record and mentioned in the report.

³⁶International Organization of Supreme Audit Institutions, *ISSAI 100*, paragraph 51.

³⁷International Organization of Supreme Audit Institutions, *ISSAI 100*, paragraph 50.

VI. References and Further Reading

Internal Audit Community of Practice. *Risk Assessment in Audit Planning*.

https://www.pempal.org/sites/pempal/files/event/attachments/cross_day-2_4_pempal-iacop-risk-assessment-in-audit-planning_eng.pdf. April 2014.

International Organization of Supreme Audit Institutions Development Initiative. *INTOSAI Development Initiative (IDI) AFROSAI/E-IT Audit Courseware*.

International Organization of Supreme Audit Institutions Development Initiative. *Performance Audit ISSAI Implementation Handbook*, version 1. <https://www.idi.no/work-streams/professional-sais/work-stream-library/performance-audit-issai-implementation-handbook>. August 2021.

International Organization of Supreme Audit Institutions. *International Standards of Supreme Audit Institutions (ISSAI) 100: Fundamental Principles of Public Sector Auditing*. 2019.

International Organization of Supreme Audit Institutions. *International Standards of Supreme Audit Institutions (ISSAI) 200: Fundamental Principles of Financial Auditing*. 2019.

International Organization of Supreme Audit Institutions. *International Standards of Supreme Audit Institutions (ISSAI) 300: Fundamental Principles of Performance Auditing*. 2019.

International Organization of Supreme Audit Institutions. *International Standards of Supreme Audit Institutions (ISSAI) 400: Fundamental Principles of Compliance Auditing*. 2019.

International Organization of Supreme Audit Institutions. *GUID 5100: Guidance on Audit of Information Systems*. 2019.

ISACA. *CISA Review Manual*, 27th ed.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*.

<https://www.isaca.org/resources/cobit>. November 2018.

ISACA. *IT Audit Framework (ITAF): A Professional Practices Framework for IT Audit*, 4th ed. October 22, 2020.

U.S. Government Accountability Office. *Federal Information System Controls Audit Manual (FISCAM)*.

<https://www.gao.gov/products/gao-09-232g>. February 2, 2009.

CHAPTER 2: IT GOVERNANCE AND MANAGEMENT

I. What Is IT Governance and Management?

IT governance can be thought of as the overall framework that guides IT operations in an organisation to ensure that it meets current business needs and that it incorporates plans for future needs and growth. It is an integral part of enterprise governance and comprises the organisational leadership, institutional structures and processes, and other mechanisms (e.g., reporting and feedback, enforcement, and resources) that ensure that IT systems sustain organisational goals and strategy while balancing risks and effectively managing resources.

It is important to understand that, according to ISACA's COBIT framework, there is a clear distinction between governance and management:³⁸

- **Governance** ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives; direction is set through prioritisation and decision-making; and performance and compliance are monitored against agreed-on direction and objectives.
- **Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

IT governance plays a key role in determining the control environment and sets the foundation for establishing sound internal control practices and reporting at functional levels for management oversight and review. It is critical to ensuring that

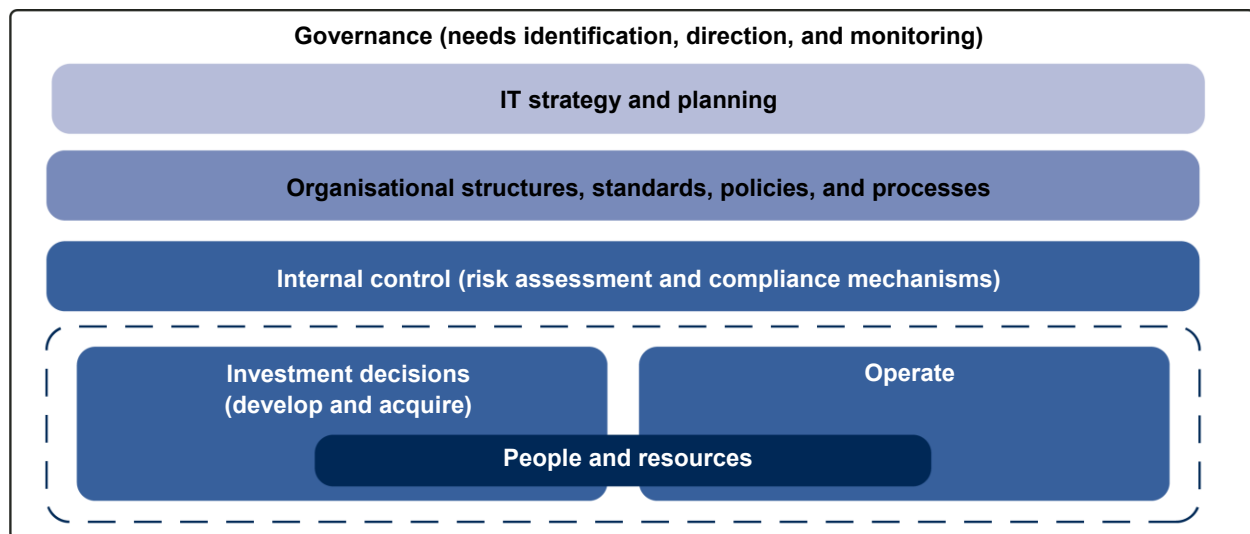
- stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives;
- direction is set through prioritisation and decision making; and
- performance and compliance are monitored against agreed-on direction and objectives.

In many organisations, governance is the responsibility of a board of directors, under the leadership of a chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.

A generic IT governance framework is represented in figure 7.

³⁸See *Section IV: References and Further Reading* of this chapter for additional references and resources related to IT governance and management best practices and frameworks.

Figure 7: Generic IT Governance Framework



Source: Unknown.

a. Needs Identification, Direction, and Monitoring

IT governance is a key component of the overall corporate governance. IT governance should be viewed as how IT creates value that fits into the overall corporate governance strategy of the organisation and never be seen as a discipline on its own. In taking this approach, all stakeholders would be required to participate in the IT governance decision-making process. This creates a shared acceptance of responsibility for critical systems and ensures that IT-related decisions are made and driven by business needs.

For IT governance to ensure that the investments in IT generate business value, and that the risks associated with IT are mitigated, it is essential that an organisational structure with well-defined roles for the responsibility of information, business processes, applications and infrastructure are put in place.

The governing body evaluates strategic options, directs senior management on the chosen strategic options, and monitors achievements. Management addresses

- overall organisation, strategy, and supporting activities for IT;
- definition, acquisition, and implementation of IT solutions and their integration in business processes;
- operational delivery and support of IT services, including security; and
- performance monitoring and conformance of IT with internal performance targets, internal control objectives, and external requirements.

It is also essential to involve IT governance in the process to identify new or updated business needs and then provide the appropriate IT (and other) solutions to the business user. During the development or acquisition of the solution to the business need, IT governance ensures that the selected solutions are responsive to the business and that necessary training and resources (i.e., hardware, tools, and network capacity) are available to implement the solution. Monitoring activities may be carried out by the internal audit or quality assurance group, which would periodically report their results to management.

II. Key Elements of IT Governance and Management³⁹

a. IT Strategy and Planning

The IT strategy represents the mutual alignment between IT strategy and business strategic objectives. The IT strategic objectives should consider the current and future needs of the business, the current IT capacity to deliver services, and resource requirements.⁴⁰ The strategy should consider the existing IT infrastructure and architecture, investments, delivery model, resourcing including staffing, and lay out a plan that integrates these into a common approach to support the business objectives.

It is important for the IT auditor to review an organisation's IT strategy not only to gain sufficient understanding of the organisation but also in order to assess the extent to which IT governance has been a part of the corporate decision-making.

Without an IT strategy, there is increased risk that organisations will not have identified how IT can meet the organisation's current and future business needs. Further, without an up-to-date IT strategic plan—linked to the organisation's overall strategic plan that includes goals, performance measures, strategies, and interdependencies among projects—organisations risk lacking a clear definition of what they want to accomplish with IT and strategies for achieving those results.

b. Organisational Structures, Standards, Policies, and Processes

Organisational structures are a key element of IT governance in articulating roles of the various management and governance bodies across the business and decision making. They should assign clearly-defined delegations for decision making and performance monitoring. Organisational structures must be supported with appropriate standards, policies, and procedures, which should enhance decision-making capacity.

Organisational structures in a public sector organisation are influenced by **stakeholders** (i.e., all groups, organisations, members, or systems who affect or can be affected by an organisation's actions). Examples of important external stakeholders include the Parliament, the Congress, and/or other government entities and the citizens. Organisational structures are also influenced by **users**, internal and external.

Internal users are the business executives and functional departments who own business processes, and individuals within the organisation who interact with business processes. External users are the agencies, individuals, and public who use products or services provided by an organisation (e.g., other departments and citizens). Another influence on organisational structures are **providers**: a company, unit, or person, both external and internal, who provide a service.

The need for IT functionalities emerges from the users and stakeholders. In all cases, appropriate governance organisational structures, roles, and responsibilities should be mandated from the governing body, providing clear ownership and accountability for important decisions and tasks. This should include relationships with key third-party IT service providers.⁴¹

The IT organisational structure usually includes an **IT steering committee**, which is the central piece of the organisational structure. The IT steering committee comprises members of top and senior management and has the responsibility for reviewing, endorsing, and committing funds for IT investments as well as ensuring that the main goals and targets assigned to the organisation are achieved. The steering committee

³⁹The key elements presented in this IT governance chapter are supported by *COBIT 5 Framework*, *COBIT 2019*, and *ISO 38500* with an extensive use of their definitions and examples.

⁴⁰International Organization for Standardization, *ISO 38500*.

⁴¹ISACA, *COBIT 2019*.

should be instrumental in devising business decisions for which technology should be provided to support business investments as well as approving how to acquire this technology. Investment decisions involving “build vs. buy” solutions are typically the responsibility of the IT steering committee generally after suitable recommendations from designated groups or committees.

The steering committee plays a critical role in promoting the necessary buy-in and providing management support for programmes that entail changes to the organisation. In many public sector organisations, IT steering committee functions are part of the management function. It is important to note that IT governance is complex and multifaceted. Different management structures like the steering committee will serve different purposes and feature different roles and responsibilities based on a variety of factors, including organisational needs, organisational sector, and organisational environment. Although the key roles and responsibilities that comprise the management function can vary among countries and sectors (e.g., public vs. private sector organisations), examples include the following:

- The **Chief Executive Officer** is the most senior official who is responsible for the total management of the organisation.
- The **Chief Financial Officer** is the most senior official who is accountable for all aspects of financial management, including financial risk and controls.
- The **Chief Operating Officer** is the most senior official accountable for the operation of the organisation.
- The **Chief Risk Officer** is the most senior official accountable for risk management across the enterprise. A Chief Risk Officer may have IT risk functions to oversee IT-related risk.
- The **Chief Privacy Officer** is a senior person who is responsible for monitoring the risk and business impacts of privacy laws, and for guiding and coordinating the implementation of policies and activities that will ensure that the privacy directives are met.
- The **Chief Information Officer** is a senior person who is responsible for the management and operation of an organisation’s IT capabilities. In many public sector organisations, the functions carried out by the Chief Information Officer may be conducted by a group or department, which has the necessary responsibilities, authority, and resources.
- The **Chief Technology Officer** is a senior person whose responsibilities may include, for example, ensuring that the organisation’s use of technology is efficient and effective, incorporating best practices and procedures into the implementation of IT capabilities, and providing the expertise to adopt emerging technologies into the organisation.
- The **Chief Information Security Officer** is the most senior official accountable for the security of all forms of enterprise information.
- The **Chief Human Capital Officer** is the most senior official who is responsible for aligning human resources policies and procedures with the organisational mission and strategic goals.
- The **Chief Knowledge Officer** is the most senior officer accountable for managing all forms of knowledge within the enterprise.

Without a well-defined organisational structure, including an IT steering committee, organisations may lack an entity responsible for making business decisions for which technology should be provided to support business investments as well as for approving how to acquire this technology. Further, organisations may lack the necessary management support for programmes. As a result, these activities may occur in an inconsistent and disorganised manner and may not result in value for money or not achieve the objectives of the programme or investment.

c. Standards, Policies, and Processes

Standards and policies are adopted by the organisation and approved by senior management. Policies lay the high-level framework for daily operations in order to meet the goals set by the governing body. Standards prescribe quantifiable measures in order to meet the policies. Standards and policies are supported by processes that define how the work or measures are to be accomplished and controlled. These goals are set by senior management to accomplish the organisation’s mission and at the same time

to comply with regulatory and legal requirements.

Standards, policies, and corresponding processes need to be reviewed and adjusted on a regular basis and need to be communicated to all relevant users in the organisation periodically. Employees of the IT department also need to be trained on how to apply and use these policies, standards, and processes in their daily operations. Policies, standards, and corresponding processes should reflect updates on new technology and threats, significant changes in processes, and new environment and regulatory requirements. It is usually an organisation's standards that an IT audit will use as its subject matter, as these measures can be audited against.

Policies and corresponding processes need to be reviewed and adjusted as needed. The same should be communicated to all relevant users in the organisation on a periodic basis. Policies shall reflect updates on new technology and threats, significant changes in processes, environment and regulatory requirements. Some key policies that guide the IT governance include the following:

- **Human resource policy:** The human resource policy deals with the hiring, training, job termination, and other functions of the organisation. It deals with roles and responsibilities of various personnel within the organisation as well as the requisite skill or training they are required to possess to carry out their duties. The human resource policy may also assign roles and responsibilities and segregation of duties. However, this function may also be delegated to a dedicated department in large and complex organisations.
- **Documentation and document retention policies:** Documentation of information systems, applications, job roles, reporting systems, and periodicity is an important reference point to align IT operations with business objectives. Appropriate documentation retention policies enable tracking and managing iterative changes to information architecture in an organisation.
- **Outsourcing policy:** IT outsourcing is most often aimed at allowing the organisation's management to concentrate their efforts on core business activities. The need for outsourcing may also be driven by the need to reduce running costs. An outsourcing policy ensures that proposals for outsourcing operations and functions are developed and implemented in a manner which is beneficial to the organisation. One of the most common examples of outsourced IT services today is cloud computing, which enables on-demand network access to a collection of configurable computing resources (e.g., networks, servers, storage, and other services). See chapter 5 for more information on outsourcing and cloud computing.
- **Remote work policy:** Organisations should establish remote work policies and guidance to ensure that their workforces are remote work ready. A key practice to facilitate remote work is to establish written remote work agreements for use between employees and managers. Remote work agreements should outline the specific work arrangement between the manager and the employee prior to the employee beginning remote work, and should establish job duties and expectations, performance standards, and measurable outcomes and deliverables.
- **IT security and privacy policy:** This policy establishes the requirements for protection of information assets, and may refer to other procedures or tools on how these will be protected. The policy should be available to all employees responsible for information security, including users of business systems who have a role in safeguarding information (i.e., personnel records and financial input data). See chapter 7 for more information on IT security and privacy policy.
- **Data management policy:** Organisations collect data from many resources, such as transactional systems, scanners, sensors, social media, and smart devices, among others. Therefore, organisations need to define the policies and procedures for how they will manage data throughout the lifecycle, such as the collection, storage, security, and disposition of the data. See chapter 4 for more information on data management.

Organisations lacking policies and standards for daily operations are at increased risk of not meeting IT-related goals. For example, a human resource policy is important for managing hiring and training, and an IT security policy is important for ensuring the protection of information assets.

d. Internal Control

As mentioned earlier, internal control is the process of introducing and implementing a system of measures and procedures to determine whether the organisation's activities are and remain consistent with the approved policies, standards, and plans. If required, necessary corrective measures are taken so that the policy objectives can be achieved.

Internal control keeps the IT system on course. Internal controls include risk management, compliance with internal procedures and instructions and with external legislation and regulations; periodic and ad hoc management reports; progress checks; and revision of plans and audits, evaluations, and monitoring.⁴²

Without internal controls, organisations face an increased risk that IT systems will not comply with internal policies, standards, laws and regulations.

i. Risk management

The management of IT risks should form an integral part of the company's risk management strategy and policies. Risk management involves identification of risks concerning existing applications and IT infrastructure, and continuous management, including a periodic review and update by the management of the risks and monitoring of mitigation strategies. IT risk management should be part of overall risk management within organisation.

The development of a risk management plan helps to facilitate the risk management process. The plan serves to document the process of identifying and assessing risks. It also documents processes, tools, and procedures used to manage and control risk throughout a project. See chapter 3 on IT development and acquisition for more information on risk management.

ii. Compliance mechanism

Organisations need to have a compliance mechanism that ensures that all the policies and associated standards and procedures are being followed. It is important to establish an organisational culture where employees understand the impact of noncompliance with stated policies, standards and procedures. The compliance supporting mechanism may also include the quality assurance group, security staff, and automated tools. A report of noncompliance should be reviewed by appropriate management and serious or repeated noncompliance issues must be dealt with. Management may choose to deal with noncompliance with refresher training, modified procedures, or even an escalating retribution procedure depending on the nature of the noncompliance (e.g., security violations and missing mandatory training).

Independent assurance, in the form of internal or external audits (or reviews), can provide timely feedback about compliance of IT with the organisation's policies, standards, procedures, and overall objectives. These audits must be performed in an unbiased and objective manner so that the managers are provided with a fair assessment of the IT project being audited.

Without a compliance mechanism in place, organisations may lack credible assurance that the process and selected work products are implemented as planned and adhere to the process description, standards, and procedures.

e. Investment Decisions

IT governance should provide business users with solutions to their new or modified requirements. These can be accomplished by the IT department through investment decisions to either develop (build) new software or systems or acquire these from vendors on a cost-effective basis. In order to make successful investment decisions, best practices typically require a disciplined approach where requirements are

⁴²"IT Governance in Public Sector: A top priority," *WGITA IntoIT*, Issue no. 25, (August 2007).

identified, analysed, prioritised, and approved; a cost-benefit analysis conducted among competing solutions; and the optimum solution selected (e.g., one which balances cost, risk, and meets a significant number of the organisation's objectives).

The development of a business case, identifying user needs and highlighting the opportunities and benefits of a solution, is a valuable tool for guiding investment decisions. The business case can begin as a high-level strategy and develop into a detailed description of key tasks, milestones, responsibilities, and roles. The business case serves as a dynamic tool requiring continuous updates to reflect the current situation and consider the future of the initiative. See chapter 3 for more information on IT development and acquisition.

f. IT Operations

IT operations is typically the day-to-day running of the IT infrastructure to support business needs. Properly managed IT operations make it possible to identify bottlenecks and plan for anticipated capacity changes (e.g., additional hardware or network resources), measure performance to ensure it meets the agreed-upon needs of the business owners, and provide help desk and incident management support to the users of IT resources. See chapter 4 for more information on IT operations.

g. People and Resources

It is recommended that management ensure through regular assessments that sufficient resources are allocated to IT for meeting the needs of the organisation, according to agreed priorities and budget constraints. Furthermore, the human aspect should be respected by the policies, practices, and IT decisions, which should consider the current and future needs of process participants. Governance management should regularly assess whether resources are being used and prioritised as the business objectives demand.

