WGITA – IDI HANDBOOK ON IT AUDIT FOR SUPREME AUDIT INSTITUTIONS

INTOSAI
IDI
DEVELOPMENT INITIATIVE

This Handbook has been endorsed
by the XXI INCOSAI held in
Beijing, China, in October 2013

Published
February, 2014

Designed and printed by www.printhouse.no

PREFACE

The Information Technology (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 increasingly computerised operations of governments and public sector organisations. The IT systems being used should ensure that they protect the data and business assets of the organisation as well as support mission, financial, and other specific goals. While the increasing use of IT has led to improving business efficiency and effectiveness of service delivery, it has also brought with it risks and vulnerabilities associated with computerised databases and business applications, which typically define an automated working environment. The role of IT audit in providing assurance that appropriate processes are in place to manage the relevant IT risks and vulnerabilities is crucial if the SAI is to meaningfully report on the efficiency and effectiveness of government and public sector operations. In the IT audit environment, processes, tools, oversight, and other ways to manage a function are also referred to as controls.

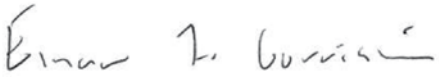
The INTOSAI Working Group on IT Audit (WGITA) and the INTOSAI Development Initiative (IDI) have jointly worked on producing an updated Handbook on IT Audit with a view to provide SAI auditors with standards and universally-recognised good practices on IT Audit. This Handbook provides a comprehensive explanation 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)*. 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 IT auditors with a complete set of guidance notes in IT audit.

The main objective of this Handbook is to provide the users with essential information and key questions needed for an effective planning of IT Audits. It is hoped that the handbook will be useful to SAIs in providing an extensive reference and practical guidance to conducting IT audits.

This project was jointly led by the chair of WGITA, namely SAI India and the IDI. WGITA member SAIs namely, the SAIs of Brazil, Indonesia, India, Poland, and the United States of America have worked together on developing this guidance. In particular WGITA and the IDI wish to thank the individual members of the team who worked relentlessly in developing this guidance. Many thanks also go to the SAIs that provided their valuable feedback and comments on the Handbook.

Shashi Kant Sharma
Comptroller & Auditor General of India
Chairman
INTOSAI Working Group on IT Audit (WGITA)



Einar J. Gørrissen
Director General
INTOSAI Development Initiative (IDI)

* www.issai.org

TEAM MEMBERS OF WGITA-IDI HANDBOOK PROJECT

1. Mr. Madhav S Panwar
Senior Level Technologist (Director), Government Accountability Office
of the United States of America

2. Mr. Paweł Banaś
Advisor to the President of Polish Supreme Audit Office (NIK)
Polish Supreme Audit Office

3. Mr. Neelesh Kumar Sah
Accountant General
Office of the Comptroller and Auditor General of India

4. Mr. Anindya Dasgupta
Director
Office of the Comptroller and Auditor General of India

5. Mr. Marcio Rodrigo Braz
Auditor
The Brazilian Court of Audit (Tribunal de Contas Uniåo)

6. Ms. Shefali S Andaleeb
Asst. Director General
INTOSAI Development Initiative (IDI)

7. Mr. Novis Pramantya Budi
Deputy Director
The Audit Board of the Republic of Indonesia

8. Ms. Ria Anugriani
Deputy Director
The Audit Board of the Republic of Indonesia

LIST OF ABBREVIATIONS

BCP	Business Continuity Plan/ Business Continuity Planning
BIA	Business Impact Assessment
CAATs	Computer Assisted Audit Techniques
COBIT	Control Objectives for Information and related Technology
DRP	Disaster Recovery Plan/ Disaster Recovery Planning
EUROSAI	European Organisation of Supreme Audit Institutions
GAO	Government Accountability Office, United States of America (USA)
ISACA	Information Systems Audit and Control Association
ISSAI	International Standards for Supreme Audit Institutions, sometimes, especially in older documents referred also as INTOSAI Standards
ISP	Information Security Policy
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology, US Department of Commerce
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
Wi-Fi	Wireless Fidelity

TABLE OF CONTENTS

INTRODUCTION

The advent of Information Technology has changed the way we all work in many ways, and the audit profession is clearly no exception. The almost ubiquitous computer, whilst undoubtedly one of the most effective business tools, has also brought with it vulnerabilities pertinent to the automated business environment. Each new vulnerability needs to be identified, mitigated, and controlled; assessing the adequacy of each control requires new methods of auditing[1].

Computers have matured from being merely data processing systems to the situation now where they collect, store and provide ready access to large amounts of data. This data is used in decision making and operating organisations' core business functions. Computers today communicate with each other and exchange data over networks – both public and private.

In fact, with the advent and growth of computer network systems, computer systems are now effectively information systems. As a reflection of this evolution, the term "EDP audit" has largely been replaced by such terms as "Information Technology Audit" and "Information Systems Audit".

With an increase in investment and dependence on computerised systems by audited entities, it has become imperative for the IT auditor to adopt an appropriate methodology and approach so that the audit can definitively identify risks to data integrity, abuse and privacy, and also provide assurance that mitigating controls are in place. In a typical IT system, especially when implemented in an environment of inadequate controls, the audited entity faces many risks that an IT auditor should be able to identify. Even when the audited entity has implemented some risk-reduction measures, an independent audit is required to provide assurance that adequate controls (General Computer Controls[2] and/or Application Controls[3]) have been designed and are operated to minimise the exposure to various risks.

CONTENT AND STRUCTURE OF THE HANDBOOK

This Handbook is intended to provide IT Auditors with a descriptive guidance on different domains in IT Auditing, as well as step-by-step guidance on how to plan these audits effectively.

In Chapter 1 of this guide, readers will find an overview of IT audit definition, SAIs' mandates, and the scope and objectives of IT audits. It also provides an explanation of IT General 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. A generic "Risk Assessment Checklist" is provided in Appendix I. The description of the IT Audit process is a generic one, based on standard audit methods

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

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

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

followed in a typical IT Audit. The users of the Handbook should refer to the manuals and audit procedure guidelines at their respective SAIs 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 their audits, either on a specific domain or a combination of domains depending on the scope and objective of IT audit being planned (financial or performance audit). For example, the guidance for the audit of IT governance can be used to plan an audit of the entity's IT governance mechanism, or for planning the audit of the general controls environment of which IT governance is an important part.

Each chapter is supported by a step-by-step guidance on developing an audit matrix provided in Appendices II-VIII. The audit matrix lists key audit issues, criteria, information required, and analysis methods. Users should note that the audit issues listed in the matrices are indicative and not comprehensive, and they are encouraged to develop the matrices according to the specific requirements of their audits. The template of the audit matrix is a generic one that could be used as working papers by the SAIs, or could be modified according to the SAIs' standards.

In addition, this Handbook includes an overview of emerging areas in IT Auditing. Chapter 9 highlights some of the areas that could be of interest to IT auditors, such as websites and portals, E-governance, Forensic Computer based audit, and Mobile Computing. This chapter contains an indicative list of audit areas and provides references to further reading for the interested user.

Technical guidance on the use of Computer Assisted Audit Techniques (CAATS) is beyond the scope of this Handbook. The SAIs are encouraged to organise separate training in CAATS 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: http://www.intosaiitaudit.org 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.

CHAPTER 1

INFORMATION TECHNOLOGY (IT) AUDIT

Introduction

In light of computerisation opportunities available across the world, organisations have been increasingly relying on the automation of their activities and information management. This forms the backdrop for auditors to gain assurance on such mechanisms and utilise the information available on such mechanisms for deriving appropriate audit conclusions.

This chapter provides an overview of the IT Audit process. It 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. The IT audit process depicted in this chapter is not documented in an international standard, but is a reflection of audit methodology embedded in the ISSAIs and other International Standards as well as of generally accepted audit practices followed by SAIs.

I. WHAT IS IT AUDIT

IT Audit is the process of deriving assurance on whether the development, implementation and maintenance of IT systems meets business goals, safeguards information assets and maintains data integrity. In other words, IT Audit is an examination of the implementation of IT systems and IT controls to ensure that the systems meet the organisation's business needs without compromising security, privacy, cost, and other critical business elements.

I.1 Mandate for IT Audits

The mandate of an SAI to conduct an audit of IT systems is contained in ISSAI 1—Lima Declaration[4]. By extension, the mandate of an SAI for IT audit is derived from the overall mandate provided to the SAI to conduct financial, compliance, performance audits or a combination of these[5]. Some SAIs may also have a specific mandate for conducting IT Audits. For example, if the SAI has a mandate to audit a tax revenue function, the SAI must audit the automated portion of the tax revenue function through a derivation of its original mandate.

I.2 IT Audit Objectives

The objective of IT Audits is to ensure that the IT resources allow organisational goals to be achieved effectively and use resources efficiently. IT audits may cover ERP Systems, IS Security, acquisition of

[4] INTOSAI *Lima Declaration*, Part VII Section 22

[5] ISSAI *100 Fundamental Principles of Public Sector Auditing*.

the business solution, System Development, and Business Continuity – all of which are specific areas of IS implementation, or could be to look at the value proposition the IS Systems may have fulfilled.

Some examples of audit objectives are:

- Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness.
- Evaluation of the processes involved in the operations of a given area such as a payroll system, or financial accounting system.
- Evaluation of the performance of a system and its security, for example, a railway reservation system.
- Examination of the system development process and the procedures.

I.3 Scope of IT Audit

Generally Supreme Audit Institutions (SAIs) perform IT Audits in conjunction with a financial statements audit, a review of internal controls, and/or as Performance Audits of IT Systems or IT Applications. In broad terms, IT audits pervade Financial Audits (to assess the correctness of an organisation's financial statements); Compliance/ Operational Audits (evaluation of internal controls); Performance Audit (including Information Systems topics); Specialised Audits (evaluation of services provided by a third party such as outsourcing etc.); and forensic audits and Information Systems' (IS) development projects audits.[6]

Irrespective of the type of audit, the IT auditor would be required to assess the policies and procedures that guide the overall IT environment of the audited entity, ensuring that the corresponding controls and enforcement mechanisms are in place. The scoping of the IT Audit would involve deciding the extent of audit scrutiny, the coverage of IT systems and their functionalities, IT processes to be audited, locations of IT systems[7] to be covered, and the time period to be covered. It will be, essentially, setting or delineating the boundaries of the audit.

I.4 IT Controls

Figure 1.1 General and Applications Control

A control is the combination of methods, policies, and procedures that ensure protection of the organisation's assets, accuracy and reliability of its records, and operational adherence to management standards.

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

The IT General Controls are the foundation of the IT Control structure. These are concerned with

[6] See EUROSAI database on IT Audit Reports for different kinds of IT Audits- http://egov.nik.gov.pl/

[7] Location would include the back-end servers (application or data or otherwise), user locations, networks in a generic manner and would also determine the physical locations to be covered in a distributed network across buildings, cities or countries, if applicable.

the general environment in which the IT systems are developed, operated, managed and maintained. General IT controls establish a framework of overall control for the IT activities and provide assurance that the overall control objectives are satisfied.

General controls are implemented using a number of tools such as policy, guidance and procedures as well as putting in place 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 IS Strategy and an IS Security Policy, setting up of an IT steering committee, organisation of IS staff to separate conflicting duties, and planning for disaster prevention and recovery.

Application Controls are specific controls unique to each computerised application. They apply to application segments and relate to the transactions and existing data. Application controls include data input validation, encryption of data to be transmitted, processing controls, etc. 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.

I.5 IT General Controls and Application Controls and their relationship

IT general controls are not specific to individual transaction streams or particular accounting packages or financial applications. The objective of IT general controls is to ensure the appropriate development and implementation of applications, as well as of program and data files and of computer operations.[8]

The design and implementation of IT general 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 changes cannot be made to either the applications (i.e. they are protected from reprogramming) or the underlying databases (the large collection of transaction data).

Most common IT general controls that enhance application controls are[9]:

- Logical access control over infrastructure, applications and data
- System development life cycle controls
- Program change management controls
- Physical access controls over the data centre
- System and data back-up and recovery controls
- Computer operations controls.

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

I.6 Why are IT controls important for the IT auditor?

Generally, the IT auditor is called upon to test technology-related controls, whereas non-IT auditors test financial, regulatory and compliance 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

[8] *ISACA, IS Auditing Guidelines-Applications Systems Review*-Document GI4, p3

[9] *Global Technological Audit Guide (GTAG) 8- Auditing Applications Controls*

audited entity so as to deliver assurance on internal controls operating in an entity. As per ISSAI Fundamental Principles of Public Sector Auditing: "auditors should obtain an understanding of the nature of the entity/programme to be audited"[10]. 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. The role of the auditor is to understand the potential business and IT risks facing the audited entity, and in turn to assess whether the deployed controls are adequate to meet the control objective. In the case of IT general 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. As ISSAI 1315 points out that even in small entities where information systems and business processes relevant to financial reporting are less sophisticated, their role is significant. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications.

In subsequent chapters, some of the key areas of IT General Controls and Applications Controls are discussed in detail. Suggested audit matrices for each of the control areas are provided in the Appendices.

II. IT AUDIT PROCESS

PLANNING FOR IT AUDITS

Audit planning is a key part of any audit, including IT Audit. In most SAIs, planning for audits is carried out at three levels – Strategic planning, Macro or Annual planning, and Micro or Entity level planning.

II.1 Strategic planning

A Strategic Plan of the SAI is a long-term (3-5 years) forecast of audit targets and objectives for the audit, including those of IT systems and respective organisations under jurisdiction of an SAI.

In some SAIs, only a list of new and emerging areas to audit with respect to IT may be included in their strategic plan. These could include looking at new methods of systems development (for example, agile programming) and acquisition or perhaps cloud computing in the public sector.

In either case, the strategic planning process and the SAI's strategic plan provides the tone and direction of an SAI's IT Audit goals for the future.

[10] *ISSAI 100* paragraph 49.

II.2 Macro planning

The macro level of audit planning is usually done on an annual cycle basis at the level of the SAI[11] for selection of the audit areas. With the rapid proliferation of modern IS systems across governments and the limitation of resources available to SAIs, **a risk-based approach** to prioritise and select suitable topics would be appropriate. Furthermore, the SAI will additionally have to incorporate obligatory audits, like those demanded by law or requested by Parliament, Congress or other oversight entities.

i. Risk-based approach

Usually SAIs have under their audit mandate a number of 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.

Steps in 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 in 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 should outline the priority, approach and schedule of IT Audits. This exercise could be done at annual intervals and thus could be a recurring plan.

Steps in Risk based Approach for Planning IT Audits

While there are risks inherent to information systems, these risks impact different systems in different ways. The risk of non-availability even for an hour can be serious for a billing system at a busy retail store. The risk of unauthorised modification can be a source of fraud and potential losses to an online banking system. A batch processing system or a data consolidation system may be relatively less vulnerable to some of these risks. The technical environments in which the systems run also may affect the risk associated with the systems.[12] A risk-based approach in selecting IT systems for audit assists the auditor in deciding the priority of audits. To use the risk assessment framework, an SAI needs to have some minimum information across agencies, usually gathered through a survey.

While a risk assessment process is one way to select the audited entity for IT audit, the SAIs also select auditable entities on a cyclical basis, using mandated audits or on account of specific requests from oversight bodies (Congress, Parliament, Legislature, etc.).

II.3 Micro (or Entity level) Planning

Micro planning involves the development of a detailed audit plan for audit of the selected audit entity, beginning with outlining the audit objectives. The audit plan will assist auditors in preparing an IT audit programme. The pre-requisite step in developing the audit programme will be to have a clear understanding of the audited entity and its Information Systems. This Handbook aims to assist the auditor once a plan has been created to populate the audit matrix with specific audit

[11] The 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 (stage two for planning) is carried out at field level.

[12] S Anantha Sayana-ISACA

objectives for each area (governance, information security, etc.) that will be investigated. Micro level planning requires an understanding of the organisation and some preliminary assessment of controls to facilitate detailed audit planning.

i. Understanding the Organisation

The extent of knowledge of the organisation and its processes required by the IT Auditor are largely determined by the nature of the organisation and level of detail in which audit work is being performed. 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 entire business process has been mapped in an IT environment[13]. 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 IS auditor should be alert.

A typical layout of an IS system in an organisation is given below:

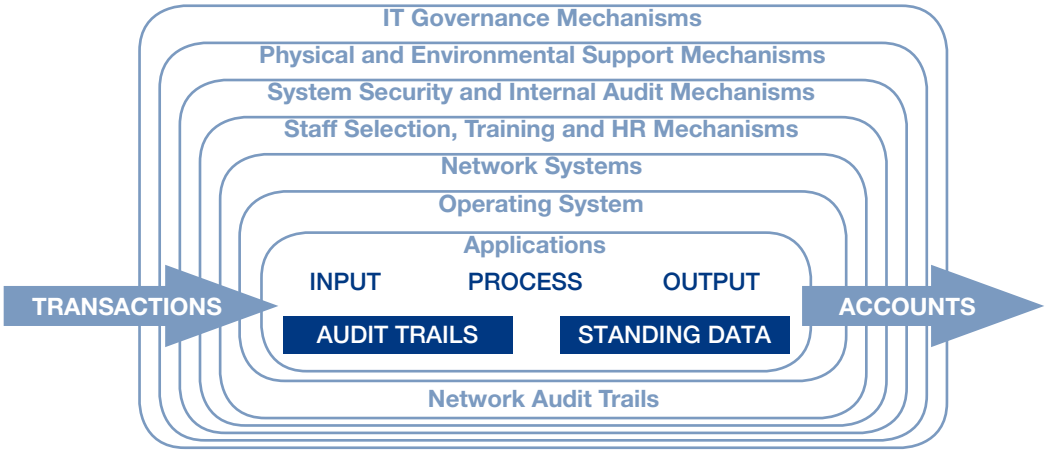


Figure 1.2: Typical IT layout in an organisation

A typical application forming the core of an IT System in a computerised organisation, will have a combination of database management system with specific databases, application software(s) mapping the business rules in the system through specific modules, 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 computers 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.

Based on the understanding developed of the Information System and the audited entity, IT Auditors may decide on their approach for IT Audits. IT Audit would eventually involve audit of General and/or Application Controls.

[13] Organisations changing over from a manual to a computerised environment would normally conduct a Business Process Reengineering (BPR) exercise. It may be possible that some of the business processes are being carried out manually along with the IT Systems. These particular scenarios would present specific interest areas for IT Auditors.

ii. Materiality

The materiality[14] of IT Audit issues should be determined under the overall framework for deciding materiality policy in a SAI in formulating an audit report. The auditor should consider the materiality of the matter in the context of the financial statements (regularity audit) or nature of the audited entity or activity.

The IS auditor should determine whether any IT general deficiency could potentially become material. The significance of such deficient IT general 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 IT general 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 an IT general control deficiency and its associated reflection on the control environment could become material when aggregated with other control deficiencies affecting the control environment[15].

iii. Allocation of Resources

IT Audit requires specific allocation of resources, especially manpower which needs to be well acquainted with typical IT systems, processes and mechanisms that govern a successful IT implementation. Apart from suitable staff resources[16], appropriate budget, infrastructure[17] and any other requirements identified should be provided for. The timeline for audit should be decided, if possible, in consultation with the audited entity.

iv. Engagement with the audited entity

The audited entity 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 entity where it may also set out the terms of such engagements. The SAI should ensure that due cooperation and support of the audited entity is sought in completing the audit, including access to records and information, whether, manual or electronic.

v. Gathering audit evidence

1. Preliminary Assessment of IT controls

The IT Auditor should conduct a preliminary assessment of IT Controls in the system under audit to derive an understanding of assurance that existing controls (General Controls and Application Controls) are reliable. The assessment of controls at this level would include:

a. Assessment that suitable IT Governance mechanisms are in place and functioning.
b. Assessment that IT objectives are aligned to the business objectives.

---

[14] *ISSAI 100* paragraph 43 defined "Materiality is often considered in terms of value but the inherent nature or characteristics of an item or group of items may also render a matter material".

[15] *Materiality Concepts for Auditing Information*, ISACA Guidelines (G6)

[16] Suitable staff resources would mean personnel who have an understanding of the Information Systems and could carry out data extraction and analysis if required, as IT Audits invariably would require use of IT skills for carrying out the audits. The SAI should refer to ISSAI 100 paragraph 52 on providing for necessary competence to its staff before undertaking an IT Audit.

[17] Would include the hardware platforms, operating systems, RDBMS, as well as storage devices, computing facilities like PCs, laptops etc. to be able to extract and analyse information.

c. Assessment that suitable mechanisms are in place for the acquisition of an IT solution (encompassing, IT application, hardware, software, human resources, network, service solutions etc).
d. Organisation-level controls embedded in IT operations that govern day-to-day IT functions, the organisation's information security procedures, business continuity and back-up procedures, change management and service delivery and feedback.

The above comprise general IT controls, which are not specific to any individual transaction stream or application but are concerned with the organisation's overall IT infrastructure, including IT-related policies, procedures and working practices. The tests have to be specifically designed using techniques including[18] interviews, surveys through questionnaires, observations, walk through[19], data capture and analysis, and vouching, etc.

2. Substantive Testing

In substantive testing the tests are designed to substantiate the assertions as per audit objectives. Substantive testing involves detailed testing of the IT Controls employing various techniques and tools for inquiry, extraction and data analysis.

Data analysis involves the items listed below[20]:

- Identify the purpose of the analysis or project
- Understand the sample(s) under study
- Be cognisant of data layouts and formats[21]
- Establish a unique identifier if matching or merging is necessary
- Statement of research questions / audit objectives
- Methods used to answer research questions
  * Criteria for evaluation
  * Evidence
  * Analysis
  * Conclusion
- File restructuring procedures (syntax creation, adding new variables as needed)
- Data-cleaning procedures (e.g. removing outliers).

Most analysis can be executed straight from a working data file. Some analysis may require transformations of the raw data, subsets, or specific input data to comply with statistical software. IT systems use many different data types and representations (numeric, string, alpha, etc). The IT auditor should be cognisant of these and use the appropriate tools for analysis. The auditor can use Generalised Audit Software or Specialised Audit Software to carry out the information analysis. Tools such as Microsoft Excel, Microsoft Access, IDEA, ACL etc. are examples of generalised audit software that provide the facility to import as well as analyse data.

---

[18] The techniques can be used for both preliminary and substantive testing. The IT Auditor can pick one or more of these techniques while conducting any of the two assessments.

[19] Walk-through tests are conducted to understand and establish the reliability of a client's IT Systems and internal control procedures. This test is more suited for either understanding the IT System or for verification of findings from Preliminary tests or results of other substantive tests. Thus it may not strictly be a test of controls.

[20] Jonathan Steinberg, *An Overview of Data Analysis*; Bruce A. Kaplan *Data Analysis Research*; Muhamad Jantan *Introduction to Data Analysis*

[21] This would be one of the most important steps before conducting data analysis. Layout would mean understanding of different databases, tables within, coding pattern utilised and relationships between table and databases. An understanding of different database models will be helpful in this regard.