Organisations can benefit from IT workforce management and planning that addresses strategic planning, ensures that IT competency and staffing needs are met, and includes recruitment and hiring practices, training and workforce development, and performance management. Key elements of proper workforce planning include

- establishing and maintaining a workforce planning process,
- developing competency and staff requirements,
- assessing competency and staffing needs regularly,
- assessing gaps in competencies and staffing,
- developing strategies and plans to address gaps in competencies and staffing,
- implementing actions to address gaps, monitoring progress in addressing gaps, and
- reporting to leadership on progress in addressing gaps.

III. Risks to the Audited Organisation

Auditors need to understand and evaluate the different components of the IT governance structure to determine whether the IT decisions, directions, resources, management, and monitoring support the organisation's strategies and objectives. To carry out the assessment, auditors need to know the key components of IT governance and management, as well as the risks associated with the inadequacy of each component in an entity.

The continuous monitoring, analysis, and evaluation of metrics associated with IT governance initiatives require an independent and balanced view to facilitate improvement of IT processes. Audit plays a significant role in the successful implementation of IT governance by providing recommendations in mitigating the risks associated with the following aspects of IT governance and management:

- alignment of the IT function with the organisation's mission, vision, values, objectives, and strategies;
- achievement of performance objectives established by the organisation and the IT function;
- legal, environmental, information quality, fiduciary, security and privacy requirements;
- control environment of the organisation;
- inherent risk within the information security environment; and
- IT investment/expenditure.

Every organisation faces its own unique challenges as its individual environmental, political, geographical, economic, and social issues differ. Although this is not an exhaustive list, the consequences presented below represent common risks that might result from the lack of proper IT governance.

a. Ineffective and Inefficient IT Systems

Public administration systems that are aimed to serve the society, business, or enhance the functionality of the government agencies are often immensely wide-ranging and complex solutions. Thus, they should be properly designed, tailored to the real needs of the organisation, competently coordinated, and efficiently run. The lack of business ownership over processes, application and data might lead to poor IT governance. Poor IT governance at the government level and at the organisation level can be the first obstacle to having good quality IT systems.

b. Perception That IT Provides a Low Contribution to Business Value

Little or no business value may be derived from major IT investments that are not strategically aligned with the organisation's objectives and resources. Such poor strategic alignment means that even good quality IT may not be efficiently and effectively contributing to the achievement of the organisation's overall objectives. A way to ensure the alignment is to involve users and other stakeholders who understand the business in IT decision making. These stakeholders can contribute to the development of the business case to ensure alignment with organisational objectives and resources.

c. Lack of Involvement of the Enterprise IT Department

Research has found that leading organisations adopt and use an enterprise-wide approach to managing IT that includes, among other things

- responsibility for "commodity IT;" that is, things like email services, help desk services, and acquisition of hardware and software;
- oversight of mission-specific systems; and
- clear responsibilities between the enterprise IT department and any business units or components.

Without centralised authority and oversight, an organisation has diminished assurance that investments in IT are being coordinated organisation-wide and that they provide an appropriate mix of capabilities that support mission needs while avoiding unnecessary duplication.

d. Exposure to Information Security and Privacy Risks

An organisation that does not have proper information security controls, structures, processes, and policies is at a greater risk of information security and privacy incidents and breaches. These risks include, among other things, misappropriation of assets; unauthorised disclosure of information; unauthorised access; and vulnerability to logical and physical attacks, cyberattacks, disruption and information unavailability, misuse of information, noncompliance with personal data laws and regulations, and failure to recover from disasters. IT security policy should define organisational assets (i.e., data, equipment, and business processes) that need protection and link to procedures, tools, and physical access controls that protect such assets.

The governance structures at the executive level of an organisation should include policies, procedures,

and processes to manage and monitor the organisation's information security and privacy protections. These documents should communicate the mission priorities, available resources, and overall tolerance of information security risks. The organisation should also have a process in place to support compliance of information security activities with applicable information security and privacy laws, regulations, and guidance. Among other things, individuals with a responsibility for protecting systems and data should report to appropriate management and be appropriately trained.

Information security governance structures are defined in more detail in other reference materials, and this is not meant to be an exhaustive list of information security governance structures. Other key information security and privacy reference materials include

- ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. 2019.
- International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27001: 2013—Information technology—Security techniques—Information security management systems—Requirements*.
- National Institute of Standards and Technology. *NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations*, rev. 5. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>. September 2020.
- National Institute of Standards and Technology. *NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>. December 2018.

e. Business Growth Constraints

Inadequate or lack of IT planning may lead to business growth being constrained by a lack of IT resources or inefficient use of existing resources. A way to mitigate this risk is to develop and periodically update an IT strategy, which would identify resources and plans to meet future needs of the business.

f. Ineffective Resource Management

To achieve optimum results for minimum costs, an organisation must manage its IT resources effectively and efficiently. Ensuring that there are enough technical, hardware, software, and human resources with appropriate knowledge and experiences available to deliver IT services is the key factor in achieving value from investments in IT. Defining and monitoring the use of IT resources in a service level agreement,⁴³ for example, allows the organisation to objectively know if resources requirements are adequate to meet the business needs.

Leveraging workforce planning to ensure the availability of properly skilled staff helps to optimise human resource management. Using the strategies previously discussed for workforce planning will benefit the organisation by establishing the process and using it to identify key staffing and skill needs and devising strategies to meet these needs.

g. Inadequate Decision Making

Poor reporting structures may lead to inadequate decision making. This may affect the organisation's ability to deliver its services and may prevent it from meeting its objectives. Steering committees and other organisational groups with appropriate representation help in making decisions that affect the organisation.

h. Project Failures

Many organisations fail to consider the importance of IT governance. They take on IT projects without fully understanding what the organisation's requirements are for the project and how this project links to the

⁴³A service level agreement defines the specific requirements and responsibilities of the service provider and sets the customer expectations.

organisation's objectives. Without this understanding, IT projects are more susceptible to failure. It is also a common failure that acquired or developed applications do not fulfil minimum security and architecture standards. These projects may incur additional costs to maintain and administer non-standard systems and applications. A defined **system development life cycle** (SDLC) and its use in development and acquisition is a way to reduce the risk of project failures. See chapter 3 on IT development and acquisition for more information on SDLC methodologies.

i. Third Party (Vendor) Dependency or Service Delivery Problems by the IT Outsourcer

If no proper processes control the acquisition and the outsourcing process, the organisation might face a situation where it depends completely on one vendor or contractor. First, this is a high risk environment since if the vendor exits the market or fails to deliver the contracted services, the organisation is going to be in difficult position. Other risks include, for example, disputes over intellectual property, systems, personal data breaches, and databases. Organisations that outsource or regularly contract with vendors for solutions may need to have an outsourcing or acquisition policy that defines what may or may not be outsourced. It is also important for organisations to identify and manage supply chain risks when developing and acquiring IT products and services. See chapter 7 on information security for more information on supply chain management.

Effective contract oversight and monitoring will help address risks associated with dependency on a third party vendor. Contracts should define service level agreements and third party's access rights. Close monitoring of third party performance, including regular status updates and deliverable reviews, help to ensure the fulfilment of contractor responsibilities. When oversight and monitoring activities identify deficiencies in third party performance, the organisation can take corrective action.

Auditors and organisations should note that third party suppliers (to include cloud services and "back office" functions provided by third party suppliers) form part of the organisation's control environment. Therefore, the application and general controls operated by the third party may also be in scope of the IT audit, in addition to any controls such as monitoring and oversight of supplier's activities.

j. Lack of Transparency and Accountability

Accountability and transparency are two important elements of good governance. Transparency is a powerful force that, when consistently applied, can help fight corruption, improve governance, and promote accountability.⁴⁴ In the absence of adequate organisational structures, strategies, procedures, and monitoring controls, the institution may fail to be fully accountable and transparent.

k. Non-Compliance with Legal and Regulatory Statements

Stakeholders require increased assurance that organisations are complying with laws and regulations and conforming to good corporate governance practice in their operating environment. In addition, because IT has enabled near seamless business processes between organisations, there is also a growing need to help ensure that contracts include important IT-related requirements in areas such as privacy, confidentiality, intellectual property, and security.⁴⁵ The various policies that an organisation has, such as IT security, outsourcing, and human resource, must incorporate the relevant legal and regulatory frameworks.

l. IT Spending That Is Unknown, Excessively High, or Insufficient

Organisations often find that they are not aware of the full amount they spend on IT, or that IT spending is

⁴⁴International Organization of Supreme Audit Institutions, *INTOSAI-P 20, Principles of Transparency and Accountability*, p.5.

⁴⁵COBIT 5 Framework, Appendix E—Principle 5—Conformance.

higher than expected. This could be because there is not one centralised organisation or individual in charge of all IT-related spending, or because business units within an organisation may not classify IT-related costs appropriately. Best practices call for IT investment decision mechanisms (i.e., IT governance boards) to approve all IT-related spending. IT investment decisions should be made based on the portfolio of needs within an organisation. Without such oversight, the organisation may not be able to ensure that its IT priorities are being met.

In addition to the risk that an organisation may not know its full IT spending, or that its IT spending may be excessively high, an organisation may find that its IT budget is insufficient to meet new business needs or emerging threats. Many organisations find that most of their IT budgets are spent maintaining their existing systems and infrastructure. For example, organisations often spend significant portions of their IT budget on software licenses and related support and maintenance. Since the identification and utilisation of software licenses is not easy without appropriate tools and specialised knowledge, there is an increased risk that funds may be spent on unutilised software.

To better control IT spending, it is important for an organisation to define its IT business needs and goals, identify projects that are not contributing to meeting them, and make decisions based on the IT portfolio as a whole. For example, cloud computing is often cited as helping to reduce operational costs, however, depending on the service, configuration, and usage of the cloud service, cloud computing can be more expensive. Good IT governance should evaluate such new business models before they are undertaken.

m. Lack of an Implemented Software Process

The absence of software process implementation can create situations where purchased or developed software does not meet business needs and/or standards. The following situations may occur:

- acquisition/development of software that does not meet the needs of the organisation's business area,
- acquisition/development of software without quality check,
- development of software that is not implemented because it lacks standard quality,
- development of software that is incomplete or not in accordance with specifications, and
- interruption or non-completion of software development projects.

IV. References and Further Reading

Federal Court of Accounts of Brazil. *Get.it: Governance Evaluation Techniques for Information Technology: A WGITA Guide for Supreme Audit Institutions*. 2016.

ISACA. Whitepaper—*Privacy in Practice 2021: Data Privacy Trends, Forecasts and Challenges*. https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whppip. 2021.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. 2019.

ISACA. *COBIT 5 Framework: A Governance Framework for the Governance and Management of Enterprise IT*. 2012.

ISACA. *CISA Review Manual*, 27th ed.

ISACA. *Vendor Management Using COBIT 5*. 2016.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 38500:2015 Information Technology—Governance of IT for the Organization*. <https://www.iso.org/standard/62816.html>. February 2015.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure*

Cybersecurity, version 1.1. <https://www.nist.gov/cyberframework/framework>. April 2018.

Organisation for Economic Co-operation and Development. *G20/OECD Principles of Corporate Governance*. <http://www.oecd.org/corporate/principles-corporate-governance>. November 30, 2015.

U.S. Government Accountability Office. *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*. GAO-20-129. <https://www.gao.gov/products/gao-20-129>. October 30, 2019

U.S. Government Accountability Office. *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*. GAO-15-315. <https://www.gao.gov/products/gao-15-315>. March 31, 2015.

U.S. Government Accountability Office. *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23)*. GAO-04-394G. <https://www.gao.gov/products/gao-04-394g>. March 1, 2004.

CHAPTER 3: IT DEVELOPMENT AND ACQUISITION

I. What Is IT Development and Acquisition?

As the role of IT has become critical to achieving business objectives and providing increased capabilities to users, organisations have increasingly sought to modernise legacy solutions and to develop and acquire new IT solutions. New IT solutions can be achieved by internally developing them or externally acquiring them through contracting, or outsourcing (see chapter 5 for additional information on outsourcing). A combination of approaches is often utilised. Organisations should choose to develop or acquire IT solutions based on which approach best meets the needs of the organisation. Sometimes IT solutions are purchased and integrated with an organisation's existing solutions. Other times, new solutions are internally developed to compensate for a lack of functionality available on the market.

Regardless of whether the organisation is taking an internal or external approach to developing, acquiring, and implementing IT solutions, the process should be planned so that risks can be managed and chances of success are maximised. Additionally, the requirements for these solutions should be identified, analysed, documented, and prioritised. Organisations should also employ a quality assurance and test function to better ensure the quality of these solutions.

Solutions are commonly built or acquired by a project team structure. Although sometimes organisations may not formalise a project, they still need to accomplish common key activities associated with planning and executing a development or acquisition process (e.g., requirements identification and risk management).

According to the Software Engineering Institute's *Capability Maturity Model® Integration (CMMI) for Acquisition*, version 1.3, organisations are increasingly acquiring capabilities since products and services are readily available and it is typically cheaper than developing them in-house. However, the risk of acquiring products that do not meet the business objective or fail to satisfy the users is very real. These risks need to be managed in order for an acquisition to successfully meet the business objectives and mission. When done in a disciplined manner, IT acquisitions can improve an organisation's operational efficiencies by leveraging suppliers' capabilities to deliver quality solutions rapidly, at lower cost, and with the most appropriate technology.

Acquiring a product or solution requires that the organisation has an understanding of its business needs and requirements as identified through its IT governance process (see chapter 2 for more information on IT governance and management). The requirements identification process should include all relevant stakeholders (process owners) who are involved in the business process, such as end users and technical staff who may need to eventually maintain and support the system. When acquiring services (e.g., helpdesk and desktop automation) requirements identification should include the IT department that will interface with the service provider. Requirements must be prioritised so that, if the project experiences a budget shortfall or other cost constraints, certain requirements can be deferred to future builds or acquisitions as appropriate.

The IT development and acquisition process comes with a number of management responsibilities. Organisations often employ a SDLC methodology to provide a project management structure and assist with fulfilling those responsibilities. There are typically five phases in SDLC: (1) initiation, (2) development and acquisition, (3) implementation, (4) operation and maintenance, and (5) disposal. SDLC methodologies are discussed in more detail in the subsequent section.

a. Project Methodologies

There are several different SDLC methodologies that can be used to develop IT systems, which range from the traditional waterfall model to the spiral model and to iterative models, such as the Agile model.

- The **waterfall model** begins with requirements development and continues sequentially through other phases—design, build, and test—using the output of one phase as the input to the next to develop a finished product at the end. This model allows the status of a development project to be easily identified and tracked based on the current phase of the project.
- The **spiral model** uses a risk-based approach to incrementally build a system by cycling through the four development phases. Using this model, each spiral, or incremental cycle, typically starts by determining the development objectives and scope for the increment. Next, alternative solutions are evaluated and risk management techniques are employed to identify and reduce risks. Then, a product for the increment (such as a prototype) is developed. Finally, the product is evaluated to determine whether the increment's initial objectives have been met.
- The **Agile model** focuses on short-duration, small-scope development phases that produce segments of a functional product. This model operates with similar phases to the traditional waterfall model—requirements, design, build, and test—but uses a shorter development cycle to achieve multiple iterations in similar time frames. Shorter, more incremental approaches to IT development have been identified as having the potential to improve the way IT is developed and implemented.⁴⁶

There are other frameworks that are related to Agile and use many of the same principles and practices. Two examples include:

- The **DevOps model** emphasizes collaboration between development, IT operations, and quality assurance with the goal of more frequent software releases. The overall DevOps values align with agile, and DevOps is considered an expansion of agile implementation practices to all areas of a product's life cycle.
- **Iterative development** breaks down work into smaller chunks known as iterations, in order to design, develop, and test in cycles.

According to the Software Engineering Institute's *CMMI for Development*, version 1.3, when establishing an organisational development and acquisition methodology, the organisation should define and maintain requirements and guidelines that can be tailored for a particular project. These requirements and guidelines should be based on the development model chosen and other issues, such as customer needs, cost, schedule, and technical difficulty.

Although organisations may select from a variety of project methodologies, there are key best practices that, when adopted, raise the likelihood of success in the development and acquisition of products or services. These include, for example, requirements development and management, risk management, project management, testing, vendor oversight (both during acquisition and later if they operate or support the system), and internal training. These areas are discussed in more detail in the subsequent section.

Regardless of the chosen project methodology, however, proper documentation is an important factor. In addition, attention should be paid to ensure that the documentation is also available after development has been completed. In situations where an organisation relies on a developer solution to communicate requirements, harmonize user records, and monitor development, it is common for documentation to be inaccessible after the end of development, making it challenging for organisations to trace the extent and compliance of that which has been produced.

II. Key Elements of IT Acquisition and Development

a. Conduct a Feasibility Study

Although there are project methodology interpretations that use different phases and different names,

⁴⁶For more information on the Agile model, see U.S. Government Accountability Office, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*, GAO-20-590g, (Sept. 28, 2020), <https://www.gao.gov/products/gao-20-590g>.

organisations may consider a feasibility study phase as an initial step, prior to the definition of requirements. A feasibility study can help to analyse the benefits and solutions for the identified problem area. The objectives of the feasibility study are to

- clearly identify the need;
- determine an optimum alternative risk-based solution (e.g. whether to develop or acquire);
- define the time frame for the implementation of the solution;
- determine the approximate cost to develop/acquire; and
- determine whether the solution fits the business strategy.

The result of the study should be a comparative report that shows the results of criteria analysed (e.g., costs, benefits, risk, resources required and organisational impact) and recommends one of the alternatives/solutions and a course of action (e.g., whether to develop or acquire a system).

b. Requirements Development and Management

When acquiring or developing new software or modifying existing information systems, project teams and developers must define the requirements and must also manage changes to those requirements. Requirements establish what the system is to do, how well it is to do it, and how it is to interact with other systems. Well-defined and managed requirements are the foundation of effective system development and acquisition efforts. The Software Engineering Institute's *CMMI for Development*, version 1.3, identifies leading practices in four areas related to developing and managing requirements:

- **Develop customer requirements.** Collect stakeholder needs, expectations, constraints, interfaces, and all automation (digitisation) requirements managed centrally by IT department or with significant involvement of IT department and translate them into customer requirements;
- **Develop product requirements.** Refine and elaborate customer requirements to develop product and product component requirements;
- **Analyse and validate requirements.** Verify usability of existing IT assets (including application software) if any; analyse and validate the requirements with respect to the end user's intended environment; and
- **Manage requirements.** Manage requirements and identify inconsistencies with project plans and work products.