Thereafter any of the following techniques, as per the requirement can be adopted by the IT Auditors such as:

a. Carry out data extraction by **obtaining a copy of data** from the audited entity. IT Auditors may have to create similar environments (operating system, database management system, hardware etc.), as at the audited entity to analyse/ extract data from the copy of data. The IT Auditor may also be required to convert data from one form to another to facilitate better reading and analysis.
b. Utilise the audit software for extracting data from varied combinations of operating system, database management systems, application system etc. IT Auditors can use **Generalised Audit Software** or **Specific Audit Software**. Generalised Audit Software could also be used for specific industries or can be the utility software that can be used to assess the functioning of various utilities of the computer systems. The usage of any of these or a combination thereof will depend on the audit objectives and scope to be covered in IT Audits.
c. Perform **test data** in situations where the quality of the programme is intended to be tested. The premise is that it is possible to generalise about overall reliability of a programme if it is reliable for a set of specific tests. Use of Test data involves ***Designing*** of Test Data and ***Creating*** of Test Data before running the programme with the test data.

The IT Auditor should 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.

III. AUDIT DOCUMENTATION

Information systems' audit documentation is the record of the audit work performed and the audit evidence supporting audit findings and conclusions. Preservation of the audit results and the audit 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 audit 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 file 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 may include 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 IS auditor should ensure that these reports carry the source of the report, the date and time and the conditions covered.
- At various points in the documentation, the auditor may add his comments and clarifications on the 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.

- For preserving electronic data, the SAIs should provide for a back-up of data received from the audited entity 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.
- 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.
- The draft and final reports of the audit should form part of the audit documentation.

IV. SUPERVISION AND REVIEW

The work of audit staff should be properly supervised during the audit[22], and documented work should be reviewed by a senior member of the audit staff[23]. The senior member of the audit staff should also provide necessary guidance, training and a mentoring role during the conduct of audit, which will be crucial in this new area – IT Audit.

V. REPORTING

An IT Audit report should follow the general layout of 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 their findings in a timely manner, and the findings should be constructive and useful to the audited entity 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.

VI. STAGES OF REPORTING

There are various ways to meet ISSAI requirements related to the concluding stage of the audit process. They depend on the traditions of Supreme Audit Institutions and their legal environment. One of them consists of three stages of reporting in the audit process, namely:

VI.1 Discussion Paper

The reporting process begins with the discussion of the first draft (discussion paper). This draft is sent to the client's middle 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 client and the auditor have discussed the contents of the discussion draft, the auditor makes the necessary amendments and sends the client the first Formal Draft.

[22] *ISSAI 100* paragraphs 39, 41

[23] *ISSAI 100* paragraph 54.

VI.2 Management Letter

The Management letter is the formal draft given to the auditee so that they 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.

VI.3 Final Audit Report

When client'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 entity'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 by the audited entity or by the auditor, including conclusions or recommendations[24].

VI.4 Formulation of conclusion and recommendations

Audit findings, conclusion and recommendations must be based on evidence. In formulating the audit conclusion or report, the IT Auditor should have regard to the materiality of the matter in the context of the nature of the audit or audited entity[25].

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

IT Auditors should report recommendations when the potential for significant improvement in operations and performance is substantiated by the reported 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, are action-oriented and specific, are addressed to parties that have the authority to act, are feasible, and, to the extent practical, are cost-effective.

For balanced reporting, noteworthy accomplishments should be reported upon, if they fall within the mandate of reporting for the SAIs.

[24] *ISSAI 100* paragraph 55

[25] *ISSAI 100* paragraph 54.

VI.5 Limitations to IT Audit

Limitations to the IT Audit should also be pointed out in the report. The typical limitations could be inadequate access to data and information, lack of adequate documentation of the computerisation process, leading the IT Auditor to devise his or her own methods of investigation and analysis to derive conclusions. Any other limitation faced by the IT Auditor should be pointed out in the report appropriately.

VI.6 Agency 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 about these efforts.

References:

1. *COBIT 4.1 Framework*, 2007, IT Governance Institute
2. IDI AFROSAI/E-IT Audit Courseware
3. *ISSAI 100 Fundamental Principles of Public Sector Auditing*
4. *ISSAI 200 Fundamental Principles of Financial Auditing*
5. *ISSAI 300 Fundamental Principles of Performance Auditing*
6. *ISSAI 400 Fundamental Principles of Compliance Auditing*

AUDIT MATRIX TEMPLATE

Use of Audit Matrix

During the planning stage, it is useful to develop an audit matrix covering all the relevant issues for audit as per the audit objective and scope of audit.

Though different SAIs use different formats of audit matrices for planning their audits, there is an overall uniformity in the information captured in the audit matrices.

A suggested format for an audit matrix[26], also utilised in this Handbook, is as below:

AUDITABLE AREA	
Audit objective:	
Audit Issue:	
Criteria:	
Information Required	Analysis Method(s)
Audit Conclusion To be filled in by auditor:	

1. Auditable Area

IT Auditors should be able to identify auditable issues during the preliminary assessment stage which comproses of a preliminary assessment of the entity and its environment, particularly the IT environment.

The auditable issues will also arise from the audit scope of IT audit. For example, in many SAIs an IT audit would be conducted in conjunction with financial and compliance audit and will involve an assessment of the IT general and application controls. In other cases, the IT audit scope could be an assessment of the entity's actions in procuring or developing new ITR systems. More and more SAIs are also conducting a full performance audit of critical IT systems. Some examples are revenue/ tax

[26] Audit Matrix outlines important Audit issues, criteria etc. under different IT Audit Areas. What is important for an IT Auditor to understand is that this matrix should be prepared at the planning stage, though the contents can be updated during IT audit process, if necessary. SAIs can make necessary modifications to the audit matrix format as well, if they deem it necessary.

assessment and collection system , railway reservations system, computerisation of civic services like property registration, population statistics and national identification numbers etc.

The auditable issues can arise both from the IT related or other governance issues, which have an impact on IS in the audited entity.

2. IT Auditors should also identify evaluation criteria that should be measurable, reliable and consistent with the audit objectives/ issues being investigated by the IT Auditor at this stage.

To satisfy the criteria, adequate information or evidence needs to be identified and collected in a manner that can be preserved for future reference to support audit conclusions. The collection of information may require specific tools and techniques. Different tools and techniques need to be identified and utilised, especially during the substantive testing stage .The analysis methods also are typical to the IS environment and need to be suitably utilised to derive relevant and meaningful conclusions. This is dealt with in the subsequent topic on substantive testing under Audit Execution.

Identifying sources of information

The typical sources of information in an organisation having IT Systems can be:

a. The flow diagrams including system flow diagram, data flow diagram, process flow diagram etc.
b. System development documents such as the User Requirement Specification (URS) document[27], and System Requirement Specification (SRS).
c. Electronic data.[28]
d. Other information available in the organisation related to its functions, control and monitoring systems etc. such as forms, budgetary information, different reports including reports from previous audits, external audits, internal reviews etc.
e. Policy, procedures, and other guidance.
f. The users of the system.

Identifying Techniques and Tools for gathering information

The audited entities will have their own combination of hardware, operating system, database management systems, application software and network software. IT auditors should be able to gather information from these sources to carry out their analysis. Understanding of the IT System and database in the organisation is clearly an essential step for data extraction.

IT Auditors should decide on the appropriateness of the use of one or more of the above techniques and ensure that they are satisfied with the integrity and usefulness of the technique. The use of any of the above techniques should not impact the integrity of application system and its data at the audited entity.

[27] URS – *User Requirement Specification Document* contains requirements that show the functions of the organisation that the IT system is supposed to carry out and the end user operability desired. This is the stage where a complete and clear delineation of user's requirements should be specified by the users. A deficient user requirement specification may ultimately lead to development of a deficient system. This is a good starting point for the IT Auditor.

[28] Electronic data would include structured data where the most common ones are Relational Database Management Systems (RDBMS) that are capable of handling large volumes of data such as Oracle, IBM DB2, Microsoft SQL Server, Sybase, and Teradata.

Data gathering techniques should be based on risk assessment carried out by the audit team, as well as the time and resources available for the audit.

Suggested audit matrices for different auditable IT areas are provided in Appendices II-VIII of this Handbook.

CHAPTER 2

IT GOVERNANCE

I. WHAT IS IT GOVERNANCE

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

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.

There are various standards and frameworks that define IT Governance principles and concepts and how an organisation may choose to implement them.

A generic IT governance framework is represented in the Figure 2.1

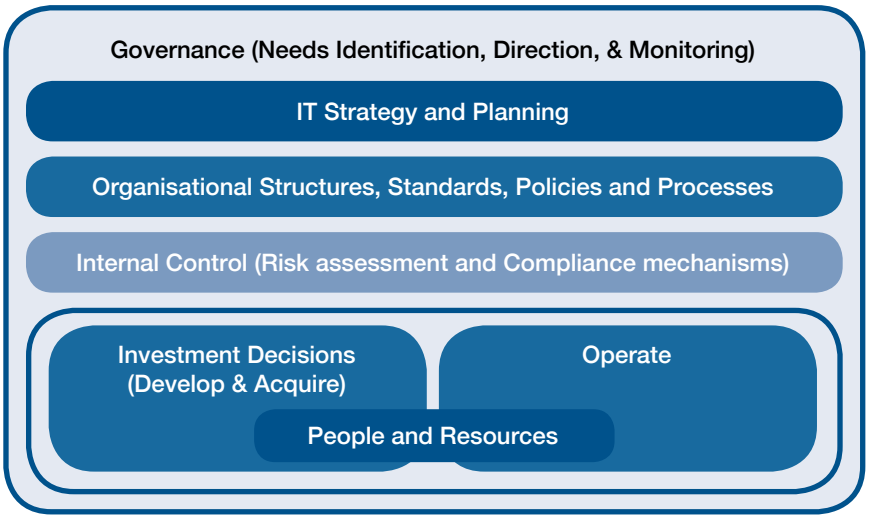


Figure 2.1 Generic IT Governance Framework

I.1 Needs Identification, Direction, & 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 decision-making process. This creates a shared acceptance of responsibility for critical systems, and ensures that IT-related decisions are made and driven by the business and not vice versa.[29]

For IT Governance to ensure that the investments in IT generate business value, and that the risks that are 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.

It is also essential that IT Governance is involved with identifying new or updated business needs, and then providing 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 (hardware, tools, network capacity, etc.) 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.

Key elements that define the IT governance of an organisation are described below.

II.2 Key elements of IT Governance[30]

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 the requirement of resources.[31] The strategy should consider the existing IT infrastructure and architecture, investments, delivery model, resourcing including staffing, and lay out a strategy that integrates these into a common approach to support the business objectives.

It is important for the IT auditor to review the IT strategy of the entity in order to assess the extent to which IT governance has been a part of the corporate decision-making in deciding the IT strategy.

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 delegation 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 entity 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.

[29] *What is IT Governance and Why is it Important for the IS Auditor*: WGITA IntoIT Issue 25, August 2007

[30] The key elements presents in this IT Governance chapter are supported by COBIT 5 Framework and ISO 38.500 with and extensive use of its definitions and examples

[31] ISO 38.500.

Internal users are the business executives, functional departments who own business processes, and individuals within the organisation who interact with business processes. External users are the agencies, individuals, public who use products or services provided by an organisation (for example other departments, citizens, etc.). 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 are required to 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[32].

c. IT organisational structure usually includes following functions:

IT Steering Committee – this is the central piece of the organisational structure. It comprises members of top and senior management and has the responsibility for reviewing, endorsing and committing funds for IT investments. The Steering Committee 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 of "build vs. buy" solutions are the responsibility of the IT Steering committee generally after suitable recommendations from designated groups or committees.

Finally, 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.

Chief Information Officer (CIO) – is a senior person who is responsible for the management and operation of organisation's IT capabilities. In many public sector organisations, the functions carried out by the CIO may be conducted by a group or department which has the necessary responsibilities, authority and resources.

d. Standards, Policies and Processes

Standards and policies are adopted by the organisation and approved by senior management. Policies lay the framework for daily operations in order to meet the goals set by the governing body. Polices are supported by procedures and/or processes that define how the work is to be accomplished and controlled. These goals are set by the senior management to accomplish the organisation's mission and at the same time to comply with regulatory and legal requirements. Policies and corresponding procedures need to be communicated to all relevant users in the organisation on a periodic basis.

Some of the key policies that guide the IT Governance include:

- **Human Resource Policy**

The HR policy deals with the hiring, training, job termination and other functions of the HR 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 HR policy also assigns roles and responsibilities and segregation of duties.

[32] *COBIT 5* – Appendix E Mapping of COBIT 5

- **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 entity.

- **Outsourcing policy**

IT outsourcing is most often aimed at allowing the entity'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 outsoursing operations, and/or functions, database and soon are developed and implemented in a manner which is in beneficial to the organisation.

- **IT security 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 (personnel records, financial input data, etc.).

II.3 Internal Control

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 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.[33]

a. Risk Management[34]

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 infrastructures, and continuous management, including an annual / periodic review and update by the management of the risks and monitoring of mitigation strategies.

b. Compliance mechanism

Organisations need to have a compliance mechanism that ensures that all the policies and associated procedures are being followed. Basically it is the organisation's culture which makes all the employees sensitive about all non-compliance issues. The compliance supporting mechanism may also include the quality assurance group, security staff, automated tools, etc. A report of non-compliance should be reviewed by appropriate management and serious or repeated non-compliance issues must be dealt with. Management may choose to deal with non-compliance with refresher training, modified

[33] *IT Governance in Public Sector: A top priority*- WGITA IntoIT Issue 25, August 2007

[34] See chapter 7 on IT Security for more detailed description.

procedures, or even an escalating retribution procedure depending on the nature of the non-compliance (security violations, missing mandatory training, etc.).

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.

I.4. Investment decisions (development & acquisition of solutions)

IT governance should provide business users with solutions to their new or modified requirements. These can be accomplished by the IT department either through developing (building) new software or systems or acquiring these from vendors on a cost-effective basis. In order to achieve these successfully, best practices typically require a disciplined approach where requirements are identified, analysed, prioritised and approved, a cost-benefit analysis conducted among competing solutions and the optimum solution selected (for example, one which balances cost and risk).

I.5 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 (additional hardware, or network resources), measures performance to ensure it meets the agreed-upon needs of the business owners, and provides help desk and incident management support to the users of IT resources.

I.6 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 or not resources are being used and prioritised as the business objectives demand.

II. RISKS FOR THE AUDITED ENTITY

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, the auditor needs to know the key components of IT Governance and Management. The auditor needs to be aware of the risks associated with the inadequacy of each component in an entity.

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

a. Ineffective, inefficient or user-unfriendly 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. They should thus be properly designed, tailored to the real needs, competently coordinated, and efficiently run. Poor IT governance at the level of government and at the level of individual organisations can be the first obstacle to having good quality IT systems.

b. Direction-less IT function not serving the business needs:

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.

c. 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 have and periodically update the IT Strategy, which would identify resources and plans to meet future needs of the business.

d. 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, most importantly, human resources available to deliver IT services is the key factor in achieving value from investments in IT. Defining and monitoring the use of IT resources, for example in a service level agreement, allows the organisation to objectively know if resources requirements are adequate to meet the business needs.

e. Inadequate decision making:

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

f. 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 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 and life cycle* (SDLC) and its use in development and/or acquisition is a way to reduce the risk of project failures.

g. Third party (vendor) dependency:

Since there are no proper processes controlling 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 if it fails to deliver the contracted services, the organisation is going to be in difficult position. There are also other issues, for example, disputes over intellectual property, systems, 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.

h. 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[35]. So, in the absence of adequate organisational structures, strategies, procedures, monitoring controls, the institution may fail to be fully accountable and transparent.

i. Non-compliance with legal and regulatory statements:

Stakeholders require increased assurance that enterprises are complying with laws and regulations and conforming to good corporate governance practice in their operating environment. In addition, because IT has enabled seamless business processes between enterprises, 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 (COBIT 5 Framework, Principle 5, and Conformance). The various policies that an organisation has,such as IT Security, Outsourcing, HR, etc. must incorporate the relevant legal and regulatory frameworks.

j. Exposure to Information Security Risks:

A lot of information security risks may arise from the absence of proper structures, processes and policies, such as: misappropriation of assets, unauthorised disclosure of information, unauthorised access, and vulnerability to logical and physical attacks, disruption and information unavailability, misuse of information, noncompliance with personal data laws and regulations, failure to recover from disasters. The IT security policy should define organisational assets (data, equipment, business processes) that need protection and link to procedures, tools, and physical access control that protect such assets.

IT Governance continues to be an area of concern for most public sector organisations. At the same time, many SAIs are increasingly focusing on IT Governance as part of their IT Audits. IT Auditors could assist IT Governance by:

Ensuring that IT Governance is on the agenda of overall corporate governance, and promoting IT Governance strategies.

Audit Matrix

The audit matrix in Appendix II is a starting point for auditors to assess the mitigating controls that the organisation has put in place and for managing the risks it faces in IT governance or lack thereof. It contains the areas discussed above.

It is important to note that IT governance issues will form part of the auditors' overall assessment of an organisation's general control environment.

[35] *ISSAI 20, Concepts of accountability and transparency,* p.4.

References / Further Readings:

1. *What is IT Governance and why is it important for the IS auditor*, WGITA, IntoIT. http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf
2. *COBIT 4.1 Framework*, 2007, IT Governance Institute
3. *COBIT 5 Framework*, 2012, ISACA
4. ISO/IEC 38500 Corporate Governance of Information Technology
5. *OECD Principles of Corporate Governance*, OECD, 1999 and 2004
6. Michaels Paul; Anand, Navin; and Iyer, Sudha; *What is IT Governance*. Computer World UK. April, 2012 http://blogs.computerworlduk.com/management-briefing/2012/04/what-is-it-governance/index.htm
7. http://www.gao.gov/new.items/d04394g.pdf

CHAPTER 3

DEVELOPMENT & ACQUISITION

I. WHAT IS DEVELOPMENT & ACQUISITION

In order to support the business strategy, IT organisations provide solutions to the business or the business user. The process of developing, acquiring, or contracting out for a solution 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 guarantee the quality of these solutions.

Commonly, solutions will be built or acquired by a project team structure. Although sometimes organisations may not formalise a project, the common activities still need to be accomplished.

The solutions can be provided either by internally developing them or externally acquiring them through acquisition or contracting or outsourcing process. Very often, a mixed approach combining these preceding approaches is utilised.

According to Carnegie Mellon University's CMMI® for Acquisition, Version 1.3, organisations are increasingly becoming acquirers of needed capabilities since products and services are readily available and are typically cheaper than building 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. When done in a disciplined manner, acquisition 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, of course, requires that the organisation has an understanding of its needs and requirements. The requirements' identification process should involve all relevant stakeholders who are involved in the business process, including end users and technical staff who may need to eventually maintain and support the system. When acquiring services (help desk, desktop automation, etc,) the requirements' identification should include the IT department that will interface with the service provider. Requirements must be prioritised so that if there is a budget shortfall or other cost constraints, some can be deferred to future builds or acquisitions as appropriate.

The definitions of requirements is only the first step in the acquisition process. Acquisition requires many additional areas to be managed, for example, risk, programme management, testing, vendor oversight both during acquisition and later if they operate or support the system, and internal training integration and/or implementation issues. There are certain best practices that when adopted, raise the likelihood of success in the acquisition of products or services.

I.1 Key elements of Development & Acquisition

a. Requirements Development & Management

For any project development or acquisition, the organisation needs to document the requirements of what it wants/needs and to manage those requirements. Managing requirements includes prioritising them, utilising adopted criteria (for example criticality, cost, and complexity), and segmenting them into phases if they all cannot be implemented in one initial system. In addition to business owners, the requirements identification process should include users, support staff, experts in the domain, and other stakeholders as appropriate. The requirements form the basis of the solicitation (request for proposal) package, and should be clear and concise. By analysing and prioritising requirements, the organisation is able to make cost and other trade-off decisions in order to get the optimum solution.

b. Project Management & Control

Project management includes defining the project plan & control activities. Project management includes defining cost and schedule baseline, 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. The project management structure should be described in the organisation's adopted System Development Life Cycle approach or acquisition strategy as appropriate. Generally it consists of a project manager, risk officer, quality assurance and configuration management support staff, personnel from the testing group if not part of quality assurance, etc. 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. Additionally 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.

c. Quality Assurance & 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 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. Agencies need to verify that the developed or acquired product meet the requirements, meet the acceptance criteria (for example, less than a certain number of non-critical errors, etc.) and have undergone testing with the 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 and/or informal) are conducted and the necessary status reports are sent to appropriate stakeholders and management. Further through the involvement of quality assurance staff senior management enforces or get information on whether the project team is following internally-set policy and procedures for the acquisition or development effort.

d. Solicitation

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 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. It is critical that the project team involve their legal department in this process. The legal team is well 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.

e. Configuration Management

Configuration Management (CM) is used to ensure that the integrity of documents, software and other descriptive or support materials that are part of the system 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. Configuration management personnel are also 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 (regression testing or integration testing).

II. RISKS FOR THE AUDITED ENTITY

When an agency is developing in-house software, there are a number of risk or challenges that it faces in ensuring project success. Some of these include 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.

Additionally, the software or system requirements gathering and approval should include users, and auditors will look at whether the users were consulted in the definition of the requirement whether personnel involved in the quality assurance area are objectively appraising 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 agency 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 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.

Audit Matrix

The audit matrix for this selection can be found in Appendix III.

References/ Further Readings:

1. http://www.dodig.mil/Audit/pmeguide.html
2. *DCAA Contract Audit Manual*. USA, 2013
3. http://www.dcaa.mil/cam.htm
4. CMMI for Development, Version 1.3
5. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm
6. CMMI for Acquisition, Version 1.3
7. http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm
8. ISACA – *System Development & Project Management Audit / Assurance Framework*
9. *COBIT 4.1 Framework*, 2007, IT Governance Institute. Acquire and Implement

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 information systems of a business (running servers, maintenance, providing necessary storage, running a helpdesk, etc.). The operations are measured and managed using Key Performance Indicators for IT operations (KPIs) that set parameters against which operational effectiveness can be measured. These measures or their equivalent are typically documented and reviewed periodically. Most organisations document these in some sort of an agreement between the business users and the IT organisation. The internal Service Level Agreement (SLA) is one such formal agreement, where these parameters and other arrangements are documented.

II. KEY ELEMENTS OF IT OPERATIONS

Some of the areas or elements of IT Operations that the auditor will need to look at to determine whether the agency is effectively managing IT Operations include, service design and delivery, capacity and service management, incident handling procedures for ensuring continuity of operations, and practices involved in managing change. These and other areas are defined in ITIL[36], one of the more widely adopted frameworks for identifying, planning, delivering and supporting IT services to the business.

To determine whether the audited entity is effectively delivering the documented services the auditor should use the SLA that should include the specific parameters for the various services. There might be instances in smaller organisations where instead of an SLA the agreement between the business and the IT group may be documented in a business chart or some other document. Regardless of what the document is called, it must be documented and agreed to by the business or users groups and the IT organisation.