According to the Software Engineering Institute, organisations should also establish and maintain plans that outline the processes for performing and achieving these leading practices for requirements and that set and reinforce expectations for relevant stakeholders. The Software Engineering Institute recommends having a documented and disciplined process for developing and managing requirements to reduce the risk of developing a system that does not meet user needs, cannot be adequately tested, and does not perform or function as intended.

c. Risk Management

Effective development and acquisition requires any organisation to identify, prioritise, and manage risks throughout each phase of the SDLC. When problems are identified, risk-handling activities can be planned and invoked as needed across the life of a project in order to mitigate adverse impacts on objectives. Effective risk management involves early and aggressive risk identification through the collaboration and involvement of relevant stakeholders. Based on the Software Engineering Institute's CMMI, risk management activities can be divided into four key areas:

- **Preparing for risk management.** Preparation is conducted by establishing and maintaining a strategy for identifying, analysing, and mitigating risks. The risk management strategy addresses the specific actions and management approach used to apply and control the risk management programme. It also includes identifying and involving relevant stakeholders in the risk management process. Activities associated with preparing for risk management include, for example, developing risk management requirements and a risk management strategy.

- **Identifying and analysing risks.** Identifying risks from the internal and external sources and then evaluating each identified risk to determine its likelihood and consequences. Analysing risks includes risk evaluation, categorisation, and prioritisation, and is used in determining when appropriate management attention is required. Activities associated with identifying and analysing risks include, for example, developing a list of identified risks and assigning a category, a priority, and source to each risk.
- **Mitigating risks.** Mitigating risks involves developing techniques and methods used to avoid, reduce, and control the probability of occurrence of identified risks. Plans for risk mitigation should be developed for the most important risks to the project. The status of each risk should be monitored periodically to determine whether established thresholds have been exceeded and risk mitigation plans should be implemented as appropriate. Activities associated with mitigating risks include, for example, developing risk mitigation plans and contingency plans.
- **Executive oversight.** The primary activities associated with executive oversight are reviews of project risk status held on periodic and event-driven bases with appropriate levels of management to provide visibility into the potential for project risk exposure and appropriate corrective actions. See chapter 2 for more information on the role of executive oversight in guiding IT activities within organisations.

d. Project Management and Control

Project management includes defining the project plan and control activities. Project management also includes defining cost and schedule baselines, defining project schedules, and involving stakeholders for key activities. Project control involves supervision and periodic reporting to take corrective actions when the performance of the project is not in accordance with the plan. For example, if the cost of the project rises substantially, the organisation may choose to cut certain functions after consultation with stakeholders to contain the cost.

A project management structure should be described in the organisation's SDLC approach or acquisition strategy as appropriate. Generally, the project management structure consists of a project manager, risk officer, quality assurance and configuration management support staff, and personnel from the testing group if not part of quality assurance. The project plan serves as the basis to guide all activities. Periodic briefings to senior management keep them aware of the status of the project and how risks are being managed. In addition, it lets them weigh in on trade-offs involving cost, schedule, and performance since it is rare that a project will meet all of its intended objectives in these areas.

e. Design/Development

Based on the requirements defined, a design should establish a baseline of system and subsystem specifications that describe the parts of the system, including how they interface and how the system will be implemented using the chosen hardware, software and network facilities. Generally, the design also includes programme and database specifications and will address any security considerations. Afterwards, during development, the design specifications are used to begin programming and formalising supporting operational processes of the system.

Over the years, business application development has occurred largely using traditional SDLC phases. As purchased packages have become more common, the design/development phases of the traditional life cycle are being replaced with the **solicitation**⁴⁷ phase.

As a result, when acquiring IT solutions, organisations often use a solicitation (request for proposal) package. Solicitation is the process of documenting the requirements of the business and collecting other reference materials that will assist the vendor in providing the IT solution. It includes generating the solicitation package and putting it out for tender, getting proposals, and selecting among the various vendors. The selection process should be transparent, objective, and based on criteria that are appropriate

⁴⁷Also referred to as selection and acquisition.

for the system or services being acquired. It is critical that the project team involve its legal department in this process. The legal team is aware of laws and regulations, and can assist with ensuring that the vendor selection criteria is fair and will be upheld in a court of law if other losing vendors contest the award.

f. Quality Assurance and Testing

Quality assurance provides project staff and management insight into the interim and final work products' quality and functionality. To do this, personnel involved in quality assurance should establish a quality assurance framework, a well-documented system user manual, and periodically evaluate the work products to see that they meet the organisation's documented quality standards and whether the staff have followed the requisite processes to develop the products. Organisations need to verify that the developed or acquired product meets the requirements, meets the acceptance criteria (e.g., less than a certain number of non-critical errors) and has undergone testing (functional, system integration and user acceptance) with user and stakeholder involvement.

The quality assurance staff should also ensure that the adopted and agreed development methodology is being followed and that the requisite oversight is being conducted. For example, they should ensure that reviews (formal or informal) are conducted and the necessary status reports are sent to appropriate stakeholders and management. Further along in the quality assurance process, quality assurance staff and senior management should assess whether the project team is following internally-set policy and procedures for the acquisition or development effort. Senior staff oversight should be evident at key stages of the acquisition or development cycle.

g. Configuration Management

Configuration management is used to ensure that the integrity of documents, software, and other descriptive or support materials that are part of the system being developed or acquired are maintained. Changes to these materials (also called work products) are managed and baselines (or versions) are established such that the organisation is able to revert back to known and tested versions as needed.

Organisations may use a configuration control board to assist with configuration management activities. A configuration control board is a group of qualified configuration management personnel who are involved in approving or authorising software for installation into the production environment. Typically this is done after user testing and any additional testing needed to ensure that other systems continue to operate as before once the new system or software is installed (e.g., integration testing⁴⁸ or regression testing).⁴⁹ It is important to include the integration with existing systems and related regression testing in the outsourcing agreement with the developer. It is also important to ensure configuration management not only in the production environment, but also in the test environment during development.

III. Risks to the Audited Organisation

When an organisation is developing in-house software, it faces a number of risks or challenges in ensuring project success. Some of these risks related to skills in the software domain, experience in testing and project management, having reasonable cost and benefits estimates, and being able to monitor and track the project status. For example, problems can arise due to the misapplication of agile software development processes and methods. These problems can include not defining key agile roles, prioritising system

⁴⁸Integration testing is the phase in software testing in which individual software modules are combined and tested as a group. It typically occurs after unit testing and before validation or acceptance testing.

⁴⁹Regression testing is a type of software testing that verifies that software that was previously developed and tested still performs correctly after it was changed or interfaced with other software. These changes may include software enhancements, patches, and configuration changes. During regression testing, new software bugs or regressions may be discovered.

requirements, or implementing automated capabilities.

Additionally, the software or system requirements gathering, testing, and approval should include all end users (e.g., internal and external users), and auditors should look at whether the users were consulted in the definition of the requirement. Auditors should also look at whether personnel involved in the quality assurance area are being independent and objective in their assessment of the quality of the system as it is being developed. As in acquisition, management needs to be briefed periodically on the status of the project and should take corrective action as appropriate.

The primary focus for auditors when faced with an organisation that has undertaken acquisition of a system (or product) is to determine whether they are managing the vendor and getting periodic reports of status and taking corrective action. In order to do this, the contract needs to specify key milestones during the development and implementation where there are formal review and status reports that provide the agency with cost, schedule, and performance information. The auditor will need to ensure that agency management or designated personnel are receiving, reviewing and taking corrective action on status reports and contract activities as appropriate.

An IT auditor should also review whether

- proper project planning is performed, including effective estimates of resources, budget, and time;
- the decision to develop/acquire was appropriate;
- the system's objectives and requirements were achieved;
- the cost and benefits identified in the feasibility study are being measured, analysed and accurately reported to management;
- scope creep was controlled, and
- periodic review and risk analysis were performed in each project phase.

IV. References and Further Reading

Chief Information Officers Council. *Resource Library: Publications, Playbooks, Guidance, and More*. <https://www.cio.gov/resources/>.

Defense Contract Audit Agency. *DCAA Contract Audit Manual*. <https://www.dcaa.mil/Guidance/CAM-Contract-Audit-Manual/>.

ISACA. *BAI01-BAI10 Manage—Audit Assurance Program*. 2014.

ISACA. *CISA Review Manual, 27th ed*. 2019.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. 2019.

ISACA. *System Development and Project Management Audit Program*. 2009.

National Institute of Standards and Technology. *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View*. <https://csrc.nist.gov/publications/detail/sp/800-39/final>. March 2011.

Software Engineering Institute. *CMMI for Acquisition*, version 1.3. <http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm>. 2010.

Software Engineering Institute. *CMMI for Development*, version 1.3. <http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm>. 2010.

Tsui, Frank and Orlando Karam. *Essentials of Software Engineering*, 2nd ed. 2011.

U.S. Government Accountability Office. *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation*. GAO-20-590G. <https://www.gao.gov/products/gao-20-590g>. September 28, 2020.

U.S. Government Accountability Office. *Census Bureau Needs to Implement Key Management Practices*. GAO-12-915. <https://www.gao.gov/products/gao-12-915>. September 18, 2012.

CHAPTER 4: IT OPERATIONS

I. What Are IT Operations?

While there are many different interpretations or definitions of IT operations, it is generally thought of as the day-to-day tasks involved in running and supporting the IT infrastructure of an organisation (e.g., running servers, conducting maintenance, monitoring security, providing necessary storage, and running a helpdesk). The operations are measured and managed using **key performance indicators** (KPI) for IT operations that set parameters against which operational effectiveness can be measured. These measures or their equivalent should be continuously monitored and reviewed periodically. Most organisations document these in an agreement between the business users and the IT organisation. The **service level agreement** (SLA) is one formal agreement, where these parameters and other arrangements are documented. This is discussed in more detail throughout this chapter.

II. Key Elements of IT Operations

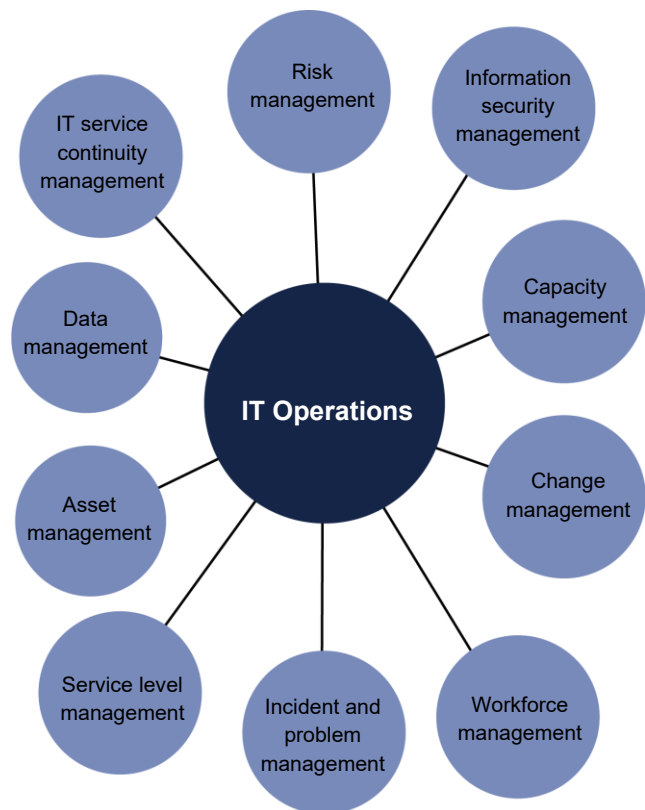
Elements of IT operations that the auditor should review to determine whether the organisation is effectively managing IT operations include, for example, IT service continuity management, information security management, capacity management, workforce management, incident and problem management handling procedures for ensuring continuity of operations, change management practices, and risk management (see fig. 8). These and other areas are defined in the Information Technology Infrastructure Library (ITIL) framework,⁵⁰ one of the more widely adopted frameworks for identifying, planning, delivering, and supporting IT services to the organisation business.

To determine whether the audited organisation is effectively delivering the documented services, the auditor should assess whether the SLA includes the specific parameters for the various services. There might be instances in smaller organisations where instead of an SLA, the agreement between the organisation and the IT group may be documented in an organisational chart or other document. Regardless of what the document is called, the parameters for delivering IT services must be documented and agreed to by the user' groups and the IT organisation.

a. IT Service Continuity Management

The purpose of continuity management is to maintain the appropriate ongoing business continuity requirements, as well as reduce downtime costs and business impacts during disaster-level incidents. The

Figure 8: Domains of IT Operations



Source: Unknown.

⁵⁰Axelos, "What is ITIL?," <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>.

IT organisation accomplishes this by setting recovery time (how long it takes to recover) and recovery point (from what point before the disaster) targets for the various IT components that support the business processes with the goal of maintaining service availability and performance at the highest possible levels. Additionally, continuity management includes periodically reviewing and updating recovery times and points to ensure that they are kept aligned with business continuity plans and business priorities. This area is addressed in more detail later in chapter 6.

b. Risk Management

Risk management is the practice to ensure that an organisation fully understands and addresses any risks to the organisation, including those related to IT operations. Risk is defined as problems that should be minimised or mitigated to avoid impact on the organisation's ability to deliver value to its stakeholders. Risks to IT operations include unauthorised system activity or behaviour, unauthorised disclosure of personally identifiable information, and unauthorised changes, among others. The risk management practices and procedures an organisation implements will guide the organisation's risk-related decisions. As discussed earlier, practices and procedures for risk management can be divided into four key areas: (1) preparing for risk management, (2) identifying and analysing risks, (3) mitigating risk, and (4) executive oversight. See chapter 3 for additional information on each of the four key areas.

c. Information Security Management

The management of information security relates to managing security-related risks, ensuring the implementation of information security controls, taking action as appropriate, and ensuring that information is available, usable, complete, and uncompromised when needed. It also relates to ensuring that only authorised users have access to the information and that it is protected when being transferred between destinations and trusted when it arrives. This area is addressed in more detail later in chapter 7.

d. Capacity Management

Capacity management includes managing the various services that support the organisation in a manner that keeps up with the demands of the organisation or users. Optimising network throughput capacity, resource availability, storage optimisation, and demand forecasting are part of capacity management. In order to manage capacity, the IT organisation needs to measure current conditions and needs to take action that facilitates providing users with additional capacity; for example, this can be accomplished by acquiring additional processing power when certain parameters are crossed (i.e., when computer utilisation is at 75 percent or greater for 60 percent of the workday).

e. Change Management

In IT organisations, the change management process is normally used to manage and control changes to the IT systems and their components, such as software, hardware, and related documentation. Change controls are needed to ensure that all changes to system configurations are authorised, tested, documented, and controlled so that the systems continue to support business operations in the manner planned, and that there is an adequate trail and record of changes.⁵¹

When implementing changes, it is important that there are segregation of development, test, and production environments and that the developers of the change are not permitted access to the production environment. This reduces the risk that untested or unapproved changes are made directly in the production environment.

⁵¹Certain IT system changes may not require all of the procedures provided in this section. For example, **standard changes** are usually very minor and low risk to IT systems and consequently may have appropriately less oversight (e.g., no need for a change board approval, but still require testing and operational sign off).

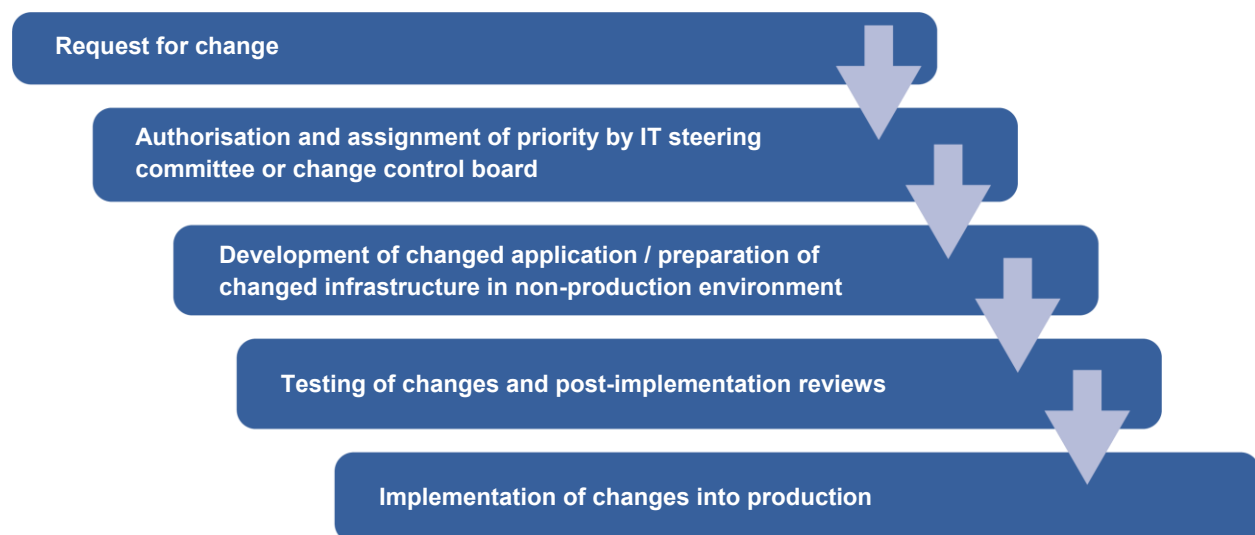
An unapproved or accidental change could have severe risks to business continuity and financial consequences for an organisation. Organisations should follow a defined change management procedure that requires approval from a board before being implemented into the operational environment. The change management process should ensure that changes are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented, and reviewed in accordance with the documented and approved change management procedures.

Changes can be identified and initiated by, for example, a change in the business environment, modification of the business model, inter-operational needs, or by the outcome of incident or a problem analysis. Change control procedures should include procedures for:

- management authorisation (e.g., documenting a process for recording a request for change),
- thorough testing and authorisation by operations management before use in live environment,
- management review of the effects of any changes,
- maintenance of adequate records,
- preparation of fall-back plans (in case anything goes wrong), and
- establishing procedures for emergency changes.

See figure 9 for steps in a change management process.

Figure 9: Steps in Change Management



Source: Unknown.

The cost of the change, the impact on the IT system and business objectives, the effect of not implementing, and future resource requirements are significant determinants in authorising and prioritising change.

Emergency changes are changes that cannot wait to go through the normal change control procedures and must be implemented with minimum delay. There is reduced time for making and testing such changes, which creates higher risk of errors and programming mistakes.

Where emergency change procedures exist, the auditor should check that they are reasonable and include some form of control. These would include emergency change approval by a member of staff with the appropriate authority, having appropriate version naming and control along with audit trail (i.e., use of automated change control applications), retrospective approval from the change board or system owner, retrospective testing, and documentation update.

f. Workforce Management

Workforce management is intended to ensure that an organisation has the right people with the appropriate skills and knowledge in the correct roles to support the organisation. For an IT organisation providing services to the business, workforce management is effective when suitably qualified and trained IT organisation personnel are deployed, sufficient resources and appropriate tools are engaged to handle network monitoring and help desk functions, and the personnel engaged are proactively engaged in addressing bottlenecks while remaining responsive to business needs. As discussed in chapter 2, organisations should regularly assess their workforce needs (e.g., competency and staffing requirements), assess gaps, and develop strategies and plans to address those gaps, among other key activities.

g. Incident and Problem Management

Incident management is the systems and practices used to determine whether incidents or errors are recorded, analysed, and resolved in a timely manner. Problem management aims to resolve issues through investigation and in-depth analysis of a major or recurring incident in order to identify the root cause. Once a problem has been identified and analysis of the root cause has been conducted, it becomes a known error or inefficiency, and a solution can be developed to address it and to prevent future occurrences of related incidents.