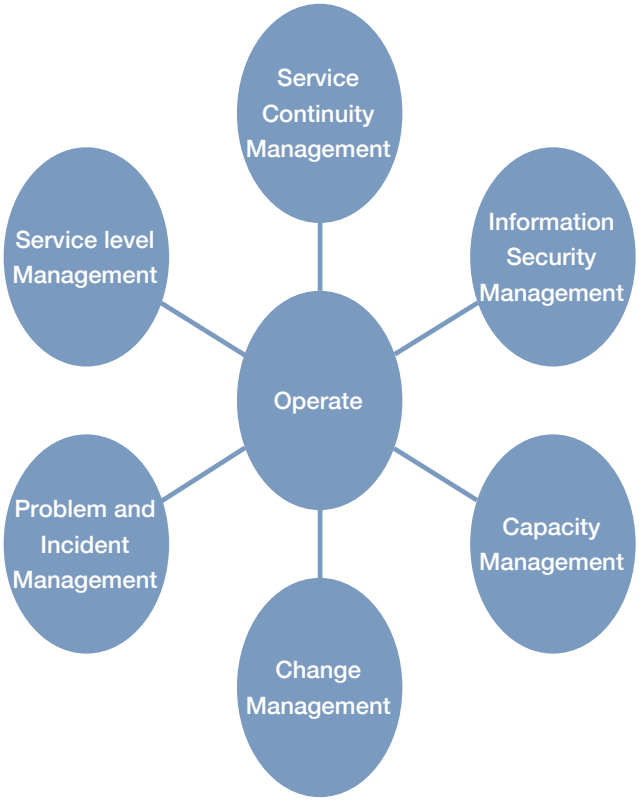


Figure 4.1 Domains of IT Operations

[36] ITIL, http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

a. IT Service Continuity management

The purpose of continuity management is to maintain the appropriate ongoing business continuity requirements. The IT organisation accomplishes this by setting recovery time targets for the various IT components that support the business processes based on agreed-to needs and requirements. Additionally, continuity management includes periodically reviewing and updating recovery times 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. Information Security Management

The management of information security relates to managing security-related risks, taking action as appropriate, and ensuring that information is available, usable, complete, and un-compromised 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.

c. Capacity Management

Capacity Management includes managing the various services that support the business in a manner that keeps up with the demands of the business or users. Optimising network throughput capacity, resource availability, storage optimisation and augmentation 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 by acquiring additional processing power when certain parameters are crossed (i.e. when computer utilisation is at 75% or greater for 60% of the workday). Additionally, for an IT organisation providing services to the business, capacity management would be effective when suitably qualified/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.

d. Problem and Incident 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 incidents 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 mechanism should be put in place for the detection of and documentation of conditions that could lead to the identification of an incident. The IT operation section should have documented procedures for detecting and recording abnormal conditions. A manual, computerised log of dedicated IT software may be used to record these conditions. Examples of incidents could include both unauthorised user access or intrusion (security), network failures (operational), low functionality of software (service delivery) or lack of end user skills (training).

e. Change Management

In IT organisations, the change management process is normally used to manage and control changes to assets, 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/record of changes.

An unapproved or accidental change could have severe risks 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 initiated e.g. by change of business environment, modification of business model, inter-operational needs or by the outcome of incident/problem analysis. Change control procedures should include procedures for management authorisation (on standard proforma or documenting process for recording Request For Change (RFC); 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 establishment of procedures for making emergency changes.

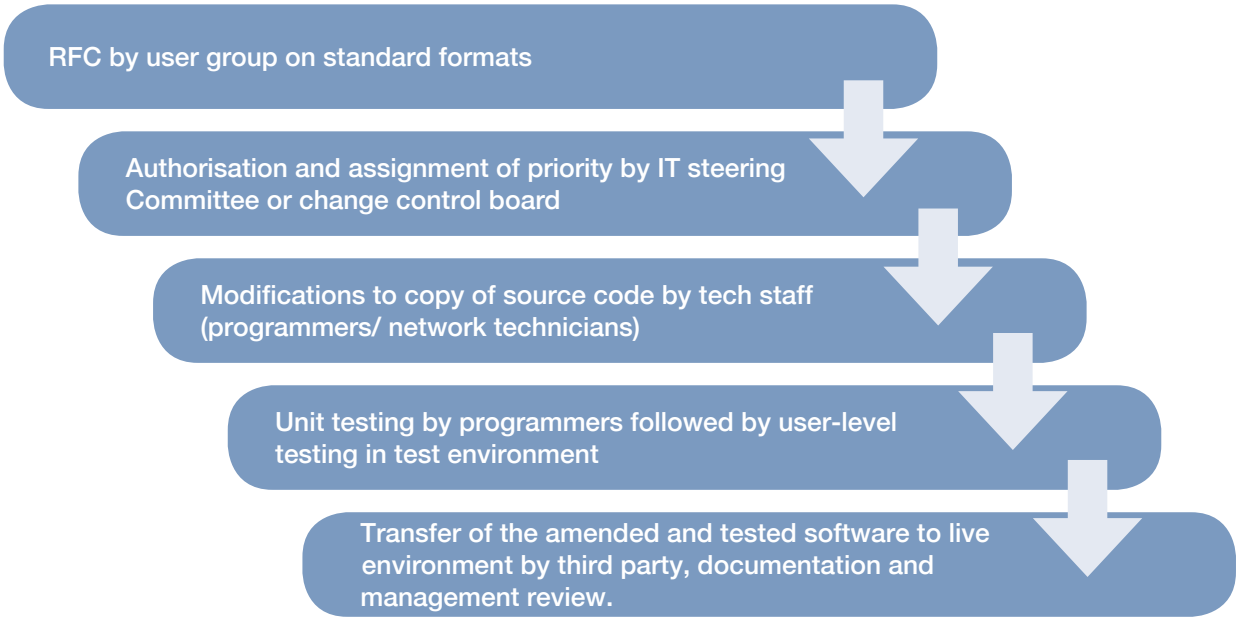


Figure 4.2: Steps in Change Management

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 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 change/s. This 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 (use of automated change control applications), retrospective approval from the change board/ system owner, retrospective testing and documentation update.

f. Service Level Agreement (SLA)

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. Generally, there is also an SLA or other formal agreement between an IT organisation and their vendor(s). For example, an IT Organisation may have multiple SLA's between themselves and the various vendors who provide them outsourcing or cloud computing services. The SLA we are discussing here is the internal SLA between the IT Organisation and the business customers within the organisation.

The SLA contains, among other items, the Key Performance Indicators (KPI) for the IT services. Review of KPI's 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, addressing gaps identified and following up on the implementation of corrective action taken as a result of evaluating of the entity's performance.
- Identifying control issues in the 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 unauthorised changes	Percentage reduction in the number of incidents resulting from unauthorised access	Tracked through Incident Management, Change Management and reported monthly.

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. Detailed guidance on audit of IT Outsourcing is provided in Chapter 5 of the Handbook.

II. RISKS FOR THE AUDITED ENTITY

The main tool for the auditor, as noted previously, is the Service Level Agreement. This lays out the parameters and performance indicators and requirements to which the IT organisation must be measured against. If this document is lacking or not formally reviewed and approved by the business owners, there is a risk that the IT resources of the organisation may not be utilised in the most effective or efficient manner. When auditing IT Operations, the auditor will need to get the document where the overall goal and technical parameters for the IT operations are defined, typically in the SLA.[37]

[37] After getting the SLA, 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 (storage, CPU, network resources, etc.) 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.

Audit Matrix

The audit matrix for this section can be found in Appendix IV.

References/ Further Readings:

1. *CISA Review manual*. ISACA. 2011
2. *CISA Item Development Guide*. ISACA.
3. http://www.isaca.org/Certification/Write-an-Exam-Question/Documents/CISA-Item-Development-Guide.pdf
4. *COBIT 5*, 2012.
5. www.uservices.umn.edu/.../sla/BEST_PRACTICE_Service_Level_Agreement
6. *NIST – Computer Security Incident Handling Guide*
7. http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.pdf
8. ISACA Change Management Audit Assurance Programme
9. ISACA – Security Incident Audit Assurance Programme
10. What is ITIL http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

CHAPTER 5

OUTSOURCING

I. WHAT IS OUTSOURCING

Outsourcing is the process of contracting an existing business process that an organisation previously performed internally or a new business function to an outside entity. The contracted entity is responsible for providing the contractually required services for an agreed fee. An agency may choose to outsource selected parts (or all) of its IT infrastructure, services or processes. The agency should have a policy or vision on what aspects or the business functions (typically IT but could be others) it outsources and which functions it will keep in-house. Depending on the criticality of the outsourced service, an organisation may choose to go with greater or lesser formal controls on the outsourced service. IT organisations may decide to outsource all or some of their operations because outsourcing offers certain advantages which include:

- **Staffing flexibility**

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.

- **Staff development**

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. As such, by relying on the physical locations of the vendor and vendor's technical expertise, the organisation may be able to have internal staff working alongside the vendor personnel for a period of time, thus providing a hands-on training to the staff.

- **Cost Reduction**

Outsourcing should typically result in cost reduction by shifting labour and other costs to the vendor which has a lower labour cost. 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 training. Organisations that do not have an on staff 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.

- **On-Call Experts**

Outsourcing enables the organisation to have on-call experts waiting in the wings to assist with existing or emerging issues. The entity is able to quickly respond to changing business needs (new mission or taking on additional functions) with the help of the expert.

• Examples of Outsourcing

According to the ISACA paper on outsourcing[38] entities can outsource various areas of business and IT Infrastructure. Some of them include:

- 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.

A recent development in outsourcing is **Cloud Computing**[39]. In this case the organisation outsources data processing to computers owned by the vendor. Primarily the vendor hosts the equipment, while the audited entity still has control over the application and the data. Outsourcing 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 they want their 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 (laptops with Wi-Fi or cell/mobile cards, smart phones, and tablets).

Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, rather than through a local computer.

I.1 Key elements of Outsourcing

a. Outsourcing Policy

Organisations need to have some policy that defines what functions can be outsourced and what functions must remain in-house. Typically organisations outsource routine IT operations, maintenance and even desktop hardware platforms. HR and personnel records are generally kept 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.

The auditor should begin with looking at the outsourcing policy and procedures of the audited entity. In bigger entities, which often have a large share of their business operations outsourced, it is essential that they have an approved outsourcing policy including clearly laid-down solicitation processes. Smaller organisations may not have a formal policy, but should follow efficient and transparent solicitation procedures.

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.

[38] Outsourced IT Environments Audit /Assurance Programme, 2009.

[39] See WGITA Guide and Handbook on Audit of Cloud Computing.

c. Vendor / contract Management

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

The auditor will need to look at whether the agency has determined their requirements for the outsourcing function prior to selecting the vendor (the specific requirements and operational parameters are in the contract and the SLA), whether the agency is monitoring that the vendor is meeting the requirements stated in the SLA (via periodic status reports), and if the agency has taken action when the vendor does not meet stipulated SLA parameters (corrective measures or payment penalties).

d. Service Level Agreement (SLA)

The Service Level Agreement (SLA) is a documented agreement between the organisation and the vendor to whom the services are outsourced 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.

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 (defect rates, response time, help desk staffing hours, etc.)
- Time to implement new functionality, rework levels
- Type of documentation required for applications developed by the vendor
- Location where services are to be performed
- Frequency of back-up, data recovery parameters
- Termination and data delivery methods and formats
- Incentive and penalty clauses.

In short, most of the items that are critical to the organisation must be put in a service level agreement. The IT auditor needs to ask for the SLA or other document (contract or formal agreement) where these parameters are documented, and ensure that the reporting from the vendor on various parameters is meeting the requirement or that the organisation has taken the necessary corrective action to address the deficiencies.

e. Benefit Realisation

Generally audited entities 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 and 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 their expertise for special cases. Whenever possible the entity should try and determine if the projected savings are being achieved on a periodic basis. This serves as one of the data points to decide whether to continue or stop with the outsourced capability.

f. Security

While outsourcing databases and its administration, IT organisations must evaluate whether vendors have sufficiently robust security practices and if vendors can meet the security requirements, internally. 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 would include possible mishandling or disclosure of 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.

II. RISKS TO THE AUDITED ENTITY

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 for some reason in unable to provide this service, Government IT organisations must be ready to assume this duty again. Also, as the development of the application would happen 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 their 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. This will also help the organisation to switch service providers, if required.

b. Vendor failure to deliver

At times a vendor might just fail to deliver a product either on time or the product must be abandoned due to lack of correct functionality. If the solicitation process is not implemented correctly there is a high likelihood that the system or services being acquired may not meet user needs, will be sub-standard, 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/or 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, system development will assist the organisation in ensuring business continuity through another service provider or by themselves.

c. Scope Creep

All outsourcing contracts contain baselines and assumptions. If the actual work varies from estimates, the client will pay the difference. This simple fact has become a major obstacle for IT organisations that are surprised that the price was not “fixed” or that the vendor expects to be paid for incremental scope changes. Most projects change by 10-15% in terms of specifications during the development cycle.

d. 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% range, and creating contractual terms around those levels is a reasonable request.

e. External (Overseas) 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.

Audit Matrix

The audit matrix for this section can be found in Appendix V.

References/ Further Readings:

1. Davison, Dean. *Top 10 Risks of Offshore Outsourcing*. 2003. http://www.zdnet.com/news/top-10-risks-of-offshore-outsourcing/299274
2. *Outsourced IT Environments Audit /Assurance Program*, 2009. ISACA. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx
3. *Governance of Outsourcing.* ISACA, 2005. http://www.isaca.org/Knowledge-Center/Research/Documents/Outsourcing.pdf
4. *Guideline on Service Agreements: Essential Elements* Treasury Board of Canada Secretariat www.tbs-sct.gc.ca
5. NIST SP 500-292, *Cloud Computing Reference Architecture*
6. NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing.*

CHAPTER 6

BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY PLAN (DRP)

I. WHAT ARE BCP AND DRP

Government organisations have come to rely increasingly on the availability and correct operation of their computer systems in order to discharge their statutory obligations. Computer systems play an important role in such diverse activities such as the assessment and collection of taxes and customs revenues; the payment of state pensions and social security benefits; and in processing national statistics (births, deaths, crime, diseases, etc). In fact, many activities cannot be carried out effectively – if at all – without the support of computers.

Loss of power, industrial actions, fire, and malicious damage can all have disastrous effects on computer systems. It may take many weeks for an organisation to resume effective business operations if they do not have a workable business continuity plan in place.

The terms Business Continuity Plan and Disaster Recovery Plan 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. The two are explained below:

- **Business Continuity Planning (BCP)** 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).

- **Disaster recovery planning (DRP)** is the process of planning and testing for recovery of information technology infrastructure after a natural or other disaster. It is a subset of Business Continuity Planning. BCP applies to the organisational business functions whereas DRP to the IT resources that support the business functions.

In essence, **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 and crisis management activities. As such, in these organisations, business continuity is seen as an all-encompassing term that covers both disaster recovery and the resumption of business activities.

However, whether as a part of the BCP or a separate document, **DRPs** 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 a company when restoring affected business processes, by

outlining the specific steps the company 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.[40]

I.1 Key elements of BCP and DRP

The IT auditor is required to assess the entity's business continuity management programmes, which involves evaluating its disaster recovery and business continuity plans and crisis management systems. To do this, auditors need to understand what is involved in developing a business continuity management strategy and the steps they should take to evaluate the effectiveness of existing programmes that incorporate necessary business continuity, disaster recovery, and crisis management efforts.

An effective continuity planning has several phases common to all information systems. The generic steps in the process are[41]:

1. Business Continuity policy and plan
2. Organisation of Business Continuity function
3. Business Impact Assessment (BIA) and Risk Management
4. Preventive controls including environment controls
5. Disaster Recovery plan
6. Documentation of the business continuity plan
7. Plan testing and training
8. Security during the BCP/ DRP implementation
9. Back-up and disaster recovery for outsourced services.

These steps represent key elements in a comprehensive business continuity planning capability. The elements are explained as below:

a. Business Continuity Policy, Plan and Organisation

An effective continuity planning starts with the establishment of an organisation's business continuity policy. The business continuity management team[42] representing all appropriate business functions also plays an important role in the success of the organisation's business continuity plan. The Business Continutiy Planning policy statement should define the organisation's overall continuity objectives, and establish the organisational framework and responsibilities for continuity planning.

b. Establishment of Business Continuity Function

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

---

40 *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

41 NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems*, provide guidance on the contingency planning processes

42 Explained in the following section.

c. Business Impact Assessment and Risk Management

i. Assessment of criticality and sensitivity of computerised 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 determines which are the most critical and what resources are needed to recover and support them. This is carried out by carrying out a risk assessment, identifying probable threats and their impacts on the organisation's information and related resources including data and application software, and operations. The risk and 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 highlight such instances in time.

ii. Identification and prioritization of critical data and operations

The criticality and sensitivity of various data and operations should be determined and prioritised based on security categorisations and an overall risk assessment of the organisation's operations. 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 one-day interruption of major tax or fee-collection systems 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 computer 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 non-computerised records.

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

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 employees 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.

v. Prevention and minimisation of potential damage and interruption

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

- Routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage; and/or arranging for remote back-up facilities that can be used if the entity's usual facilities are damaged beyond use.
- Establishing an information system recovery and reconstitution capability so that the 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.
- Effective hardware maintenance, problem management, and change management.

vi. Implementation of data and program backup 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 computerised 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.

vii. 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.

viii. 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.

d. Preventive 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 computer facilities.

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 shut-down procedures during extended power outages.

e. Disaster Recovery Plan

A disaster recovery plan 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. It is important that these plans be clearly documented, communicated to the affected staff, and updated to reflect current operations.

i. Documentation of up-to-date recovery plan

Disaster recovery plans should be documented, agreed on by both business and information security departments, and communicated to affected staff. The plan should reflect the risks and operational priorities that the entity has identified. It 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 continuity plan should be available, with some stored at off-site locations to ensure they are not destroyed by the same events that made the primary data processing facilities unavailable.

ii. Alternate site arrangements

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 computer hardware and telecommunications services as well as with suppliers of business forms and other office supplies.

f. Testing

i. Periodically testing of the continuity plan

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 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 people has occurred. It is important for top management to assess the risks of continuity plan problems, 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 plan. As such, they should be reported to top management so that the need for modification and additional testing can be determined, and so that top management is aware of the risks of continuing operations with an inadequate continuity plan.

g. Security

The security of the resources and operations should be in-built in the business continuity plan 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 data recovery for outsourced services

Many organisations outsource all or part of their activity 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 business continuity and disaster recovery plan is in-built in 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 an application software being maintained by the service provider. The ownership of the business process should be retained by the organisation. The organisation should also have a continuity plan to ensure continuity on the service provider winding up their business or being taken over by another company.

II. RISKS TO THE AUDITED ENTITY

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. BCP/DRP 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 agencies serve many mission-critical needs (payments to citizens, providing 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 agencies have a BCP / DRP process that ensures that the agency is able to continue to serve citizens.

In assessing whether the BCP / DRP processes are able to guarantee and protect the reliability and continuity of IT Infrastructure and business process, there are some audit risks that auditors can focus on when assessing the effectiveness of a business continuity and disaster recovery plan. These would involve the development of disaster recovery and business continuity plans to cover all critical functional areas. If the disaster recovery of a critical functional area is compromised, the business continuity will be compromised. If the roles and responsibilities are not clear and understood by relevant personnel, a good continuity plan may also become ineffective.

The procedure of business impact assessment, preventive and environmental controls, documentation, testing of the continuity plan and training of the concerned personnel support the effective implementation of business continuity plan of the organisation. Deficient security in the implementation of business continuity plan and disaster recovery plan pose the risk of 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 the BCP and DRP are not fully under the control of the organisation. There are risks of security of data, loss of data, unauthorised handling and leakage of data that need to be addressed. The continuity of the function through the outsourced service provider itself presents a risk through either loss of the business knowledge, process ownership and thus inability to change the service provider in case of deficient performance and in other cases the closure or takeover of the service provider by other entities.

Audit Matrix

The audit matrix for this section can be found in Appendix VI.

References:

1. GAO *Federal Information Systems Audit Manual* (FISCAM)
2. *COBIT 4.1 Framework*, 2007, IT Governance Institute
3. NIST *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34
4. *The IT Auditor's Role in Business Continuity Management*, Internal Auditor, January 2008 edition.

CHAPTER 7

INFORMATION SECURITY

I. WHAT IS INFORMATION SYSTEM SECURITY

Information Security can be defined as the ability of a system to protect information and system resources with respect to confidentiality and integrity. The protection of information and information systems against unauthorised access or modification of information, whether in storage, processing, or transit, and against denial of service to authorised users. Information security includes those measures necessary to detect, document, and counter such threats. Information security allows an organisation to protect its Information System infrastructure from unauthorised users. Information security comprises computer security and communications security.

A fundamental aspect of IT governance is the security of the information to ensure its **availability, confidentiality** and **integrity** – on which everything else depends. Information security needs to be many things to the enterprise. It is the gatekeeper of the enterprise's information assets. That calls for the 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. Providing information to those who should have it is as significant as protecting it from those who should not have it. Security must enable the business and support its objectives rather than becoming self-serving.

I.1 The necessity of Information Security

Information Security is increasingly more important for government institutions 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.

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 does not have a guarantee of information security then it will deal with the risks and 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 information technologies grow, 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:

- **Law** – violations of legal and regulatory requirements.
- **Reputation** – damage to the organisation's standing, causing breach of trust with other organisations or damaging the image of government or state.
- **Finance** – e.g. fines, compensations, reduced sales, repair or restore costs.
- **Productivity** – reduction of effectiveness and/or efficiency in a project, programme or whole service provided by the organisation.
- **Vulnerability** – systems and data accessed in an unauthorised way are prone to malware and may be opened for further intrusions.

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.

I.2 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[43]. The elements 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 their information security responsibilities. The human resources function may be responsible for initial awareness training for new employees. The training should proceed during their employment and up to the termination should 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 any other employee's 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, it should be considered to form cross-functional teams. The use of cross-functional teams encourages communication and collaboration and reduces departmental isolation and duplicated efforts.

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

[43] ISACA Business Model for Information Security, 2010.

- **Alignment of information security and business objectives:** It is necessary for aligning information security and business objectives since it enables and supports business objectives. The information security programme aligns with the organisation, and requires information security controls to be practical and provide real, measurable risk reduction.

- **Risk Assessment:** The application of information security must be complemented by risk assessment, to determine the form of control required. Often risk assessment is ignored, which may result in under protection of sensitive infratructure and information , or in some cases wasteful overprotection. The application of risk assessment will help management to select appropriate controls to mitigate risk effectively.

  The risk assessment process includes the identification and analysis of:

  * All assets and processes 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.
  * Selection of appropriate security measures and analysis of the risk relationships.

- **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 one to another areas, impacts and supports the 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.

I.3 Key elements of Information Security

a. Information Security Environment

To support the successful implementation of Information Security effectively, there are some critical elements that must be met. These are:

- **Confidentiality** is preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The confidentiality aspect is very important because it involves privacy issues that must be provisioned. To constantly maintain it, the system must ensure that each individual keep up the right to control on what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for.

- **Integrity** is guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity[44]. To certify the integrity of the information, an authentication mechanism is necessary to ensure that users are the persons they claim to be. While the process of ensuring that the information created or transmitted needs to meet the requirements of non-repudiation[45].

[44] **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.

[45] **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.

- **Availability** is ensuring that all information systems including hardware, communication networks, software applications and the data they hold shall be available to users at necessary times to carry out business activities. It should also ensure timely and reliable access to and use of information. However, meeting the security principle on the use of hardware, communication networks, software applications, and on the use of 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.

Information security is about minimising exposure, based upon risk management, in all areas of 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 the 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.

The discussion of Information Security in organisation covers 12 domains which are:

b. Risk assessment

Risk assessment is the process of identification, analysis, and evaluating risks in the IT Security infrastructure. It is the process of assessing security-related risks from internal and external threats to an entity, its assets, and personnel.

c. Security Policy

The organisation's security policy is the set of laws, rules, and practices that regulate how an organisation manages, protects, and distributes resources to achieve specified security objectives. These laws, rules, and practices must identify criteria for according 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.