A formal process should be put in place for the documentation of conditions that could lead to detection and identification an incident. The IT operation section of the SLA should have documented procedures for detecting and recording abnormal conditions. To facilitate analyses of these abnormal conditions, organisations often maintain logs of all incidents. A manual, or automated log of dedicated IT software may be used to record these conditions. Examples of incidents could include unauthorised user access or intrusion (security), network failures (operational), low functionality of software (service delivery), or lack of end user skills (training).

In the audit of incident and problem management, the auditor should examine incident/problem reports and logs to ensure that they are resolved in a timely manner and are assigned to individuals or groups most capable of resolving the incident/problem. In some cases, disaster recovery plans may be invoked to resolve an incident. See chapter 6 for more information on disaster recovery plans and chapter 7 for information security incident management.

h. Service Level Management

As mentioned earlier, the SLA documents the various parameters that the IT organisation uses to provide service to the business. The parameters in the SLA are generally agreed to by the business owners and the IT organisation. The auditor will use the parameters in the SLA to see whether the IT organisation is meeting the service levels and whether the business owners are satisfied and taking appropriate action if there are deviations from the agreed service level parameters. These parameters include quantifiable metrics such as availability, utilisation, or number of errors. Generally, there is also an SLA or other formal agreement between an IT organisation and its vendor(s). For example, an IT organisation may have multiple SLAs with the various vendors who provide outsourcing or cloud computing services.

Some organisations may also have an agreement between the IT organisation and the business customers within the organisation, which is referred to as an Operational Level Agreement (OLA). OLAs are similar in content to SLAs described above but are internal agreements that a service provider would define to describe how they would meet SLAs. An OLA could contain information such as response time for addressing incidents, or availability of servers. In general, OLAs are used to represent internal relationships between an IT service provider and another part of the organisation.

The SLA and OLA contains, among other items, the KPIs for the IT services. Review of KPIs will assist the auditor to ask questions related to

- whether the systems are operating as per the documented agreements;

- whether mechanisms are in place for identifying gaps in performance or security, addressing gaps identified, and following up on the implementation of corrective action taken as a result of evaluating of the organisation's performance; and
- identifying control issues in the organisation entity being audited thereby helping to determine the nature, timing, and extent of testing.

For example, KPI measures and the corresponding definitions and goals for change management are given below:

Process	Goal (Critical Success Factor)	Key Performance Indicator	Measurement Architecture
Change management	Reduce incidents caused by unintended changes	Percentage reduction in the number of incidents resulting from unauthorised access	Tracked through incident management, change management, and reported monthly

In cases where the KPIs may not be providing a means for an organisation to effectively evaluate progress and achievement of goals, the auditor may want to conduct further assessment of the KPIs. When assessing KPIs, an auditor should determine whether they contain important attributes that will help make them effective in monitoring progress and determining how well an organisation or vendor is achieving its goals. Some examples of these attributes include the following:

- **Clarity.** The measure is clearly stated, and the name and definition are consistent with the methodology used to calculate it.
- **Measurable target.** The measure has a numerical goal; the measure is quantifiable or has quantifiable targets or other measures that permit expected performance to be compared with actual results.
- **Objectivity.** The measure is reasonably free from significant bias or manipulation that would distort the accurate assessment of performance.
- **Reliability.** The measure produces the same result under similar conditions.
- **Baseline and trend data.** The measure has baseline and trend data associated with it to identify, monitor, and report changes in performance and to help ensure that performance is viewed in context.
- **Linkage.** The measure is aligned with division and organisation-wide goals and missions and is clearly communicated throughout the organisation.⁵²

There may be cases where the IT organisation has outsourced the bulk of its functions to a vendor. In such a case, the IT organisation is the liaison between the vendor and the users and is responsible for managing the vendor to ensure that business needs are met. See chapter 5 for more information on outsourcing.

i. Asset Management

Asset Management the process of identifying and creating an inventory of assets of either tangible or intangible value that is worth protecting and includes people, information, infrastructure, finances and reputation. An asset cannot be effectively protected or managed if, for example, it is not identified. In addition, asset management allows for organisations to ensure its assets are maintained, upgraded, and disposed of properly. In the past, assets were easier to control as they were often managed within the organisation's domain, but organisations now outsource services and assets. Some benefits of asset management include improving utilisation, eliminating waste, enabling productivity, and supporting business continuity management.

⁵²For more information on key attributes of KPIs, see U.S. Government Accountability Office, *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*, GAO-17-183, (Mar. 16, 2017), <https://www.gao.gov/products/gao-17-183>.

j. Data Management

Data management is the practice of managing and securing data as a valuable resource for an organisation. Managing data requires the organisation to collect, store, and secure data as well as access, integrate, and clean the data for analysis. Organisations collect data from many resources, such as transactional systems, scanners, sensors, social media, and smart devices, among others. The organisation can use the data collected to help make decisions and create value. Data management includes activities such as:

- creating, accessing, and updating data
- storing data across multiple facilities and clouds
- ensuring high availability and disaster recovery
- using data to support applications, analytics, and algorithms
- ensuring data privacy and security
- disposing of data in accordance with applicable laws and regulations

Data management systems are used by organisations to manage the data needed to support the organisation's analytics and algorithms. While organisations should have automated tools help manage these systems, database administrators will still need to be present for manual intervention.

To better manage an organisation's data, the organisation might implement data governance practices. Data governance is a framework for managing an organisation's data. Organisations need to define the policies and procedures for how they will manage data throughout the entire lifecycle of the data. Data governance will help organisations protect their data by documenting data assets and access controls, defining data ownership and responsibilities, and defining distribution policies internally and externally. Other functions of data management include

- **data architecture management**, which defines the data needs of the organisation.
- **data development**, which designs, implements, and maintains solutions to meet the data needs of the organisation.
- **data operations management**, which plans, controls, and provides support for structured data throughout the entire lifecycle of the data.
- **data security management**, which executes security policies and procedures to ensure the confidentiality, integrity, and availability of data.
- **data warehouse and business intelligence management**, which provides processes to make decisions to support data reporting, query, and analysis.

III. Risks to the Audited Organisation

The main tools for the auditor, as noted previously, are the SLA and OLA. These agreements lay out the parameters, performance indicators, and requirements which the IT organisation must be measured against. If these documents are lacking or not formally reviewed and approved by the business (process) owners, the organisation's IT resources may be at risk of not being used effectively or efficiently. After getting the SLA and OLA, the auditor will need to get periodic reports from the IT organisation that measure and report on the status of the indicators as well as management review of the same and any actions items or directions to the IT organisation when there are significant deviations from the agreed parameters.

In the area of change management, the auditor should check to see whether there are change control procedures in place that ensure the integrity of the system and they ensure that only approved and tested applications are introduced into the operational environment.

The auditor should also be concerned about how the agency is managing capacity (e.g., storage, CPU, and network resources) in a proactive manner to be responsive to the users and managing incidents and other security issues so that the business functions are not compromised.

IV. References and Further Reading

Atlassian. *What Is IT Asset Management (ITAM)?* <https://www.atlassian.com/itsm/it-asset-management>. 2022.

Axelos. *What is ITIL?* <https://www.axelos.com/best-practice-solutions/itil/what-is-itil>.

Axelos. *ITIL Foundation: ITIL 4 Edition (ITIL 4 Foundation)*. Norwich: TSO, 2019.

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarone. *NIST Special Publication 800-61, rev. 2: Computer Security Incident Handling Guide*. <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>. 2012.

CISA. *Item Development Guide*. https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/cisa/cisa-item-development-guide_bro_eng_0219.pdf. October 2018.

Cisco. *Service Level Management: Best Practices White Paper*. <https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15117-sla.html>. October 4, 2005.

DAMA International. *Data Management Body of Knowledge*, 1st ed. <https://www.dama.org/cpages/body-of-knowledge>. 2010.

ISACA. *Change Management Audit Programme*.

ISACA. *CISA Review Manual*. 27th ed. <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KokCEAS>. ISACA, 2011.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. 2019.

Knight, Michelle. *What is Data Governance?* <https://www.dataversity.net/what-is-data-governance/>. December 18, 2017.

Oracle. *What Is Data Management?* <https://www.oracle.com/database/what-is-data-management/>.

Profisee. *Data Governance—What, Why, How, Who & 15 Best Practices*. <https://profisee.com/data-governance-what-why-how-who/>.

SAS. *Data Management: What It Is and Why It Matters*. https://www.sas.com/en_us/insights/data-management/data-management.html.

U.S. Government Accountability Office. *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*. GAO-20-129. <https://www.gao.gov/products/gao-20-129>. October 30, 2019.

U.S. Government Accountability Office. *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Visibility Initiatives*. GAO-17-183. <https://www.gao.gov/products/gao-17-183>. March 16, 2017.

CHAPTER 5: OUTSOURCING

I. What Is Outsourcing?

Outsourcing is the process of contracting an existing business function or service that an organisation previously performed internally or contracting a new business function or service to an outside entity. The contracted entity is responsible for providing the contractually required services for an agreed fee. An organisation may choose to outsource selected parts (or all) of its IT infrastructure, services, or processes. The organisation should have a policy or vision on what business functions (typically IT but could be others) it outsources and which functions it will keep in-house.

a. Advantages of Outsourcing

Outsourcing offers certain advantages, which include:

i. Staffing flexibility

If a project requires skills that the organisation does not currently have, the organisation may decide to outsource the project instead of training internal staff—to save time and cost of training. In addition, outsourcing will allow operations that have seasonal or cyclical demands to bring in additional resources when an organisation needs them, and release them when the seasonal operations are over. This can be especially beneficial in volatile markets where staffing flexibility and scalability can reduce risk.

ii. Cost reduction

Outsourcing typically results in cost reduction by shifting labour and other costs to a vendor that has lower labour costs. IT organisations look to outsource tasks that would be more costly to complete in-house. An example of this type of task would be a software-related task requiring specialised skills. Organisations that do not have employees qualified to complete this task can benefit financially by outsourcing this task. Outsourcing of non-core operations also helps the organisation to focus on its core business and deliver results efficiently.

iii. On-call experts

Outsourcing enables the organisation to have on-call experts waiting to assist with existing or emerging issues. The organisation is able to quickly respond to changing business needs (e.g., new missions or taking on additional functions) with the help of the expert. In addition, experts can assist internal staff working alongside the vendor by providing hands-on training and knowledge transfer.

iv. Risk mitigation

Especially in volatile markets, organisations may look to mitigate risk by increasing their levels of outsourcing. For example, organisations can decrease the IT resources and staff maintained by the organisation and, in turn, outsource these capabilities to allow greater flexibility and scalability in ever changing environments. IT organisations may decide to outsource all or some of their operations and, depending on the criticality of the outsourced service, an organisation can decide to go with greater or lesser formal controls on the outsourced service. It is critical to remember that the organisation retains ultimate responsibility for the provision of those functions or services, as it has transferred the function, not the responsibility.

b. Examples of Outsourcing

According to ISACA,⁵³ organisations can outsource various areas of business and IT infrastructure. For example:

- Operating infrastructure that may include data centre and related processes
- 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

One of the most commonly outsourced IT services today is **cloud computing**. Cloud computing is a model for enabling on-demand network access to a collection of configurable computing resources (e.g., applications, networks, servers, storage, and other services). Among other benefits, cloud computing can enable organisations to access computing resources on a pay-per-use basis and provide flexibility in being able to rapidly scale an IT solution.

As an example, an organisation can outsource data processing or another service to computing resources owned by the vendor. The vendor typically hosts the equipment, while the organisation still has control over the application and the data. Cloud computing may also include utilising the vendor's computers to store, back-up, and provide online access to the organisation's data. The organisation will need to have a robust access to the internet if it wants its staff or users to have ready access to the data or even the application that processes the data. In the current environment, the data or applications are also available from mobile platforms (i.e., laptops with wireless internet connections or cell/mobile cards, smart phones, and tablets).

Cloud computing is often categorised into three separate service models:

- **Software as a service**—The organisation uses an application and infrastructure provided by the vendor.
- **Platform as a service**—The organisation uses the cloud infrastructure provided by the vendor to run applications owned by the vendor.
- **Infrastructure as a service**—The organisation outsources various computing resources to a vendor such as processing, storage, and networks from a vendor. The organisation does not manage the infrastructure, but controls the application and operating system used.

In addition to the different service models, there are four separate deployment models:

- **Private cloud**—The infrastructure is provisioned for exclusive use by a single organisation.
- **Community cloud**—The cloud infrastructure is provisioned for a community of consumers that often have shared considerations, such as a mission, security, and compliance considerations.
- **Public cloud**—The infrastructure is provisioned for open use by the general public and is typically operated by a business, academic, or government organisation.
- **Hybrid cloud**—The infrastructure is a composition of two or more of the infrastructures previously noted that are interoperable to enable data and applications portability.

Proper cloud configuration can reduce the risk of security concerns and applying additional security controls can create a defensible cloud environment. In addition, cloud computing contracts should include a clause related to non-disclosure of sensitive data and need to define what constitutes a breach of security and describe how the vendor will notify the organisation of a breach.

In summary, cloud computing can deliver benefits to an organisation, such as cost containment, immediate provisioning, dynamic flexibility and scalability, and backup solutions to limit downtime. However, like all outsourcing, cloud computing has risks and challenges when implemented. For example, cloud computing can introduce additional risks, such as misconfiguration, misunderstanding shared responsibilities, poor access controls, shared cloud resources with other tenants of the cloud service provider, and supply chain

⁵³Outsourced IT Environments Audit /Assurance Programme (2009).

vulnerabilities. The flexible costing model of cloud computing can also become very expensive if the organisation does not monitor and control its use.

II. Key Elements of Outsourcing

a. Outsourcing Policy

Organisations need to have a policy that defines what functions can be outsourced and what functions must remain in-house.⁵⁴ Organisations typically outsource routine IT operations, maintenance, and desktop hardware platforms. Human resources and personnel records are generally in-house functions as these require close monitoring and are subject to many privacy and security requirements that may not make them cost effective to outsource.

An auditor should begin with reviewing the outsourcing policy and procedures of an organisation. It is essential that bigger organisations, which often have a large share of their business operations outsourced, have an approved outsourcing policy that includes clearly defines outsourcing processes. Smaller organisations may not have a formal policy but should follow efficient and transparent solicitation procedures. Regardless of size, organisations must have a clear governance strategy in order to set the direction and objectives for outsourcing.

b. Solicitation

Solicitation is the process of documenting the requirements of the system and collating other reference materials that will assist the vendor in building the system. It includes generating the solicitation package and putting it out for bid/tender, getting proposals, and making a selection among the various vendors. The selection process should be transparent and objective and based on criteria that are appropriate for the system or services being acquired. Before making the final decision, the organisation should thoroughly review the potential vendor for any potential issues or impediments to delivering the service.

c. Vendor Management

Vendor management is a key element of outsourcing to ensure that the services are rendered according to the expectations of the organisation. The organisation should have processes in place to ensure periodic follow-up regarding the status of the project, quality of service, and testing of built products prior to introduction into the operational environment. Additionally, as a part of the vendor monitoring process, the organisation may also audit the vendor's internal quality assurance process to ensure that vendor personnel are following contractually-approved policies and plans for all of their work.

An important component of vendor management is the SLA. As mentioned earlier, the SLA is a documented agreement between the organisation and the vendor and is a key tool to managing vendors. The SLA should define the services the vendor is expected to perform as well as the technical parameters for those services since it is a legally binding agreement between the vendor and the organisation.

From a vendor management perspective, typical areas covered in an SLA include

- the 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 (e.g., defect rates, response time, and help desk staffing hours);

⁵⁴International Organization for Standardization/International Electrotechnical Commission, *Information Technology—Cloud Computing—Guidance for Policy Development* (Geneva, Switzerland: International Organization for Standardization, January 2019).

- time to implement new functionality and rework levels;
- level of access rights to be granted to the vendor to perform their services;
- type of documentation required for applications developed by the vendor;
- location where services are to be performed;
- frequency of back-up and data recovery parameters;
- termination and data delivery methods and formats;
- regular reporting process and incident/problem information sharing; and
- incentive and penalty clauses.

For cloud computing SLAs, an organisation can incorporate a number of practices into contracts to help ensure cloud computing services are performed effectively, efficiently, and securely.⁵⁵ These include

- defining measures of performance such as, level of service (e.g., duration), capacity level (e.g., maximum number of users), and response time (e.g., how quickly a transaction is processed);
- specifying how and when the organisation has access to its own data and networks hosted by the vendor, especially when terminating the contract;
- specifying how the cloud provider will monitor performance and when the organisation will review performance;
- specifying security metrics, such as who has access to the data and protections around the data; and
- specifying the notification that will occur during a breach of agreement.

In short, most of the items that are critical to the organisation must be put in the SLA. The IT auditor needs to ask for the SLA or other document (contract or formal agreement) where these parameters are documented. The auditor will need to look at whether the organisation has determined its requirements for the function being outsourced prior to selecting the vendor (i.e., the specific requirements and operational parameters are in the contract and the SLA), whether the organisation is monitoring that the vendor is meeting the requirements stated in the SLA (via periodic status reports), and if the organisation has taken action when the vendor does not meet stipulated SLA parameters (i.e., corrective measures or payment penalties).

d. Cost Benefit Analysis

Organisations can outsource to realise cost savings. These are achieved when the cost to provide these services are cheaper from a vendor than utilising in-house labour or infrastructure. There are other benefits that are not directly measurable, such as leveraging the vendor's infrastructure for rapidly scaling the level of service or using its expertise for special cases. Whenever possible, the organisation should try to determine if the projected savings are being achieved on a periodic basis. This determination as one of the data points to decide whether to continue or stop with the outsourced capability.

e. Security

While outsourcing, IT organisations must evaluate whether vendors have sufficiently robust security practices and if vendors can meet the internal security requirements. While most IT organisations find vendor security practices impressive (often exceeding internal practices), the risk of security breaches or intellectual property protection is inherently increased by the fact that the data has been outsourced. Privacy concerns must be also addressed. Other security concerns include possible mishandling or disclosure of

⁵⁵International Organization for Standardization/International Electrotechnical Commission, *ISO/IEC 19086-1, Information technology—Cloud Computing—Service Level Agreement (SLA) Framework—Part 1: Overview and Concepts* (Sept. 15, 2016), <https://www.iso.org/standard/67545.html> and U.S. Government Accountability Office, *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*, GAO-16-325, (Apr. 7, 2016), <https://www.gao.gov/products/GAO-16-325>.

sensitive data, unauthorised access to data, and applications and disaster recovery plan. Although these issues rarely pose major impediments to outsourcing, the requirements must be documented.

The use of cloud computing also increases the need for robust security practices due to the nature of its features. Some of the security concerns include dependency on third parties, increased complexity of compliance with laws and regulations (in some cases across multiple countries), reliance on the internet as the primary conduit of data, and the dynamic nature of cloud computing (e.g., multiple processing locations). More information on these concerns and the related risks is included later in this chapter.