A recommended form of IT Security policy is given below:

Elements of an IT Security Policy	Definition of information security – objectives and scope (including data confidentiality)
	Detailed security principles, standards and compliance requirements • 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, Internet
	Mode and method of access
	Back-up procedures
	Procedures to deal with malicious software/ programs
	Elements of security education and training
	Process for reporting suspected security incidents
	Business continuity plans
	Methods of communicating to staff the policy and procedures adopted for IS security

d. Organisation of IT security

Organisation of the IT security implies implementing the security policy for the entity. This could be the work given to a unit or an individual, who work with the IT organisation to acquire appropriate tools and implement the right processes to implement the security policy effectively. They are additionally responsible for providing the initial and refresher training to the staff and address security incidents. There is also a need to ensure that the data of the organisation that is accessed by or transferred to external organisations is suitably protected. The auditor will need to see if this entity is able to implement the IS requirements as documented by the organisation.

e. Communications & Operations Management

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

f. Asset management

Asset management, broadly defined, refers to any system whereby things that are of value to an entity or group are monitored and maintained. Asset management is a systematic process of operating, maintaining, upgrading, and disposing of assets cost-effectively.

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

For a government entity, IT asset management is very important in the current fiscal environment because financial constraints may not allow them to replace lost or stolen assets in a reasonable manner. Furthermore, the organisation may be at risk if they do not have a full inventory of their assets when they need to upgrade software to meet future business needs.

g. 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 institution'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 topic 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 company'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 or Change of Employment:** To prevent unauthorised access to sensitive information, access should be revoked immediately upon termination/separation 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.

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

h. 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; and 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 (for example, limiting access within a facility and/or to specific assets, and environmental controls to reduce physical incidents such as fires and floods).

Security inevitably incurs costs and, in reality, it can never be perfect or complete – in other words, 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 authorized from unauthorized people (e.g. using pass cards/badges 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 CCTV systems).
- Trigger appropriate incident responses (e.g. by security guards and police).

i. 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 computer-based IT system. 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 is another means of access control as well as biometric devices. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment.

In a government environment, access control is important because many government entities process sensitive data and privacy concerns limit who should view various parts of the information. Access control ensures that only users with the process credentials have access to sensitive data.

j. IT systems acquisition, development and maintenance

The Systems Development Life Cycle (SDLC), or software development process in systems engineering, IT systems and software engineering, is a process of creating or altering IT systems, and the models and methodologies that people use to develop these systems. In software engineering, the SDLC concept underpins many kinds of software development methodologies. These methodologies form the framework for planning and controlling the creation of an IT system or the software development process.

Maintenance of an IT system during its life cycle includes changes and updates to the system as a result of new requirements, fixing of system errors, and enhancements made as a result of new interfaces.

k. IT security incident management

In the fields of computer security and information technology, 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.

l. Business continuity management

Business Continuity Planning is the process an organisation uses to plan and test the recovery of their 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).

m. Compliance

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

II. RISKS TO THE AUDITED ENTITY

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 all significant risks identified at most organisations:

- Unauthorised disclosure of information
- Unauthorised modification or destruction of information

- Vulnerability of IS attack
- Destruction of the IS infrastructure
- Disruption of access to or use of information or an information system
- Disruption of information system processing
- Information or data stolen.

Looking for 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 IS responsibility structure
- Inappropriate **human resources** solutions
- Ineffective use of **financial resources** allocated to information security, information security **value** (cost-benefit) structure not aligned with business needs or goals
- Information security not **monitored** or monitored ineffectively.

The auditor should begin with assessing the adequacy of risk assessment methods and take into consideration 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 can be used. At the end, the auditor may develop a detailed audit programme according to the needs and development during the audit fieldwork.

When carrying out an information security audit, the auditor should address issues related to the 12 domains (as above) in information security[46].

Audit Matrix

The audit matrix for this section can be found in Appendix VII.

References/ Further Reading:

1. ISSAI 5310 *Information System Security Review Methodology*
2. ISO 27000 series *Information Security Management System*
3. ISO 27005 *information security risk management*
4. ISACA *RiskIT Framework*
5. *COBIT 4.1 Framework*, 2007, IT Governance Institute
6. *COBIT 5 Framework*, 2012, Isaca
7. ISACA ITAF – *A Professional Practices Framework for IT Assurance*. USA. 2008
8. ISACA *Information Security Audit/Assurance Program*, 2010
9. ISACA *IT Risk Management Audit/Assurance Program*, 2012
10. COSO *Enterprise Risk Management Framework*.

[46] ISO 27000 series *Information Security Management System*.

CHAPTER 8

APPLICATION CONTROLS

I. WHAT ARE APPLICATION CONTROLS

An application is specific software used to perform and support a specific business process. It may include both manual and computerised procedures for transaction origination, data processing, record keeping and report preparation. Each entity would be likely to 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, possibly, an integrated (ERP) enterprise resource planning system.

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.

Since application controls are closely related to individual transactions, it is easier to see why testing the controls will 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. It would not be obvious that testing the client's general IT controls (e.g. change control procedures) would provide a similar level of assurance for the same account balance.

Depending on the specific audit goals, the application review might have different approaches. So the way controls should be tested may vary from one audit to the other. For instance, the application review might be focused on legal and standards compliance, so the main point is to verify whether application controls properly help addressing those issues. From another perspective, the application review might be a part of a performance audit, thus it is 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.

The steps to be performed in carrying out an application controls review might involve a cyclical process of activities. Even though it might be interesting to start from the business perspective, it is

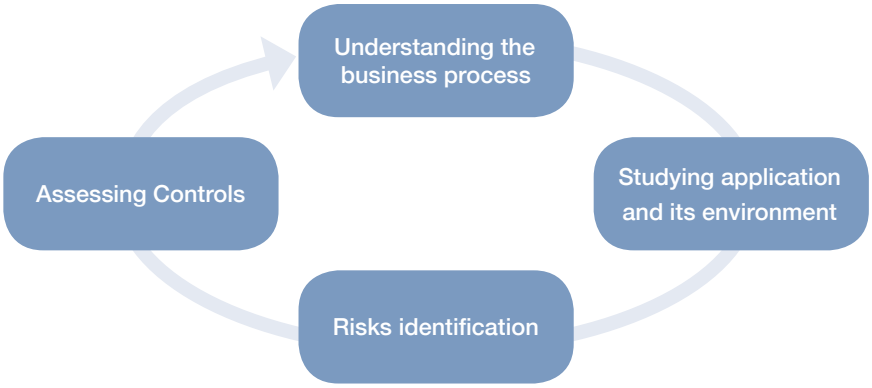


Figure 8. 1
Application Review Cycle

important to note that there is no strict heirarchy among these steps. Some of them are listed below and are briefly described in the following sections.

- **Understanding the business process:** before exploring technical matters regarding the application, it might be useful to obtain an overview of the business processes automated by the application – its rules, flows, actors, roles and related compliance requirements. Understanding the underlying business is an important step to be able to verify the consistency of the application controls and the automated processes. The extent of this step will vary according to the audit objective. It is usually done through the study of the operating/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.

- **Studying application and its environment:** study the design and behaviour of the application either by reviewing documentation (organisation diagrams, dataflow diagrams, user manuals) or by interviewing key personnel. Study key functions of the software at work by observing and interacting with operating personnel during work. Through discussions, perform a walk-through of the business process and application from source entry through output and reconciliation to see how processes actually flow and observe any associated manual activities that could act as complementary controls. Discuss with managers, operators and developers and obtain documentation on technical infrastructure: operating system, network environment, database management system, interfaces with other applications, sourced in-house or outsourced, batch entry/ real-time/ online transaction processing. This gives an indication of how the tech infrastructure impacts the application.

- **Risks identification:** mainly to identify risks associated with the business activity/function served by the application (what can go wrong?) and to see how these risks are handled by the software (what controls it?). Sometimes a business process risk assessment might be already available (it might have been done by a previous audit, internal audit or by management) and the auditor could benefit from its use after assessing the confidence of the existent risk assessment.

- **Assessing controls:** after being aware of the environment (business and technical) surrounding the application the auditor might be more confident to assess the controls used to address the existent risks. The auditor should use judgment when assessing the application controls and should be careful when putting forwards recommendations for improvements. For example, excessive details in transaction logging may add to entity cost overheads, and may not indicate desired trails. The assessing would involve the evaluation of different kind of application controls that are described in the following section.

I.1 Key elements of application controls

Application Controls are specific controls unique to each computerised application. When business processes are automated into an IT application, the business rules are also built into the application in the form of application controls. They apply to application segments and relate to the transactions and standing data.

While the general IT controls in an entity 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. They ensure that initiation of transactions are properly authorised, valid input data is processed, completely recorded and accurately reported.

Illustration

In an online payment application (see online payment gateway screenshot below), 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 built into the application would make sure that these conditions are inviolable, making the transactions valid.

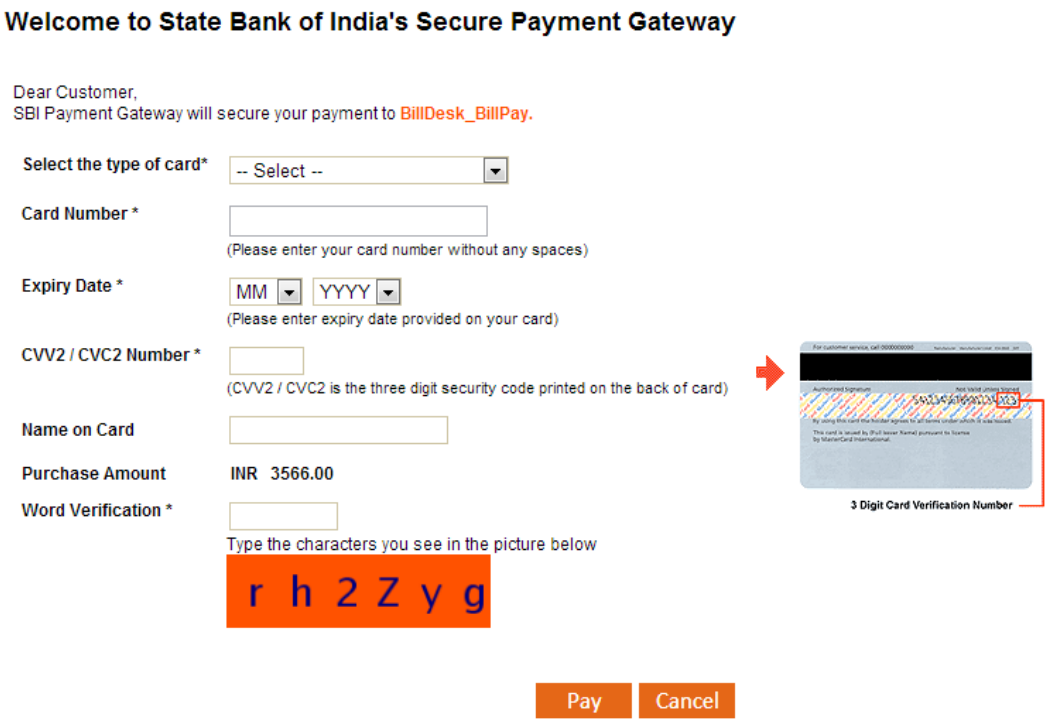


Figure 8.2: Application Controls example

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 (approved) before it is entered onto the system.

The combination of manual and automated control chosen is often a result of cost and control considerations at the design stage of an application.

An application can be divided into the following 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.