Some vendors, or service organisations, are independently audited due to their size and number of organisations under contract and will have a service organisation control report, which will list the information security controls and their effectiveness. These reports include an independent assessment of the vendor or service organisations controls that can include internal controls, and controls related to security, availability, integrity, and confidentiality. The auditor can request this report through the organisation.

III. Risks to the Audited Organisation

a. Retaining Business Knowledge and Ownership of Business Process

There is an inherent risk of loss of business knowledge, which resides within the developers of applications. If the vendor is unable to provide this service, IT organisations must be ready to assume this duty again. Also, as the development of the application occurs outside the organisation, the organisation also runs the risk of abdicating or losing the ownership of the business process, which may be claimed by the service provider as its intellectual property. Organisations need to address this issue at the time of entering into contract, and ensure that they have complete documentation of the system development process as well as the system designs. It is essential that the solicitation package sent to the vendor is aligned with the organisation's strategic planning, clearly defined, and detailed so that there are no doubts, inaccuracies, or lack of clarity about requirements. This will also help the organisation to switch service providers, if required.

b. Vendor Failure to Deliver

A vendor may fail to deliver a product either on time or the product must be abandoned due to lack of correct functionality. If the outsourcing process is not implemented correctly, there is a high likelihood that the system or services being acquired may not meet user needs, will be substandard, cost more, will require significant resources to maintain and operate, or may be of such poor quality that it will need to be replaced in the near future. A poor contract, flawed system of vendor selection, unclear milestones, and unfavourable market conditions are some of the common reasons for vendor failure.

IT organisations need to have contingency plans for such an event. When considering outsourcing, IT organisations should assess the implications of vendor failure (i.e., does failure have significant business performance implications?). Availability of detailed documentation on system design and system development will assist the organisation in ensuring business continuity through another service provider or by itself.

c. Lack of Organisation Personnel Prepared to Manage Outsourcing Contracts

The organisation must prepare and maintain qualified personnel able to carry out the correct management of outsourcing contracts. If it does not have enough qualified personnel, during the entire contract execution, the audited organisation may make overpayments to the vendor or not obtain the expected results or outsourcing fail completely. In addition, it is in organisations best interest to create a competitive environment for contracts in which suppliers are constantly being evaluated and maximised. Without proper oversight organisations will not be able to maximise flexibility and control of their IT services.

d. Inaccurate Cost and Schedule Estimates

All outsourcing contracts contain baselines and assumptions. If the actual work varies from estimates, the client will pay the difference. This has become a major obstacle for IT organisations that are surprised that the price was not “fixed” (e.g., for cloud computing resources) or that the vendor expects to be paid for incremental scope changes. Additionally, organisations often create overly optimistic or unrealistic business cases that can cause significant scope creep throughout integration of outsourced services.

e. Turnover of Key Personnel

Rapid growth among outsourcing vendors has created a dynamic labour market. Key personnel are usually in demand for new, high-profile projects, or even at risk of being recruited by other offshore vendors. While offshore vendors will often quote overall turnover statistics that appear relatively low, the more important statistic to manage is the turnover of key personnel on an account. Common turnover levels are in the 15-20 percent range, and creating contractual terms around those levels is a reasonable request.

f. External Risks

Employing overseas service providers is a common form of outsourcing, especially in a cloud computing environment. In this scenario, the risks to such outsourcing would involve foreign regulations on information storage and transfer may limit what can be stored and how it can be processed, data may be used by law enforcement of a foreign country without the knowledge of the organisation, privacy and security standards may not always be commensurate, and disputes because of the different legal jurisdictions cannot be totally avoided.

g. Information Security

Outsourcing can bring a variety of information security risks, such as the mishandling or disclosure of sensitive data or the unauthorised access to data, as mentioned earlier. Further, the business impact and risks associated with the use of cloud computing services include the following areas and processes:

- a greater dependency on third parties, which can lead to increased risk due to
 - vulnerabilities in external interfaces,
 - aggregated data centres,
 - reliance on independent assurance processes, and
 - organisations no longer owning the data or overseeing the controls used by third parties;
- the increased complexity of compliance with laws and regulations, with effects on
 - a greater magnitude of privacy risk,
 - the trans-border flow of personally identifiable information, and
 - contractual compliance;
- a reliance on the internet as the primary conduit to the enterprise’s data, which introduces
 - security issues associated with a public environment and
 - internet connectivity and availability issues;
- the dynamic nature of cloud computing, including the possibility that
 - the location of processing facilities may change according to load balancing,
 - processing facilities may be located across international boundaries,
 - operating facilities may be shared with competitors, and
 - legal issues (liability, ownership, etc.) relating to differing laws in hosting countries may put data at risk;
- IT governance risks such as
 - a loss of IT governance and control by the organisation when using cloud services,

- less reactivity of the client's command compared to the internal provision of the service, and
- a lack of internal support due to organisational culture and the customer perception of greater risks associated with cloud services; and
- audit-related risks such as
 - the inability to access system and security logs from third parties,
 - the loss or incomplete provision of information from the provider to the customer relating to security incidents and the provision of audit trails, and
 - the absence of log data isolation among different clients or other log data leaks.

h. Vendor Lock

Vendor lock is an issue that occurs in outsourcing when finding a new vendor or moving operations in-house becomes too expensive. This can be caused by organisations making significant contributions to a unique product or service provided by a vendor, but only being able to use the product or service with the current vendor. This can be especially troublesome in a cloud environment, where moving data to a different type of environment may require reformatting the data. In addition, organisations may become dependent on the software they are using with a specific cloud provider and will not easily be able to change vendors. Organisations can reduce the risk of vendor lock by evaluating cloud services carefully, ensuring that the data can be easily transferred, performing functional backups of the data, and using different cloud services across multiple providers.

IV. References and Further Reading

Federal Court of Accounts, TCU (SAI Brazil). *Report Highlights: Cloud Computing*.

https://portal.tcu.gov.br/en_us/biblioteca-digital/report-highlights-cloud-computing.htm. July 15, 2015.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC, 19086-1:2016, Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework—Part 1: Overview and Concepts*. <https://www.iso.org/standard/67545.html>. September 15, 2016.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC, 19086-2:2018, Cloud computing – Service level agreement (SLA) framework – Part 2: Metric model*. Geneva, Switzerland: International Organization for Standardization, December 2018.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC, TR 22678:2019, Information technology – Cloud computing – Guidance for policy development*. Geneva, Switzerland: International Organization for Standardization, January 2019.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC, 27036-1:2014, Information technology—Security techniques—Information Security for Supplier relationships – Part 1: Overview and concepts*. Geneva, Switzerland: International Organization for Standardization, April 1, 2014.

International Organization for Standardization. *ISO 37500:2014, Guidance on Outsourcing*. Geneva, Switzerland: International Organization for Standardization, November 11, 2014.

National Institute of Standards and Technology. *Special Publication 500-292: Cloud Computing Reference Architecture*. http://www.nist.gov/customcf/get_pdf.cfm?pub%5Fid=909505. September 2011.

National Institute of Standards and Technology. *Special Publication 800-144: Guidelines on Security and Privacy in Public Cloud Computing*. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>. December 2011.

National Institute of Standards and Technology. *Special Publication 800-145: The NIST Definition of Cloud Computing*. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. September 2011.

National Security Agency. *Mitigating Cloud Vulnerabilities*. https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/csi-mitigating-cloud-vulnerabilities_20200121.pdf. January 22, 2020.

Treasury Board of Canada Secretariat. *Guideline on Service Agreements: Essential Elements*. <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25761§ion=html>. July 4, 2012.

U.S. Government Accountability Office. *Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance*. GAO-16-325. <https://www.gao.gov/products/GAO-16-325>. April 7, 2016.

CHAPTER 6: BUSINESS CONTINUITY MANAGEMENT

I. What Is Business Continuity Management?

The availability and correct operations of IT systems is critical to the ability of government organisations to fulfil their statutory obligations. These systems play an important role in such diverse activities as the assessment and collection of taxes and customs revenues; the payment of state pensions and social security benefits; and in processing national statistics (e.g., births, deaths, crime, and diseases). In fact, many activities cannot be carried out effectively—if at all—without the support of information systems. In order to limit disruption and downtime of these systems, organisations should develop a continuity planning strategy and associated procedures.

By nature, disasters and other crisis are often unexpected events. While not all of these events are avoidable, continuity planning can often limit the impact of these unexpected events. Loss of power, industrial actions, fire, and malicious damage can all have disastrous effects on information systems. It may take many weeks for an organisation to resume effective business operations if it does not have a workable continuity plan in place. In addition, many IT operations are often outsourced to external service providers. If operations at an outsourced service provider are disrupted due to disaster, it could also have a disastrous effect on the organisation.

In order to prevent possible service disruptions from known risks, organisations should conduct various business continuity management activities to help prevent service disruptions, including **business continuity planning**, **disaster recovery planning**, and **information system contingency planning**, among others. The terms business continuity planning and disaster recovery planning are at times used synonymously, but are in fact two distinct but complementary terms. Both are important for the IT auditor, because together they ensure that the organisation is able to operate at some defined capacity after a natural or man-made disruption. Information system contingency planning is similar to disaster recovery planning, but focuses on the recovery of a system regardless of the location of the system. The terms are further explained below:

- **Business continuity planning** is the process an organisation uses to plan and test the recovery of its business processes after a disruption. It also describes how an organisation will continue to function under adverse conditions that may arise (for example, natural or other disasters, or even in the absence of key personnel). The end goal of business continuity planning is for an organisation to create the most resilient organisation possible. This includes continuing mission critical functions at all times during any type of disaster or disruption.
- **Disaster recovery planning** is the process of planning and testing for recovery of IT infrastructure after a natural or other disaster. It is complimentary to business continuity planning. Business continuity planning applies to the organisational business functions whereas disaster recovery planning applies to the IT infrastructure that supports the business functions.
- **Information system contingency planning** is the process of planning and testing for recovery of individual information systems. This is also complimentary of business continuity planning and addresses the recovery of a single system. Information system contingency planning is meant to be a guide for system recovery and can be activated for that system regardless of location.

In essence, a **business continuity plan (BCP)** addresses an organisation's ability to continue functioning when normal operations are disrupted. This plan incorporates the policies, procedures, and practices that allow an organisation to recover and resume manual and automated mission-critical processes after a disaster or crisis. Besides stating the practices that must be followed in the event of an interruption, some BCPs include other components, such as disaster recovery, emergency response, user recovery and contingency, information system contingency, and crisis management activities. As such, in these organisations, business continuity planning is seen as an all-encompassing process that covers both disaster recovery and the resumption of business activities.

However, whether as a part of the BCP or a separate document, **disaster recovery plans (DRP)** should define the resources, actions, tasks, and data required to manage an organisation's recovery process in the event of a business interruption. This plan should also assist an organisation when restoring affected business processes, by outlining the specific steps the organisation must take in its path towards recovery. Specifically, the DRP is used for the advanced preparation and planning needed to minimise disaster damage and for ensuring the availability of the organisation's critical information systems. In terms of IT, DRPs address the recovery of critical technology assets, including systems, applications, databases, storage devices, and other network resources.⁵⁶

In addition to developing DRPs, **information system contingency plans (ISCP)** are a critical step in implementing a comprehensive business continuity planning programme. Organisations may develop ISCPs for each system based on the criticality of that system. In general, ISCPs describe similar steps and procedures as the BCP, but ISCPs are developed independent of specific sites and locations. Among other things, an ISCP provides key system specific information, such as roles and responsibilities, inventory information, assessment procedures, and detailed recovery procedures for that system.

II. Key Elements of Business Continuity Management

The IT auditor is required to assess the organisation's business continuity management programmes, which involves evaluating its BCPs, DRPs, and ISCPs, among others. To do this, auditors need to understand what is involved in developing a business continuity management programme and the steps they should take to evaluate the effectiveness of existing programmes.

Effective continuity planning has several phases common to all information systems. The generic phases in the process are:⁵⁷

- business continuity policy, plan, and organisation;
- establishment of business continuity management team;
- business impact assessment and risk assessment;
- preventive and environment controls;
- plan documentation;
- plan testing and training;
- security implementation; and
- back-up and disaster recovery for outsourced services.

These phases represent key elements in a comprehensive business continuity planning capability. The elements are explained in greater detail below.

a. Business Continuity Policy, Plan, and Organisation

Effective business continuity management starts with establishing a business continuity management policy. The business continuity management policy statement should define the organisation's overall continuity objectives, and establish the organisational framework and responsibilities for continuity planning. The business continuity management team (discussed later) representing all appropriate business functions also plays an important role in the success of the organisation's BCP. Turnover of key

⁵⁶IIa.org, *The IT Auditor's Role in Business Continuity Management*, IIA Publication.

<http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management>

⁵⁷For guidance on the contingency planning processes, see National Institute of Standards and Technology, *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.

staff can be a business continuity challenge for any organisation and steps need to be taken to ensure proper resources are available.

i. Prevention and minimisation of potential damage and interruption

An organisation should take a number of steps to prevent or minimise the damage to automated operations that can occur from unexpected events. These steps can be categorised as

- routinely duplicating or backing up data files, computer programmes, and critical documents with offsite storage; and/or arranging for remote back-up/disaster recovery facilities that can be used if the organisation's usual facilities are damaged beyond use;
- establishing an information system recovery and reconstitution capability so that an information system can be recovered and reconstituted to its original state after a disruption or failure;
- installing environmental controls, such as fire suppression systems or back-up power supplies;
- ensuring that staff and other system users understand their responsibilities during emergencies; and
- effective hardware maintenance, problem management, and change management.

Additionally, when outsourcing, the organisation should establish the vendor has similar mechanisms in place and that the mechanisms are effective.

ii. Implementation of data and programme back-up procedures

Routinely copying data files and software and storing these files at a secure, remote location are usually the most cost effective actions that an organisation can take to mitigate service interruptions. Although equipment can often be readily replaced, the cost could be significant and reconstructing data files and replacing software can be extremely costly and time consuming. Indeed, data files cannot always be reconstructed. In addition to the direct costs of reconstructing files and obtaining software, the related service interruptions could lead to significant financial losses.

iii. Training

Staff should be trained in and be aware of their responsibilities in preventing, mitigating, and responding to emergency situations. For example, information security support staff should receive periodic training in emergency fire, water, and alarm incident procedures, as well as in their responsibilities in starting up and running an alternate data processing site. Also, if outside users are critical to the organisation's operations, they should be informed of the steps they may have to take as a result of an emergency.

iv. Plans for hardware maintenance, problem management, and change management

Unexpected service interruptions can occur from hardware equipment failures or from changing equipment without adequate advance notification to system users. To prevent such occurrences requires an effective programme for maintenance, problem management, and change management for hardware equipment.

b. Establishment of Business Continuity Management Team

To be successful, a business continuity management team must be organised in terms of representing all appropriate business functions. Senior management and other related officials must support a business continuity programme and be associated with the process of developing the policy. Roles and responsibilities in the team should be clearly identified and defined.

c. Business Impact Assessment and Risk Assessment

i. Assessment of criticality and sensitivity of system operations and identification of supporting resources

In any organisation, the continuity of certain operations is more important than other operations, and it is not cost effective to provide the same level of continuity for all operations. For this reason, it is important that the organisation determine which operations are the most critical and which resources are needed to recover and support them. This determination is carried out by performing a risk assessment and business impact assessment,⁵⁸ which are intended to identify probable threats and their impacts on the organisation's information and related resources, including data and application software, and operations. A business impact assessment is used to identify and prioritise system components by associating them with the organisation's business process the system supports. The risk and business impact assessment should cover all functional areas. A decision on residual risk should accordingly be taken where the impact of a possible threat is minimal or control systems are adequate to mitigate such instances in time.

ii. Identification and prioritisation of critical data and operations

The criticality and sensitivity of various data and operations should be determined and prioritised based on security categorisations, availability requirements, and an overall risk assessment of the organisation's operations.⁵⁹ Such a risk assessment should serve as the foundation of an organisation's security plan. Factors to be considered include the importance and sensitivity of the data and other organisational assets, and the cost of not restoring data or operations promptly. For example, a 1-day interruption of a major tax or fee collection system or a loss of related data could significantly slow or halt receipt of revenues, diminish controls over millions of dollars in receipts, and reduce public trust. Conversely, a system that monitors employee training could be out of service for perhaps as much as several months without serious consequences.

Generally, critical data and operations should be identified and ranked by those personnel involved in the organisation's business or programme operations. It is also important to obtain senior management's agreement with such determinations, as well as concurrence from affected groups.

The prioritised listing of critical information resources and operations should be periodically reviewed to determine whether current conditions are reflected in it. Such reviews should occur whenever there is a significant change in the organisation's mission and operations or in the location or design of the systems that support these operations.

iii. Identification of resources supporting critical operations

Once critical data and operations have been determined, the minimum resources needed to support them should be identified and their roles analysed. The resources to be considered include

- IT resources, such as hardware, software, and data files;
- networks, including components such as routers and firewalls;
- supplies, including paper stock and pre-printed forms;
- telecommunications services; and
- any other resources that are necessary to the operation, such as people, office facilities and supplies, and paper records.

Because essential resources are likely to be held or managed by a variety of groups within an organisation, it is important that programme and information security support staff work together to identify the resources needed for critical operations.

⁵⁸For an example of a business impact assessment template, see https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_bia_template.docx.

⁵⁹For more information on security categorisations, see <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>.

iv. Establishing emergency processing priorities

In conjunction with identifying and ranking critical functions, the organisation should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed. A carefully developed processing restoration plan can help organisations begin the restoration process immediately, and make the most efficient use of limited computer resources during an emergency. Both system users and information security support staff should be involved in determining emergency processing priorities.

d. Preventative and Environmental Controls

Environmental controls prevent or mitigate potential damage to facilities and interruptions in service. Examples of environmental controls include

- fire extinguishers and fire suppression systems,
- fire alarms,
- smoke detectors,
- water detectors,
- emergency lighting,
- redundancy in air cooling systems,
- back-up power supplies,
- existence of shut-off valves and procedures for any building plumbing lines that may endanger processing facilities,
- processing facilities built with fire-resistant materials and designed to reduce the spread of fire,
- policies prohibiting eating, drinking, and smoking within IT facilities,
- offsite back-up storage, and
- technical security controls, such as cryptographic key management.

Environmental controls can diminish the losses from some interruptions, such as fires, or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also, uninterruptible or back-up power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shutdown procedures during extended power outages.

e. Plan Documentation

Continuity plans, such as BCPs, DRPs and ISCPs, should be clearly documented, communicated to the affected staff, and updated to reflect current operations. In addition, plans must be maintained in a ready state that reflects the current environment. DRPs and ISCPs should be clearly aligned with the BCP and provide step-by-step instructions on minimising the impact of a disaster. As technology changes, recovery strategies and plans may be modified. Changes to these plans requires a change to the business impact assessment so that new contingency requirements and priorities are clearly documented.

i. BCP

A BCP focuses on sustaining an organisation's mission/business processes in the event that a disaster or disruption occurs. BCPs are critical to providing procedures for how an organisation will maintain operations during and after a disaster or disruption. The BCP may be written for a single business unit or across the entire organisation. In addition, the BCP may be scoped to address the functions that have been determined to be most critical. The BCP must be coordinated with other recovery plans to ensure procedures and expectations are aligned.

The BCP should include elements, such as a business impact assessment, to help guide recovery priorities for the BCP. Recovery strategies should also be documented, such as resource requirements for recovery and management approval of recovery strategies. The BCP should document information such as recovery teams and data collection requirements. Further, the BCP should include exercise and maintenance requirements for ensuring that recovery strategies are updated and accurate. These elements will help establish a thorough BCP that can guide other plans, such as the DRP.

ii. DRP

A DRP should be developed for restoring critical applications; this includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. Organisation-level policies and procedures define the recovery planning process and documentation requirements. Furthermore, an organisation-wide plan should identify critical systems, applications, and any subordinate or related plans.

DRPs should be agreed on by both business and information security departments, and communicated to the appropriate staff. The plan should reflect the risks and operational priorities that the organisation has identified. They should be designed so that the costs of recovery planning do not exceed the costs associated with the risks that the plan is intended to reduce. The plan should also be detailed and documented enough so that its success does not depend on the knowledge or expertise of one or two individuals. Multiple copies of the DRP should be available, with some stored at offsite locations to ensure they are not destroyed by the same events that made the primary data processing facilities unavailable.

Depending on the degree of service continuity needed, choices for alternative sites or facilities will range from an equipped site ready for immediate back-up service, referred to as a **hot site**, to an unequipped site that will take some time to prepare for operations, referred to as a **cold site**. In addition, various types of services can be prearranged with vendors. These include making arrangements with suppliers of IT hardware and telecommunications services, as well as with suppliers of business forms and other office supplies.

iii. ISCP

Organisations should develop contingency plans for each information system that could be impacted in the event of a disaster.⁶⁰ The ISCP should be written in coordination with other plans, such as the DRP. Information systems can be very complex and support multiple different business functions. To this end, organisations need to work with management when developing ISCPs to ensure that the appropriate criticality is assigned and that the impact of a system outage or disruption is understood.

An ISCP will typically contain five main components: supporting information, activation and notification, recovery, reconstitution, and appendices. The following provides a brief description of each of these five components:

- **Supporting information**—This includes providing essential background or contextual information that makes the plan easier to understand, implement, and maintain.
- **Activation and notification**—This includes notifying recovery personnel, conducting an outage assessment, and activating the plan.
- **Recovery**—This includes implementing recovery strategies to restore system capabilities, repair damage, and resume operations.
- **Reconstitution**—This includes validating successful recovery and deactivating the plan. This component could include functionality testing to ensure all system functionality has returned to normal operation.

⁶⁰For guidance on the contingency planning processes, see National Institute of Standards and Technology, *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*.

- **Appendices**—This includes valuable information that was not contained in the body of the plan.

Including these components will help ensure an organisation is better positioned to address system related disasters.

f. Plan Testing and Training

i. Periodically testing of the continuity plans

Testing continuity plans is essential to determine whether they will function as intended in an emergency situation. Testing should reveal important weaknesses in the plans, such as back-up facilities that could not adequately replicate critical operations as anticipated. Through the testing process, these plans need to be substantially improved.

The frequency of continuity plan testing will vary depending on the criticality of the organisation's operations. Generally, continuity plans for very critical systems and functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key staff has occurred. It is important for senior management to assess the risks of potential problems in executing the continuity plan, and develop and document a policy on the frequency and extent of such testing.

ii. Updating of continuity plan based on test results

Continuity test results provide an important measure of the feasibility of the continuity plans. As such, they should be reported to senior management so that the need for modification and additional testing can be determined, and so that senior management is aware of the risks of continuing operations with inadequate continuity plans.

iii. Training

Training personnel who have continuity plan responsibilities is critical to ensuring that those personnel are familiar with their roles and possess the necessary skills to accomplish those roles. This ensures that staff are prepared to participate in testing and actual outage events. In addition, staff should be trained to the extent necessary to conduct their roles without needing to refer back to documentation of their roles. Documented walkthroughs to simulate the contingency with all key persons present can also be a useful tool.

g. Security Implementation

The security of the resources and operations should be built into the BCP as the critical data, application software, operations, and resources stand to be compromised easily during any instance of disaster or a business continuity management activity. For example, during the back-up of data, lack of security can lead to creation of duplicate copies and leakage of important data. At the same time, it may be possible that the data being backed up is compromised during the process of back-up (data being copied from transaction server to data being saved on a back-up server).

h. Back-up and Disaster Recovery for Outsourced Services

Many organisations outsource all or part of their IT operations to a service provider. Since the day-to-day operation and controls would be carried out by the service provider, it will be essential for the organisation to ensure that the BCP and DRP are built into the contract. The organisation would also need to monitor that the business continuity and disaster recovery preparedness is ensured by the service provider. This would include security preparedness of the service provider as well. The organisation may also need to ensure that the service provider maintains the confidentiality of the data. The ownership of the business process and related risk should be retained by the organisation. The organisation should also have a BCP to ensure continuity if a service provider discontinues its business. As mentioned earlier, service

organisation control reports are often available to provide this assurance as part of the contract with the vendor.

III. Risks to the Audited Organisation

Critical services or products are those that must be delivered to ensure survival, avoid causing loss, and meet legal or other obligations of an organisation. Continuity planning is a proactive planning process that ensures that business processes and IT infrastructure of an organisation are able to support mission needs after a disaster or other disruption. Government organisations serve many mission-critical needs (providing payments to citizens, as well as health care, education, defence, and other services that citizens rely upon). If these services are disrupted for long periods of time, it will lead to both financial and other losses. Auditors should ensure that all government organisations have continuity planning processes that ensure organisations are able to continue to serve citizens.

In assessing whether an organisation's continuity planning processes are able to improve the reliability and continuity of IT infrastructure and business processes, auditors can focus on some audit risks to determine the effectiveness of the planning. These audit risks include determining whether the organisation has developed critical documents, including BCPs, DRPs, and ISCPs, that cover all critical functional areas. Further, if the roles and responsibilities are not clear and understood by relevant personnel, a good BCP may become ineffective.

Developing a business impact assessment, preventive and environmental controls, and documentation; testing the continuity contingency plan; and training personnel support the effective implementation of a business continuity management programme. Deficient security in implementing a BCP and DRP pose the risk that an organisation will experience loss of data, loss of valuable time, and other costs due to ineffective recovery in case of a disaster.

Outsourced services present a distinct risk area where continuity planning is not fully under the control of the organisation. Risks related to the security of data, loss of data, unauthorised handling, and leakage of data need to be addressed. Additionally, organisations face continuity risks related to the loss of business knowledge or process ownership, as well as the inability to change the service provider in case of deficient performance or closure.

IV. References and Further Reading

Ila. "The IT Auditor's Role in Business Continuity Management," *Internal Auditor*. <https://elearn.iaa.org.au/mod/resource/view.php?id=10550>. January 2008.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 22301:2019—Security and Resilience—Business Continuity Management Systems—Requirements*. <https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:en>. 2019.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 22300:2021—Security and Resilience—Vocabulary*. <https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en>. 2021.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 22313:2020—Security and Resilience—Business Continuity Management Systems—Guidance on the Use of ISO 22301*. <https://www.iso.org/standard/75107.html>. 2020.

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. 2019.

National Institute of Standards and Technology. *Special Publication 800-34: Contingency Planning Guide for Federal Information Systems*. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>.

National Institute of Standards and Technology. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>. September 2020.

National Institute of Standards and Technology. *Standards for Security Categorization of Federal Information and Information Systems, FIPS 199*. <https://csrc.nist.gov/publications/detail/fips/199/final> February 2004.

U.S. Government Accountability Office. *Federal Information Systems Audit Manual (FISCAM)*. <https://www.gao.gov/products/gao-09-232g>. February 2, 2009.

CHAPTER 7: INFORMATION SECURITY

I. What Is Information Security?

As noted in chapter 1, information security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.⁶¹ Information security includes those measures necessary to govern, prevent, detect, document, and counter such threats and allows an organisation to protect its information system infrastructure from unauthorised users.

Information security is closely related to but distinct from cybersecurity, which is the process of protecting information by preventing, detecting, and responding to cyberattacks, often from external sources.⁶² Cybersecurity involves strategy, policy, and standards regarding the security of, and operations in, cyberspace, and encompasses, among other things, threat and vulnerability reduction; incident response, resiliency, and recovery; and information assurance.⁶³ Although many of the key elements of information security discussed later in this chapter are applicable to cybersecurity, the primary focus of this chapter is on information security policies, procedures, and practices that organisations should be implementing. A separate audit guidance document on cybersecurity and data protection is in development as part of another INTOSAI WGITA project.

As mentioned earlier, a fundamental aspect of information security is the ability to ensure the **confidentiality, integrity, and availability** of information – on which everything else depends.

- **Confidentiality** is preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorised disclosure of information.
- **Integrity** is guarding against improper information modification or destruction, which includes ensuring information non-repudiation⁶⁴ and authenticity.⁶⁵ A loss of integrity is the unauthorised modification or destruction of information.
- **Availability** is ensuring that all information systems including hardware, communication networks, software applications, and the data they hold are available to users at necessary times to carry out business activities. It should also ensure timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Information security needs to be many things to the enterprise, and ultimately must be a tool that enables the organisation and supports its objectives rather than becoming self-serving. One way that information security can support business objectives is by being the gatekeeper of the enterprise's information assets.

⁶¹National Institute of Standards and Technology, *Glossary* (2021), <https://csrc.nist.gov/glossary>.

⁶²National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, 2018.

⁶³National Initiative for Cybersecurity Careers and Studies, *Cybersecurity Glossary*, <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary>.

⁶⁴**Non-repudiation** is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Non-repudiation may not be necessary to evaluate integrity to meet an audit objective.

⁶⁵**Authenticity** is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. Authenticity may not be necessary to evaluate integrity to meet an audit objective.

This calls for the organisation's information security programme to protect organisational data while also enabling the enterprise to pursue its business objectives—and to tolerate an acceptable level of risk in doing so.

In addition, this calls for the organisation to provide the appropriate amount of information to the appropriate users. Applying information security principles to the use of hardware, communication networks, software applications, and data access will require an access control policy. The objective of **access control** is to ensure that users access only those resources and services that they are entitled to access, and that qualified users are not denied to access services that they legitimately expect to receive. Providing information to those who should have it is as significant as protecting it from those who should not have it.

At its core, information security is about minimising exposure, based upon risk management, in all areas of the IT governance model. Failure to implement and monitor risk mitigation processes in one area may cause damage in the entire organisation. Even if it is broadly known that managing information security risks effectively is essential to an organisation's safety, these risks are often overlooked or safety precautions are not updated in response to changing conditions.

a. The Necessity of Information Security

Information security is increasingly more important for government organisations. As the interconnection of public and private networks and the sharing of information resources increase the complexity of controlling access and preserving the confidentiality, integrity, and availability of data, there is an increased need for organisations to establish information security programmes.

Information systems are incredibly complex assemblages of technology, processes, and people that collaboratively function together to accommodate the processing, storage, and transmission of information to support an organisation's mission and business functions. Therefore, it is essential that every organisation builds an information security programme.

The objective of an information system security programme is to protect an organisation's information by reducing the risk of loss of confidentiality, integrity, and availability of that information to an acceptable level. If the organisation has not established an information security programme, then it will have an increased risk of facing potential threats to the organisation's operations, the achievement of the overall objectives, and ultimately affect the credibility of the organisation.

As the potential, complexity, and role of IT grows, information security becomes an increasingly important topic of IT audits. It is a critical factor of organisations' activities, because information security weaknesses may lead to severe damage. Potential impacts of information security weaknesses include:

- Violations of legal and regulatory requirements;
- Fines, compensations, reduced sales, repair, or restore costs;
- Reduction of effectiveness and/or efficiency in a project, programme, or whole service provided by the organisation;
- Loss or theft of computer resources, assets, and funds;
- Inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personally identifiable information, and proprietary business information;
- Hacking and potential ransom demands;
- Disruption of essential operations supporting critical infrastructure, national defence, or emergency services;
- Undermining of organisational missions due to incidents that damage the organisation's reputation and/or finances;
- Use of computer resources for unauthorised purposes or to launch attacks on other systems; and
- Damage to networks and equipment.

This damage may be caused by:

- **security breaches**—both detected and undetected;
- **unauthorised external connections**—to remote sites;
- **exposure of information**—disclosure of corporate assets and sensitive information to unauthorised parties. One example of how this may occur is known as social engineering, which is a manipulation technique used by criminals that relies on the basic human instinct of trust to trick people into giving up confidential information;
- **insider threats**—users who exploit their positions within organisations to gain unrestricted access and cause damage; and
- **system vulnerabilities**—systems and data accessed in an unauthorised way are prone to a broad range of malicious attacks and may be opened for further intrusions.

The increased use of social media by government organisations can also become an area of potential IT audits. The use of these social media services—including popular services like Facebook, Twitter, and YouTube—provides opportunities for agencies to more readily share information with and solicit feedback from the public. However, the use of these services can pose challenges in protecting personal information and ensuring the security of information and systems, among other areas. For example, attackers may use social media to collect information and launch attacks against an organisation's information systems. In addition, privacy could be compromised if clear limits are not set on how the organisation uses personal information to which it has access in social networking environments. To help address these challenges, organisations should have policies and procedures in place for security risk management and privacy protection that address the use of social media.⁶⁶

b. Formation of Information Security Culture

A determinant to the success of information security programmes in an organisation is the creation of organisational cultures addressing security issues. To uniformly address these and other issues in a large organisation, a business model of information security should be followed.⁶⁷ Key elements of a successful information security culture involve the following:

- **Creating security awareness.** This consists of general information security awareness activities and targeted educational sessions for employees. These sessions are good opportunities to begin to introduce information security responsibilities. The human resources function may be responsible for initial awareness training for new employees. The training should proceed during employment and up to the termination to always promote security awareness.
- **Seeking management commitment.** Management commitment is one attribute that is unique in the formation of information security culture. The commitment is shown by management not only in preparing formal documentation of information on security policies, but also by being actively involved. If the management does not genuinely support the information security programme, it can discourage employees' sense of obligation or responsibility to the programme. It is therefore critical for management to accept ownership for information security and fully support the programme.
- **Building solid coordination by setting cross-functional teams.** Since information security involves many aspects of the organisation that require coordination, forming cross-functional teams (e.g., teams with members from multiple divisions, including IT) should be considered. The use of cross-functional teams encourages communication and collaboration and reduces departmental isolation and duplicated efforts.

⁶⁶For more information on auditing an organisation's policies and procedures for using social media, see U. S. Government Accountability Office, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, (June 28, 2011), <https://www.gao.gov/products/GAO-11-605>.

⁶⁷ISACA, *Business Model for Information Security*, 2010.

The establishment of information security culture is an integral part of the implementation of governance within an organisation, and is characterised by the following:

- **Alignment of information security and business objectives.** It is necessary to align information security and business objectives since security objectives enable and support business objectives. The information security programme needs to align with the organisation and provide information security controls that are practical and provide real, measurable risk reduction.
- **Balance among organisation, people, process, and technology.** Effective information security requires organisational support, competent personnel, efficient processes, and selection of appropriate technology. Each element interacts with other areas—impacting and supporting other elements, often in complex ways—so, it is crucial to achieve a balance among them. If any one element is deficient, information security is diminished.
- **Risk management.** The application of information security must be driven by risk management. The National Institute of Standards of Technology describes the following four aspects of the risk management process in its special publication on managing information security risk:⁶⁸
 - Assignment of security risk management responsibilities to senior leaders/executives;
 - Ongoing recognition and understanding by senior leaders/executives of the information security risks to organisational operations and assets, individuals, and other organisations, arising from the operation and use of information systems;
 - Establishing the organisational tolerance for risk and communicating the risk tolerance throughout the organisation, including guidance on how risk tolerance impacts ongoing decision-making activities; and
 - Accountability by senior leaders/executives for their risk management decisions and for the implementation of effective, organisation-wide risk management programmes.

II. Key Elements of Information Security

The discussion of information security in an organisation covers 12 domains:

- Risk assessment
- Security policy
- Organisation of IT security
- Operations and records management
- Asset management
- Human resources security
- Physical and environmental security
- Access control
- IT systems development, acquisition, and maintenance
- IT security incident management
- Business continuity management
- Compliance

a. Risk Assessment

Risk assessment is the process of identification, analysis, and evaluating risks in the IT security infrastructure. It is also the process of assessing security-related risks from internal and external threats to

⁶⁸National Institute of Standards and Technology, *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View*, 2011.

an entity, its assets, and personnel. The risk assessment process includes the identification and analysis of

- all assets and processes related to the system;
- outsourced environments related to the system;
- potential threats that could affect the confidentiality, integrity, or availability of the system;
- system vulnerabilities and the associated threats;
- potential impacts and risks from the threat activity;
- protection requirements to mitigate the risks; and
- selection of appropriate security measures and analysis of the risk relationships.

An improperly performed risk assessment may result in underprotection of sensitive infrastructure and information, or in some cases wasteful overprotection. The National Institute of Standards of Technology outlines four steps of the risk assessment process in its special publication *Guide for Conducting Risk Assessments*.⁶⁹

- **Prepare** for the assessment by developing an organisational risk framework.
- **Conduct** the assessment by
 - identifying threat sources and events,
 - identifying vulnerabilities and predisposing conditions,
 - determining the likelihood of occurrence,
 - determining the magnitude of impact in the event of a security breach, and
 - using the above information to determine overall risk.
- **Communicate** the results of the assessment
- **Maintain** the assessment.

Risk assessments are not one-time activities that provide permanent and definitive information for decision makers to guide and inform responses to information security risks. Rather, organisations should employ risk assessments on an ongoing basis, with the frequency of the risk assessments and the resources applied during the assessments commensurate with the expressly defined purpose and scope of the assessments.

The application of risk assessment will help management to select appropriate controls to mitigate risk effectively. To select appropriate security controls, Federal Information Processing Standards Publication 199 defines three levels of potential impact—low, moderate, and high—on organisations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).⁷⁰ The application of these definitions must take place within the context of each organisation and the overall national interest.

- The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.
- The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.
- The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets, or individuals.

This impact categorisation affects the stringency of testing in many information security domains. For

⁶⁹National Institute of Standards and Technology, Joint Task Force Transformation Initiative, Special Publication 800-30, *Guide for Conducting Risk Assessments*, 2012.

⁷⁰Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.

example, with respect to access controls, organisational risk assessments (and risk tolerance) are important factors in determining access control policies and procedures. Access control policies and procedures for a given resource should be appropriate to the level of impact (i.e., the loss of confidentiality, integrity, or availability) a security breach of that resource would have on the organisation.

b. Security Policy

The organisation's security policy is the set of laws, rules, and practices that regulate how it manages, protects, and distributes resources to achieve specified security objectives. These laws, rules, and practices must identify criteria for individuals' authority, and may specify conditions under which individuals are permitted to exercise their authority. To be meaningful, these laws, rules, and practices must provide individuals with a reasonable ability to determine whether their actions violate or comply with the policy.

See the table for recommended elements of an IT security policy.

Elements of an IT security policy	Definition of information security – objectives and scope (including data confidentiality)
	Detailed security principles, standards, and compliance requirements (e.g., IT department personnel should not have operational or accounting responsibilities)
	Definition of general and specific responsibilities for all aspects of information security
	Use of information assets and access to email and internet
	Mode and method of access (to include access control and authentication policies)
	Back-up procedures
	Procedures to deal with malicious software and programmes (e.g., continuous monitoring, intrusion detection, and intrusion prevention systems)
	Elements of security awareness and training
	Process for reporting and responding to suspected security incidents
	Business continuity plans
	Patch management
	Physical security
	Methods of communicating to staff the policy and procedures adopted for information security

c. Organisation of IT Security

Organisation of IT security often necessitates implementing a security policy for an entity. Responsibility for implementing the security policy could be given to a unit or an individual, who subsequently works with the organisation to acquire appropriate tools and processes to implement the policy effectively. Once the policy is implemented, the organisation would additionally be responsible for providing training to staff and responding to security incidents. The organisation also needs to ensure that its data that accessed by or transferred to external organisations are suitably protected. The auditor will need to ensure that external organisations can implement the security requirements.

d. Operations and Records Management

An organisation needs to keep track of the process and procedures it uses for its business operations. This includes the set of organisational procedures and processes that ensure the correct data processing and documenting procedures for media and data handling, emergency procedures, network security logging, and back-up procedures.

e. Asset Management

Asset management, broadly defined, refers to any system whereby things that are of value to an organisation are monitored and maintained. Asset management is a systematic process of operating, maintaining, upgrading, and disposing of assets in a cost effective manner.

For IT, asset management includes maintaining an accurate inventory of equipment, data, knowing what licences are for associated equipment, and the maintenance and protection (e.g., lock-down and controlled room) of equipment. IT asset management also includes managing the software and process documentation that are valuable to an organisation.

IT asset management is very important, as an organisation may be at risk if it does not have a full inventory of its assets. Without a full inventory of IT assets, it is impossible for organisations to know if it is applying appropriate security controls to the totality of its assets. A lack of a full IT asset inventory can also lead to complications when organisations need to upgrade software to meet future business needs.

f. Human Resources Security

Employees handling personal data in an organisation need to receive appropriate awareness training and regular updates in an effort to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organisation's security policy. The organisation's data must be protected from unauthorised access, disclosure, modification, destruction, or interference. The management of human resources security and privacy risks is necessary during all phases of employment association with the organisation.

The three areas of human resources security are:

- **Pre-employment:** This includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining the depth of candidate's screening levels – all in accordance with the organisation's IT security policy. During this phase, contract terms should also be established.
- **During employment:** Employees with access to sensitive information in an organisation should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats.
- **Termination of employment:** To prevent unauthorised access to sensitive information, access should be revoked immediately upon termination of an employee with access to such information. This also includes the return of any assets of the organisation that was held by the employee. During this phase, a special form could be prepared to document all the work done by the employee and to ensure that all access has been revoked and all assets have been returned.

A programme of security awareness should be in place, reminding all staff of the possible risks and exposure, as well as their responsibilities as custodians of the organisation's information.

g. Physical and Environmental Security

Physical security describes measures that are designed to deny access to unauthorised personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information. In addition, it includes guidance on how to design structures to resist potentially hostile acts. Physical security can be as simple as a locked door or as elaborate as multiple layers of barriers, armed security guards, and guardhouse placement.

Physical security is primarily concerned with restricting physical access by unauthorised people (commonly interpreted as intruders) to controlled facilities, although there are other considerations and situations in which physical security measures are valuable (e.g., limiting access within a facility or to specific assets, and environmental controls to reduce physical incidents, such as fires and floods).

Security inevitably incurs costs and can never be complete; security can reduce but cannot entirely eliminate risks. Given that controls are imperfect, strong physical security applies the principle of defence in depth using appropriate combinations of overlapping and complementary controls. For instance, physical access controls for protected facilities are generally intended to:

- deter potential intruders (e.g., warning signs and perimeter markings);
- distinguish authorised from unauthorised people (e.g., using pass cards and keys);
- delay, frustrate, and ideally prevent intrusion attempts (e.g., strong walls, door locks, and safes);
- detect intrusions and monitor/record intruders (e.g., intruder alarms and closed-circuit television systems); and
- trigger appropriate incident responses (e.g., by security guards and police).

Environmental controls apply primarily to organisational facilities that contain concentrations of system resources (e.g., data centres, mainframe computer rooms, server rooms, and communication rooms). Insufficient environmental controls, especially in very harsh environments, can have a significant adverse impact on the availability of systems and system components that are needed to support organisational mission and business functions.

h. Access Control

Access control refers to exerting control over who can interact with a resource. Often but not always, this involves an authority, who does the controlling. The resource can be a given building, group of buildings, or IT systems. Access control is—whether physical or logical—in reality, an everyday phenomenon. A lock on a car door is essentially a simple form of access control. A PIN on an ATM system at a bank as well as biometric devices are other means of access control. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment. Access control ensures that⁷¹

- identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes;
- physical access to assets is managed and protected;
- remote access—if used by the organisation—is managed;
- access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties;⁷²
- network integrity is protected (e.g., network segregation, network segmentation);
- identities are proofed and bound to credentials and asserted in interactions; and
- users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organisational risks).

Organisational risk assessments and risk tolerance are important factors in determining access control policies and procedures. Access control policies and procedures for a given resource should be appropriate to the level of impact (that is, the loss of confidentiality, integrity, and/or availability) a security breach of that resource would have on the organisation.

In a government environment, access control is important because many government entities process

⁷¹U.S. Government Accountability Office, *Federal Information System Controls Audit Manual*, 2009.

⁷²The principle of least privilege requires that each subject be granted the most restrictive set of privileges needed for the performance of authorised tasks. Application of this principle limits the damage that can result from accident, error, or unauthorised use of an information system. Separation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions, and recording custody of assets to separate individuals. This principle is commonly used in large IT organisations so that no single person is in a position to introduce fraudulent or malicious code without detection.

sensitive data and privacy concerns limit who should view various parts of the information. Access control ensures that only users with the proper credentials have access to sensitive data.

i. IT Systems Development, Acquisition, and Maintenance

It is important for organisations to identify and manage supply chain risks when developing and acquiring IT products and services. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, **supply chain risk management** is a critical organisational function. A primary objective of cyber supply chain risk management is to identify, assess, and mitigate products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain. Cyber supply chain risk management activities may include:⁷³

- determining cybersecurity requirements for suppliers;
- enacting cybersecurity requirements through formal agreement (e.g., contracts);
- communicating to suppliers how those cybersecurity requirements will be verified and validated;
- verifying that cybersecurity requirements are met through a variety of assessment methodologies, including security operations centre reports, if available; and
- governing and managing the above activities.

Ongoing maintenance is required after the successful development or acquisition of an IT product or service. Maintenance of an IT system during its life cycle includes changes and updates to the system (e.g., installing patches) as a result of new requirements, fixing system errors, and enhancements made as a result of new interfaces.

For installing patches, organisations should employ **patch management**. Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they mitigate software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation.⁷⁴

j. IT Security Incident and Event Management

As mentioned in chapter 4 on IT operations, incident management is the systems and practices used to determine whether incidents or errors are recorded, analysed, and resolved in a timely manner. In the fields of computer security and IT, IT security incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events. IT security incident management is a specialised form of incident management.

Organisations should establish a formal incident response process, plan, and policy. The typical incident response process consists of four phases:

- **Preparation.** This phase involves establishing and training an incident response team; creating an incident response capability so that the organisation is ready to respond to incidents; and preventing incidents by ensuring that systems, networks, and applications are sufficiently secure by applying risk-informed security controls to information systems.
- **Detection and analysis.** This phase involves detecting incidents through a variety of means with varying levels of detail and fidelity. Means of detection include network-based and host-based intrusion

⁷³National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, 2018.

⁷⁴National Institute of Standards and Technology, *Special Publication 800-40, rev. 3: Guide to Enterprise Patch Management Technologies*, 2013.

detection and prevention systems, antivirus software, log analysers, and user reports. Once an incident is detected, the organisation's incident response team should work quickly to analyse and validate each incident, following a predefined process and documenting each step taken.

- **Containment, eradication, and recovery.** Upon detection, organisations should strive to contain the incident. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, and disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident. Containing the incident provides time for the organisation to develop a tailored remediation strategy.

Upon containment, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets and boundary router access control lists).

- **Post-incident activity.** After resolving an incident, organisations should communicate the experience to related IT staff and leverage it as an opportunity to learn and improve. Post-incident activities include holding lessons learned sessions, collecting incident data, retaining evidence, and revising incident response processes based on lessons learned from the incident.

k. Business Continuity Management

Business continuity planning is the process an organisation uses to plan and test the recovery of its business processes after a disruption. It also describes how an organisation will continue to function under adverse conditions that may arise (e.g., natural or other disasters). See chapter 4 for more information on business continuity management.

I. Compliance

The IT auditor should review and assess compliance with all the internal and external (e.g., legal, environmental and information quality, and fiduciary and security) requirements.

III. Risks to the Audited Organisation

IT security policies, procedures, and their enforcement enables an organisation to protect its IT infrastructure from unauthorised users. IT security policy for an organisation lays out the high-level requirements for the organisation and its employees to follow in order to safeguard critical assets. It also provides for training of staff on security issues and ensures that they follow established procedures for data access and control. Additionally, the IT policy refers to laws and other regulations that the organisation is required to follow. There are many obstacles that organisations face in regard to the implementation of an effective information security system. Without effective governance to deal with these obstacles, IT security will have a higher risk of failure in meeting the organisation's objectives.

Every organisation faces its own unique challenges as its individual environmental, political, geographical, economic, and social issues differ. Any one of these issues can present obstacles to providing effective IT governance, and it is the responsibility of the IT auditor to point out information security risks to the management.

The following are examples of significant risks identified at most organisations:

- unauthorised disclosure of information,
- unauthorised modification or destruction of information,

- information system attack,
- destruction of the information system infrastructure,
- disruption of access to or use of information or an information system,
- disruption of information system processing, and
- theft of information or data.

When assessing audited organisations' risk exposures, special attention should be given to following areas:

- information security strategies not aligned with IT or business requirements;
- policies not applied uniformly with varying enforcement;
- non-compliance with internal and external requirements;
- information security not included in projects' portfolio maintenance and development processes;
- architecture design resulting in ineffective, inefficient, or misguided information security solutions;
- inadequate physical security measures and assets management;
- inadequate hardware system application configuration;
- inefficient organisation of information security processes and undefined or confusing information security responsibility structure;
- inappropriate human resources solutions;
- ineffective use of financial resources allocated to information security and the information security value (cost-benefit) structure not aligned with business needs or goals; and
- information security not monitored or monitored ineffectively.

When carrying out an information security audit, the auditor should address issues related to the 12 previously mentioned domains in information security.⁷⁵ The auditor should begin with assessing the adequacy of risk assessment methods and consider audit issues related to the implementation of information security. An audit matrix will assist the auditor to raise audit questions, criteria for evaluation, documents required, and technical analysis to be used. At the end, the auditor may develop a detailed audit programme according to the needs and development during the audit fieldwork.

IV. References and Further Reading

Cichonski, Paul, Thomas Millar, Tim Grance, and Karen Scarone. NIST Special Publication 800-61, rev 2: *Computer Security Incident Handling Guide*. <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>. 2012.

ISACA ITAF. *A Professional Practices Framework for IT Assurance*. USA, 2008.

ISACA. *Risk IT Framework*. <https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2>. 2020.

ISACA. *COBIT 5 Framework*. <https://www.isaca.org/bookstore/cobit-5/wcb5>. 2012.

ISACA. *Information Security Audit/Assurance Program*. 2010.

ISACA. *IT Risk Management Audit/Assurance Program*. 2012.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27000: Information Security Management System*. <https://www.iso.org/standard/54534.html>. 2013.

⁷⁵International Organization for Standardization, *ISO 27000 Series Information Security Management System*.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27005: Information Security Risk Management*. <https://www.iso.org/standard/75281.html>. 2018.

National Institute of Standards and Technology. *Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems*. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>. February 2004.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1. <https://www.nist.gov/cyberframework/framework>. 2018.

National Institute of Standards and Technology. *Special Publication 800-40, rev. 3: Guide to Enterprise Patch Management Technologies*. <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>. 2013.

National Institute of Standards and Technology. *Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View*. <https://csrc.nist.gov/publications/detail/sp/800-39/final>. 2011.

U.S. Government Accountability Office. *Federal Information System Controls Audit Manual (FISCAM)*. <https://www.gao.gov/products/gao-09-232g>. February 2, 2009.

U.S. Government Accountability Office. *Information Security: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*. <https://www.gao.gov/products/gao-15-758t>. July 8, 2015.

U.S. Government Accountability Office. *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*. GAO-21-171. <https://www.gao.gov/products/gao-21-171>. December 15, 2020.

CHAPTER 8: APPLICATION CONTROLS

I. What Are Application Controls

As stated earlier, an internal control is a process designed to provide reasonable assurance that

- operations, including the use of organisation resources, are effective and efficient;
- financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use are reliable; and
- applicable laws and regulations are followed.

Information system controls consist of those internal controls that are dependent on information systems processing and include general controls (organisation-wide and system-level), business process application controls, and IT-dependent user controls (controls performed by people interacting with information systems).

Business processes are the principal functions used by an organisation to accomplish its mission. A business process application is a combination of hardware and software that is used to process business information in support of a specific business process. It may include both manual and computerised procedures for transaction origination, data processing, record keeping, and report preparation. Each organisation may have a number of applications running, ranging in size from an enterprise-wide system that is accessed by every employee to a small client application accessed by one employee. The application software could be a payroll system, a billing system, an inventory system or, an integrated enterprise resource planning system.

Business process application controls, commonly referred to as **application controls**, are specific controls unique to each IT application. When business processes are automated into an IT application, business rules are also built into the application in the form of application controls. They apply to application segments and relate to both transactions and standing data. Application controls are those controls over the completeness, accuracy, validity, confidentiality, and availability of transactions and data during application processing.

- **Completeness controls** should provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output.
- **Accuracy controls** should provide, among other things, reasonable assurance that transactions are properly recorded, with the correct amount/data, and on a timely basis.
- **Validity controls** should provide reasonable assurance that (1) all recorded transactions actually occurred, relate to the organisation, and were properly approved in accordance with management's authorisation; and (2) output contains only valid data.
- **Confidentiality controls** should provide reasonable assurance that application data and reports and other output are protected against unauthorised access.
- **Availability controls** should provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed.

An application controls review enables the auditor to provide the management with an independent assessment of the efficiency and effectiveness of the design and operation of internal controls and operating procedures relating to automation of a business process, and identify application-related issues that require attention. While the general IT controls in an organisation set the tone for the overall control environment for the information systems, application controls are built into specific applications to ensure and protect the accuracy, integrity, reliability, and confidentiality of information. For example, they ensure that the initiation of transactions is properly authorised and that valid input data is processed, completely recorded, and accurately reported. General controls help to ensure that the work performed to implement

an application control is proportionate to the risk of its failure; for instance, the likelihood of a key configuration for an application control being accessed by inappropriate persons or changed without proper authorisation or testing.

Since application controls are closely related to individual transactions, testing them can more directly provide the auditor with assurance on the accuracy of a particular functionality. For example, testing the controls in a payroll application would provide assurance as to the payroll figure in a client's accounts. Due to their wider scope, testing the client's general IT controls (such as change control procedures) may not provide a similar level of assurance for the same account balance.

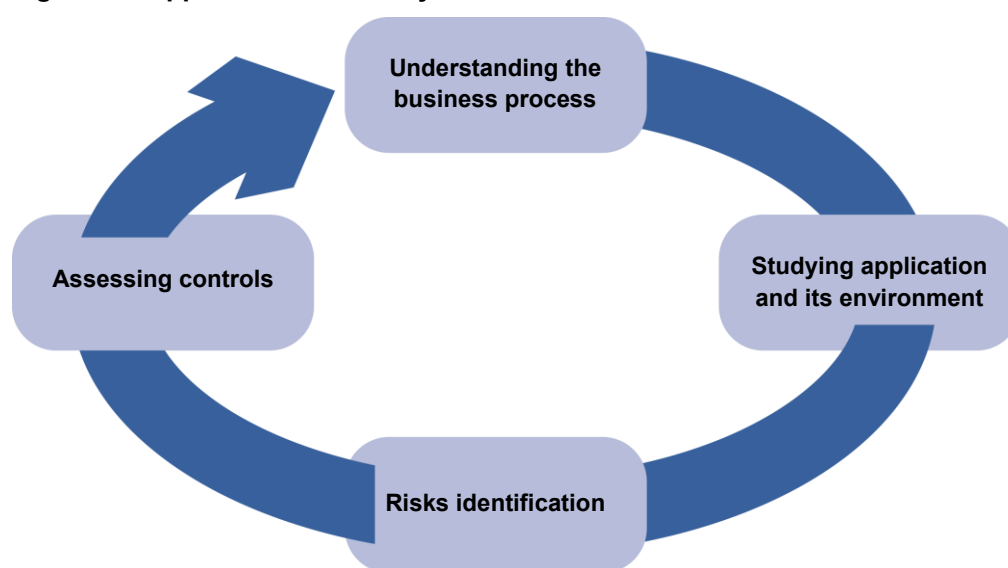
Depending on the specific audit goals, there may be different approaches for reviewing and testing application controls. For instance, the application review might be focused on legal and standards compliance, in which case the objective would be to verify whether application controls properly help address those issues. Alternatively, the application review might be a part of a performance audit, in which case it would be important to see how business rules are translated into the application. During an information security analysis, the focus might be on the application controls responsible for assuring data confidentiality, integrity, and availability.

a. Application Control Review Process

The steps to be performed in carrying out an application controls review often involve a cyclical process of activities. Figure 10 shows the common steps in the review cycle for application controls. Even though, as shown by the arrow, it is intuitive to start with a wider understanding of the business process, it is important to note that there is no strict hierarchy among these steps.

A brief description of each of the four phases follows the figure.

Figure 10: Application Review Cycle



Source: Unknown.

i. Understanding the business process:

In order to explore technical matters regarding the application, it is useful to first obtain an overview of the business processes automated by the application—its rules, flows, actors, roles, and related compliance requirements. Understanding the underlying business process is an important step to be able to verify the consistency of the application controls and the automated processes. The activities that are a part of this step will vary according to the audit objective. It is usually done through the study of the operating and work

procedures, process flow chart of the organisation, or other reference material. The audit team might also need to meet and interview business managers, IT executives, and key application users. The audit team can also find value in creating their own flow charts and by noting the processes, controls, systems, interfaces and reports that make up the process. Flow charts created by the audit team can be useful because often client-owned process flows are either too complex and detailed, or not quite detailed enough, to be comprehensible and to identify the relevant aspects and risks in the process.

ii. Studying the application and its environment:

After gaining awareness of the business process, the auditor should obtain an understanding of the specific networks and systems that are used to support the key business process applications. Information obtained during this step is important to assist in the identification of critical control points and to provide a foundation for understanding where application-level controls are applied. Activities in this step include reviewing documentation (such as organisation diagrams, dataflow diagrams, and user manuals); interviewing key personnel; conducting studies of key functions of the software at work by observing and interacting with operating personnel during work; and, through discussions, performing a walk-through of the business process and application from source entry through output and reconciliation to see how processes actually flow. These steps also allows an auditor to observe any associated manual activities that could act as complementary controls.

Auditors can also obtain documentation on technical infrastructure (i.e., operating system; network environment; database management system; interfaces with other applications; sourced in-house or outsourced; and batch entry, real-time, and online transaction processing), which they can discuss with managers, operators, and developers. These discussions and documentation can be a useful indication of how the infrastructure impacts the application.

iii. Risks identification:

Based on the auditor's understanding obtained in the previous steps, the auditor should assess, on a preliminary basis, the nature and extent of information systems risk related to the key applications. The goal of this step is to identify risks associated with the business activity/function served by the application, to determine what could potentially go wrong with the application, and to see how these risks are handled by the controls in place in the application software. A business process risk assessment may be already available, from such sources as a previous audit or management review. The auditor can benefit from its use after assessing the confidence of the existent risk assessment.

iv. Understanding and assessing controls:

Within each key business process application, the auditor should obtain an understanding of the particular types of application level controls that are significant to the audit objectives. Once aware of the environment (business and technical) surrounding the application, the auditor may be better able to assess the controls used to address the existent risks. The auditor should use judgment when assessing the application controls and should consider costs and benefits when putting forward recommendations for improvements. For example, excessive details in transaction logging may add to cost overheads, and may not indicate desired trails. This assessment involves an evaluation of application controls along the lines of what is described in the following section. The auditor may also identify that there is more than one control mitigating the same risk, which could result in a process improvement recommendation to the client.

b. Illustration

For an illustration of elements of application controls, see figure 11. In an online payment application one input condition could be that the credit card expiry date should fall beyond the date of transaction. Another would be that the card number has to be valid and match both the name of the cardholder and the card verification value (CVV number) as per the credit card issuer's database. Yet another would be that the details when transmitted over the network should be encrypted. The controls, such as those built into the application, would ensure that these conditions are inviolable and better validate the transactions.

Figure 11: Application Controls Example

Welcome to State Bank of India's Secure Payment Gateway

Dear Customer,
SBI Payment Gateway will secure your payment to **BillDesk_BillPay**.

Select the type of card*

Card Number*
(Please enter your card number without any spaces)

Expiry Date *
(Please enter expiry date provided on your card)

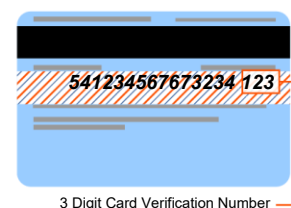
CVV2 /CVC2 Number *
(CVV2 / CVC2 is the three digit security code printed on the back of card)

Name on Card

Purchase Amount **INR 3566.00**

Word Verification *
Type the characters you see in the picture below

r h 2 Z y g



Source: Unknown.

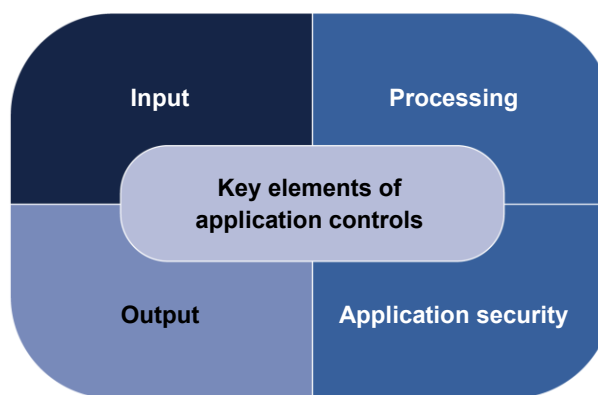
In addition to automated controls such as these, application controls also include manual procedures that operate in proximity to an application. These controls are not only built into specific applications, but also surrounding business processes. For example, a data entry clerk may require a data input form to be signed (i.e., approved) before it is entered into the application. The combination of manual and automated controls chosen is often a result of cost and control considerations when an application is first designed.

II. Key Elements of Application Controls

An application can be divided into the following primary segments: data input (data origination and data entry); transaction processing; data output (distribution of results) and security (logging, communications, storage). The controls in an application are built into each segment of the application, along with controls that restrict access to the application and master files.

Although it is not realistic to provide detailed test steps and checklists for every possible permutation of an application, an auditor must be aware of control concepts that are common to almost all applications and business processes. Understanding these common application controls can be used to generate thought and ideas regarding more specific audit test steps to the application being audited.

Figure 12: Key Elements of Application Controls



Source: Unknown.

Some of the most common control elements for each of the four key areas are shown in figure 13:

Figure 13: Examples of Application Controls

Input controls	<ul style="list-style-type: none"> Data entry/field checks (e.g. validation of entered credit card numbers) Source documents management (e.g. preparation and retention procedures) Error handling mechanisms (error messages, suspense files) Data entry authorisation rules (e.g. segregation of duties)
Processing controls	<ul style="list-style-type: none"> Business rules mapping Integrity and completeness checks, report of out-of-balance conditions Automated calculations Input reconciliations
Output controls	<ul style="list-style-type: none"> Completeness and accuracy validations, reconciliation Output review and tracking Review and follow-up of application-generated exception reports Output labeling, handling, retention and distribution procedures
Application security controls	<ul style="list-style-type: none"> Traceability mechanisms (audit trails, log review, use of unique identifiers) Logical access control to functionalities and application data Stored data protection

Source: Unknown.

a. Input Controls

The objectives of the input controls are seeking to validate and authenticate the acts of source data preparation, authorisation and entry so that accurate, reliable, and complete data is accepted by the application in a timely manner. While data input can be manual or system interface driven, errors and omissions can be minimised through good input from design, adequate segregation of duties regarding the origination and approval of input documents, and placing relevant authenticity, accuracy and completeness checks (with menu options or interactive messages). The following table lists key elements of input control.

Elements of input control	Description
Data entry checks (validity, completeness, duplicate checks)	Automated validity checks on the data entered (e.g., journey date falls outside the booking open period); completeness checks to ensure that all the key transaction information has been entered (e.g., date of journey, names of passenger, identity numbers are required fields); duplicate checks compare new transactions with transactions previously posted (e.g., check against duplicate invoices); assurance that inputs falling beyond parameters determined by management generate an error.
Source documents management	Documentation of source document preparation procedures, including a defined transaction data strategy and document retention procedures; source documents for data inputs are logged and traceable; source documents should provide predetermined input codes to reduce errors and include a portion to document authorisation.
Error handling procedures	Procedures exist for dealing with rejected input. (e.g., use of appropriate error messages, prompts enabling re-input, and use of suspense data); errors are investigated and subsequent correction measures taken.
Authorisation of input	Manual procedures and supervisory level authorisation of data is required on data entry form. (e.g., authorisation of bill of entry details by supervisor before entered by data entry clerk for processing in Customs applications); approval procedures are followed for data input.

b. Processing Controls

The objective of processing control measures is to seek to protect data integrity, validity, and reliability and guard against processing errors throughout the transaction processing cycle—from the time data are received from the input sub-system to the time data are dispatched to the database, communication, or output sub-system. They also ensure that valid input data is processed only once and that detection of erroneous transactions does not disrupt the processing of valid transactions. In doing so, they seek to enhance the reliability of the application programmes that execute instructions to meet specific user requirements.

The control procedures in this area also include establishing and implementing mechanisms to authorise the initiation of transaction processing, enforcing that only appropriate and authorised applications and tools are used, and routinely verifying that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors or buffer overflow, monitoring transaction/record counts, performing referential integrity checks and range checks, and comparing control and hash totals.

In real time systems some other compensating controls used are one-for-one checking, retrospective batching, exception reporting, and suspense account reporting. The following table lists key elements of processing controls.

Elements of processing control	Description
Business rules mapping	Inspect configurations to ensure that transactions are executed in accordance with predetermined parameters and tolerances, specific to an organisation's risk management. Document parameters and tolerances and have management regularly review the resulting restrictions. Ensure that transactions are matched with management authorisations.
Integrity and completeness checks	Inspect a selection of system logs for transactions. Determine whether the applications perform appropriate edit and validation checks against processed data, produce appropriate error messages or rejections, and appropriately communicate processing errors to users.
Automated calculations	Determine the extent to which application processing of data is automated and standardised. Inspect the design documentation supporting processing and verify that proper versions of the applications and data are being used.
Input reconciliation	Inspect periodic reconciliation procedures to determine whether reconciliations are performed and documented, inspecting some further for adequate supporting evidence. Determine if the system is configured to auto balance, where possible.

c. Output Controls

The objectives of output controls are measures built into the application to ensure that transaction output is complete, accurate, and correctly distributed. They also seek to protect data processed by an application from unauthorised modification and distribution.

The control processes include proper definition of outputs, desired reports at the system design and development stage, proper documentation of report extraction logic, controls limiting access to processed data, output review, reconciliation, and review. The following table lists key elements of output controls.

Elements of output control	Description
Integrity checks for completion and accuracy	Perform data integrity checks through reconciliation of process outputs to inputs for accuracy and completeness, according to documented procedures. Review output for acceptability and completeness, including of control totals and error logs. Review volume, value, and type of output against expectations.
Output review, follow-up, and tracking, including of processed results	Inspect management procedures for defining and assigning output or reports with relation to end user needs. Inspect reports tracking processing results, the content and timing of management reviews of processed results, and degree to which management monitors overrides applied to transactions. Review and follow-up of application-generated exception reports. Examine output reports for compliance with applicable laws and regulations.
Output labelling, handling, distribution, and retention	Inspect procedures in place to monitor use of output data in management reports or other external communications and inspect selected data from these communications. Ensure the user access to output data is aligned with their role.

d. Application Security Controls

Application security is concerned with maintaining confidentiality, integrity, and availability of information at the application layer. For the purpose of an audit of application security, it is important to understand the interfaces (i.e., the different sources of data input to and output from the application) and also the way data are stored.

Most applications are accessed through individual user IDs and passwords to the application. However, other forms of login have become increasingly popular, given the magnitude of applications used in a corporate environment. Therefore, the design of the application for user provisioning and access should be understood upfront. For example, an auditor might need to review an organisation's policies and procedures for obtaining and revoking user access in order to understand the access rules used by the application. User access can be governed locally by the application, or across multiple, related systems organisation-wide using a single sign-on scheme.⁷⁶

To be able to understand the application security control procedures, the auditor also needs to understand the actors, roles, and responsibilities involved with the application, such as administrators, power/privileged users, and regular users. An application's access control method can vary and can include a standard user ID and password model, use of digital certificates to affirmatively identify a user,⁷⁷ use of a token or biometric⁷⁸ information, and use of multiple methods in two-factor or multi-factor authentication.⁷⁹ Access may be controlled for each module, menu option, or screen in an application, or controlled through objects and roles. The IT auditor should review the design of the access control module, keeping in mind the criticality of the functions/actions available.

Examples of auditable issues regarding application security controls include the following:

- **Examination of audit monitoring and configuration management.** This examination includes traceability of transactions, such as transaction logging and audit trail logging; log reporting and monitoring; control of the movement of, and access to, programmes, data, and programme libraries; periodically assessing changes; and use of unique user IDs and roles in making changes. Ideally, an

⁷⁶Single sign-on permits a user to use one set of login credentials to access multiple applications.

⁷⁷Digital certifications are created by a trusted source to provide assurance on an individual's identification.

⁷⁸Biometric capabilities are used to identify individuals based on measurable anatomical, physiological, and behavioural characteristics.

⁷⁹Multi-factor authentication requires at least two different types of authentication elements in order to gain access.

audit trail log should record what records or fields were amended, when they were amended, from what to what, and who made the amendment.

- **Examination of access controls.** This examination includes a review of user accounts, permissions, and password management policies. use of guest, test, and generic accounts; privileged and administrator accounts use and compensatory controls; procedures for granting and revoking access; job termination procedures and access removal; adoption of the least privilege principle; IT/development team access to production databases; formal procedures for approving and granting access; use of strong passwords; periodic changes enforcement; and password encryption.
- **Control of the setup and maintenance of master data.** Master data are key information shared between multiple application functions. Controls include inspecting data configuration for key fields; ensuring that amendments to standing data are authorised and performed according to standing change rules; the standing data is up-to-date and accurate, and consistent across the organisation; and the integrity and confidentiality of the master data is maintained. Examples of standing data are supplier and customer details (name, address, telephone, account number); inflation rates; system administration data, such as password files and access control permissions.
- **Segregating user access.** User access should be segregated to conflicting transactions and activities, and this access should be monitored through formal operating procedures, supervision, and review.
- **Contingency planning.** This planning includes assessing the criticality and sensitivity of the application, evaluating steps to prevent and minimise potential damage or interruption to the application, and evaluating the organisation's broader contingency planning.

III. Interface and Data Management System Controls

In addition to the business process application controls above, interface and data management controls play a key supplementary role in ensuring applications function properly.

a. Interface Controls

Interface controls impact how business process applications interface with one another. They consist of those controls over the a) timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis, and b) complete and accurate migration of clean data during conversion. Interfaces result in the structured exchange of data between two computer applications. These applications may reside on the same or different computer systems, which may or may not reside in the same physical environment. Interfaces are periodic and recurring in nature.

The objectives of interface controls are to implement an effective strategy and design, and to implement processing procedures to ensure that interfaces are processed completely and accurately, errors are corrected, that access to interface data and processes are properly restricted, and that data are reliable and obtained only from authorised sources. To the extent that data input is obtained from other applications, an auditor's assessment of this data should be coordinated with the data input controls listed above.

b. Data Management Controls

Applications that support business processes typically generate, accumulate, process, store, communicate and display data. Applications that handle significant volumes of data often employ data management systems to perform certain data processing functions within an application. Data management systems use specialised software, which may operate on specialised hardware. Data management systems include database management systems, specialised data transport/communications software (often called middleware), cryptography used in conjunction with data integrity controls, data warehouse software and data reporting/data extraction software. Many of the data input and processing controls, such as edit checks, existence checks and thresholds described in previous sections are implemented in functions of data management systems. These types of controls implemented in data management systems are often referred to as business rules.

When assessing the effectiveness of application controls, the auditor should evaluate functions of data management systems specific to the business processes under review, in addition to general controls. In most large scale and/or high performance applications, various components of data management systems reside on different servers, which often employ various operating systems and hardware technologies. The auditor should obtain an understanding of the interconnected combination of data management technologies and appropriately consider related risks.

Understanding the logical design and physical architecture of the data management components of the application is necessary for the auditor to adequately assess risk. In addition to supporting the data storage and retrieval functions, it is typical for applications to employ data management systems to support operational aspects of the application, such as the management of transient user session state data, session specific security information, transactional audit logs and other functions that are essential to the application's operation. Controls associated with these types of functions can be critical to the security of the application.

Controls in a data management system should include consideration of the access paths to the data management system. Generally, access to a data management system can be obtained directly, through access paths facilitated by the application, or through the operating system underlying the database management system.

Data management systems have built-in privileged accounts that are used to administer and maintain the data management system. The auditor's objective is to determine whether appropriate controls are in place for securing these privileged accounts. In addition to privileged accounts, the auditor should obtain an understanding of the role the data management system plays in authentication and authorisation for the application.

IV. Risks to the Audited Organisation

Consequences of application control failures will usually depend on the nature of the business application. The risks can vary from user's dissatisfaction to real disasters and loss of lives. For example, the organisation may lose market share if a service becomes unavailable, the organisation may lose money if online sales systems are missing buying orders, the confidence of citizens in government services may decrease, the absence of compliance with legal standards can lead to court suits, electricity might not reach people's houses, and banking accounts might be susceptible to fraud.

Specifically, in the absence of proper input controls, organisations risk that erroneous or fraudulent processing may occur and that the application will fail to deliver business objectives. If this occurs, the data processed by the application might be inconsistent and improper output will be provided by the programmes. Further, it is possible to override system controls in very specific situations. In this case, there must be compensating controls such as logs and authorisation rules; otherwise, the override privilege might be misused and lead to inconsistent data entered into the application.

Managing source documents or avoiding improper data entry authorisation are also important input controls in mitigating risks to an organisation. In the absence of proper management of source documents, it might not be possible to trace the source of information in the system, legal compliance might not be achieved, and retention policies may be infringed, leading to unreliable data being inserted into the application. Conversely, in the absence of authorisation controls, unauthorised data might lead to errors or fraud.

Failure in processing controls may lead to processing errors and failure to meet business goals for the application. These failures might emerge due to incorrect mapping of business rules, inadequate testing of programme code, or inadequate control over different versions of programmes to restore integrity of processing after a problem occurs or unexpected interruption. In the absence of necessary processing control practices, there could be repeated erroneous transactions affecting business objectives and goodwill.

With real-time processing systems, some of the control measures are not available, such as reconciliation

of input and output batch totals for ascertaining completeness of input and retention of some data origination documents to maintain an audit trail log. However, real time systems embed other compensating controls within the application, including interactive data completeness, validation prompts, and logging of access attempts.

The lack of adequate output controls leads to the risks of unauthorised data modification/deletion, creation of wrongly customised management reports, and breach of data confidentiality. Also, the results of generating wrong output will very much depend on the way that information is used by the business.

In the application security context, the insufficiency of logging mechanisms may make it impossible to trace misbehaviour back to the specific authors. Also, the user awareness of the existence of logging review procedures and reporting mechanisms can mitigate the risk of information systems misuse. Standing data errors have a far-reaching effects on the application, since this data might be used for a very large extent of the application's transactions.

More broadly, insufficient use of information security controls can lead to risks with varying degrees of severity, including loss of income, service disruption, loss of credibility, business interruption, misuse of information, legal consequences, judicial cases, and intellectual property abuse. These risks and the mitigating controls are covered in more detail in chapter 7 on information security.

IV. References and Further Reading

Davis, Chris, Mike Schiller and Kevin Wheeler. *IT Auditing: Using Controls to Protect Information Assets*, 2nd ed. January 31, 2011.

ISACA. *IT Audit and Assurance Guideline G38, Access Controls*. 2007.

National Institute of Standards and Technology. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*, rev. 5.
<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>. September 2020.

Office of the Comptroller & Auditor General of India. *Manual of Information Technology Audit*, vol. I.
https://ag.ap.nic.in/GSSA/PDF_Files/ITAM_Vol_I.pdf.

U.S. Government Accountability Office. *Federal Information Systems Audit Manual (FISCAM)*.
<https://www.gao.gov/products/gao-09-232g>. February 2, 2009.