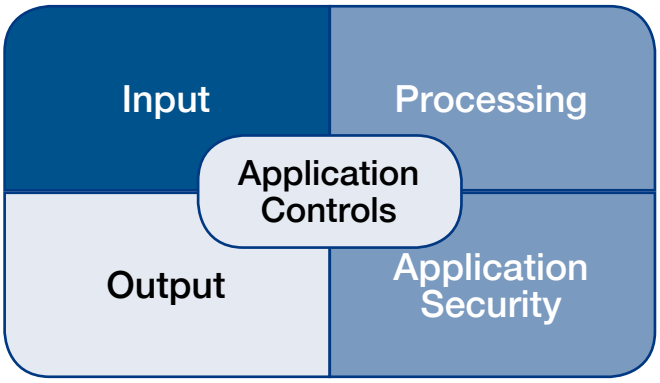


Figure 8.3: Application Controls 'Key Elements'

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

Some of the most common control elements are given in a snapshot in the table below:

Input Controls	• 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	• Business rules mapping • Integrity and completeness checks, report of out-of-balance conditions • Automated calculations • Input reconciliations
Output Controls	• 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	• Traceability mechanisms (audit trails, log review, use of unique identifiers) • Logical access control to functionalities and application data • Stored data protection

Figure 8.4 Some examples of Application Controls

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.

A significant proportion of these measures are designed at the development stage of an application during different stages of systems development after the business rules are laid down at the requirements definition. 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).

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).
Source documents management	Documentation of source document preparation procedures; source documents logging; source document numbering (traceability); and document retention procedures.
Error handling procedures	Procedure for dealing with rejected input. (E.g.: error messages, subsequent correction measures, prompts enabling re-input, use of suspense data).
Authorisation of input	Manual procedures/supervisory level authorisation of data 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.

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 is received from the input subsystem to the time data is 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. Moreover, they seek to enhance the reliability of the application programs that execute instructions to meet specific user requirements.

The control procedures include establishing and implementing mechanisms to authorise the initiation of transaction processing, and to enforce that only appropriate and authorised applications and tools are used. They routinely verify that processing is completely and accurately performed with automated controls, where appropriate.

The control types may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks and buffer overflow.

In real time systems some of the compensating controls would be one for one checking, retrospective batching, exception and suspense account reporting.

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.

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, 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 is stored.

Most applications are accessed through individual user IDs and passwords to the application. However, other forms of login, such as single sign-on mechanisms, have become increasingly popular, given the magnitude of applications used in a corporate environment. So, the design of the application for user provisioning should be understood upfront. An auditor might need to review entity's policy and procedures for obtaining and revoking user access in order to understand the extent to which the access rules are embedded in each application layer and to ensure that the application has controls around provisioning and de-provisioning access.

To be able to understand the application security control procedures, the auditor needs to understand the actors, roles and responsibilities involved with the application, such as administrators, power users, regular users etc. The design of the logical access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for each module, menu option, each screen 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. Indeed, it is necessary to be able to recognise the mechanisms used for ensuring the authoring and traceability of transactions as well as to protect the data stored by the application.

Following there is an example list of auditable issues regarding application security controls:

- Traceability of transactions: transaction logging; use of unique user IDs; logs reporting and monitoring; ideally the audit log should record what records or fields were amended, when they were amended, from what to what, and who made the amendment.

- User accounts, permissions and password management: 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; password encryption etc.

- Masterfile and standing (semi-permanent) data protection: controls to ensure that amendments to standing data are authorised; users are held accountable for any changes made; the standing data is up-to-date and accurate; and the integrity of the masterfiles is maintained. Examples of standing data: supplier and customer details (name, address, telephone, account number); inflation rates; system administration data, such as password files and access control permissions etc.

- Conflicting duties and segregation of duties adoption: different user roles; access rights available for each user profile; segregation of duties rules.

II. RISKS TO THE AUDITED ENTITY

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 houses; banking accounts might be susceptible to fraud etc.

Specifically, the significant risks possibly occurred in the absence of proper input controls are the risk of erroneous or fraudulent processing and the application will fail to deliver business objectives. The data processed by the application might be inconsistent and improper output will be provided by the programs. What is more, even in the presence of such controls it might be possible to override them 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 to be entered into the application.

Procedures for managing source documents and data entry authorisation are also an important kind of input controls. In the absence of proper management of source documents, it might not be possible to trace the source of information which was inputted into the system, legal compliance might not be achieved, and retention policies may be infringed, unreliable data may be inserted into the application. On the other hand, in the absence of authorisation controls, unauthorised data might lead to errors or fraud.

In general, failure in processing controls may lead to processing errors and failure to meet business goals for the application. They emerge due to incorrect mapping of business rules, inadequate testing of program code, or inadequate control over different versions of programs 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 such as reconciliation of input and output batch totals for ascertaining completeness of input, retention of some data origination documents for audit trail are not available. However, real time systems embed other compensating controls within the application, including interactive data completeness, validation prompts, logging of access attempts, etc.

The lack of adequate output control 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 itself mitigate the risk of information systems misuse. Standing data errors have a far-reaching effect on to the application, since this data might be used for a very large extent of the application's transactions.

Actually, the risks of not properly dealing with information security go well beyond that. They can lead to consequences 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 the Information Security Chapter.

Audit Matrix

The audit matrix for this section can be found in Appendix VIII.

References:

1. ISACA IT Audit and Assurance Guideline G38, Access Controls
2. *IT Audit Manual* Volume I, SAI India
3. *IT Auditing: Using Controls to Protect Information Assets*, Second Edition by Chris Davis, Mike Schiller and Kevin Wheeler McGraw-Hill/Osborne
4. *Singleton, Tommie W. Auditing applications* – Part 2. ISACA Journal, Vol IV. 2012.

CHAPTER 9

ADDITIONAL TOPICS OF INTEREST

This section provides an overview of some other topics related to IT Audit that the auditor may come across in the course of their audits. There are a lot of emerging areas in IT that could become auditable subjects. Thus, the auditor should be aware of the existence of these areas, and be able to thrive in an audit with these kind of subjects.

Even though these areas might have some technical differences or specific aspects, they can be audited using the same approaches and techniques that are being discussed thoughout this guidance. Possibly, they would require some additional audit questions/issues that the auditor could develop on his or her own when dealing with these subjects, and clearly depending on the audit objectives.

1. Websites/portals

Websites are information systems located on the internet or even intranets that provide services and content such as text, images, video, audio etc. A web portal organises information from different sources in a uniform way, while providing a consistent look and feel. Usually, web portals offer services including search engines, news, information, access to systems, databases and entertainment. Examples of public web portals are AOL, iGoogle, Yahoo, India.com.

Audit areas

- User experience
- Security, privacy
- Response time
- Outsourcing related issues

Further References/Readings:

1. http://en.wikipedia.org/wiki/Web_site
2. http://en.wikipedia.org/wiki/Web_portal
3. Kenyon, Geoff. *Technical Site Audit Checklist*. 2011, http://www.seomoz.org/blog/how-to-do-a-site-audit
4. Jones, Harrison. *How-to: Guide -to Performing Website Audits*. 2011 http://www.techipedia.com/2011/website-audit-guide/

2. Mobile computing

There is a growing effort to deliver services to the public through all kinds of IT channels. This relates to the use of wireless communication technologies to provide applications and information. Nowadays, many applications are being offered in a mobile environment. Mobile phones, tablets, wi-fi networks, TVs, and a whole range of new electronic devices and tools are delivering information. Mobile computing can be seen as an IT access point (PC, laptop, etc.) but they have some special audit areas that may be important.

Audit areas

- Wireless security, privacy, encryption
- User experience
- Specific policies regarding mobile computing in the organisation
- Risks of using personal devices to access corporate data and services
- Risks of unauthorised access to the data that reside on the device
- Increased risks of damage or theft of corporate devices

Further References/Readings:

1. ISACA IT Audit and Assurance Guideline G 27 – Mobile Computing
   http://www.isaca.org/Knowledge-Center/Standards
2. ISACA Mobile Computing Security Audit/Assurance Program
   http://www.isaca.org/auditprograms

3. Forensics Audit (or Computer Forensics)

Forensics audit is a type of audit that is carried out to examine digital media for evidence regarding an investigation or dispute. The evidence preservation is a must during a computer forensic analysis. It includes the approach, tools and techniques to examine digital information for identifying, preserving, recovering, analysing and presenting facts and opinions about the information stored.

It is mostly associated with criminal investigations in order to help law enforcement agencies and provide strong evidence in a court trial. Computer forensics have been applied in a number of areas including, but not limited to, fraud, espionage, murder, blackmail, computer misuse, technology abuse, libel, malicious mails, information leakage, theft of intellectual property, pornography, spamming, hacking and illegal transfer of funds[47].

Audit areas

The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

[47] ISACA's IT Audit and Assurance Guideline G38 Computer Forensics.

- Evidence (data, access, log) retention for analysis
- Capture and preserve data as close to the breach as possible
- Data collection standards for possible law enforcement use
- Minimally invasive data capture process without disruption to business operations
- Identification of attackers if possible.

Further References/Readings:

1. ISACA IT Audit and Assurance Guideline G 27 – Mobile Computing http://www.isaca.org/Knowledge-Center/Standards
2. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*
3. http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
4. *Electronic Crime Scene Investigation: A Good Practice Guide for Computer-Based Electronic Evidence*
5. http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf
6. Computer Forensics. Wikipedia
7. http://en.wikipedia.org/wiki/Computer_forensics

4. Electronic Government, Electronic Governance and Mobile Governance (eGov, e-Gov and m-Gov)

The advent of information technology has changed pervasively how governments provide services to their citizens. While the technology spreads among the population, governments are concerned with new approaches for delivering information and applications to benefit the public. Electronic government, electronic governance (known as eGov or e-gov) and mobile governance are some areas that deal with this subject. These concepts are related, although they are not perfect synonyms.

Audit areas

For audit purposes, the auditor should be aware that governments are generally required to provide services in an economic, efficient and effective manner. Very often, delivering the services electronically enables the widest reach at a reasonable cost.

In an audit perspective, auditing information systems or businesses process involved in an e-gov or m-gov strategy does not differ from a traditional IT audit. The auditor may need to look at some additional policy and enforcement mechanisms (for example, an organisational policy on mobile computing, encryption software, limiting personal smart-phone use, etc.).

Further References/Readings:

1. Eletronic Governance. Wikipedia
2. http://en.wikipedia.org/wiki/E-Governance
3. Mobile Governance. Ministry of Communications and Information Technology. Government of India
4. http://mgov.gov.in/msdpbasic.jsp
5. United Nations E-Governance Survey
6. http://www2.unpan.org/egovkb/global_reports/10report.htm

5. Electronic commerce (E-commerce)

Electronic commerce (E-commerce) refers to any type of business or commercial transactions made across networks. It encompasses, but is not limited to, the selling and trading of information, commodities and services.

Although in the vernacular e-commerce usually refers only to the trading of goods and services over the Internet, broader economic activity is included. E-commerce consists of business-to-consumer and business-to-business commerce as well as internal organisational transactions that support these activities[48].

A whole range of technologies and business processes are now related to E-commerce such as: portals, electronic funds transfer, online banking, supply chain management, marketing, online shopping, mobile commerce, inventory management etc.

Audit areas

There are several aspects which are crucial for an e-commerce system. Some of these should be taken into account when deciding audit objectives, e.g.:

- Availability
- Transactions security
- Scalability of the solution
- User experience and, mostly important
- The business process undertaken by the e-commerce strategy.

The business processes undertaken through e-commerce strategies require strong security mechanisms in order to provide mainly integrity, confidentiality, non-repudiation and authenticity of the online transactions. Thus, a set of processes and technologies called Public-Key Infrastructure (PKI) comes into place.

[48] E-Commerce. Encyclopedia Britannica. http://www.britannica.com/EBchecked/topic/183748/e-commerce.

PKI comprises a set of standard cryptographic algorithms and techniques to enable users to communicate securely over non-secure public networks to ensure information is communicated to the intended receiver. Without this technology, e-commerce as we know it would be impossible[49].

In order to audit e-commerce systems, very often the auditor needs to have knowledge of the main components of a PKI Infrastructure:

- Public and private keys
- Digital signature mechanisms
- Digital certificates
- Certification and registration authorities
- Cryptographic algorithms.

While the auditor does not need to be an expert in these areas, they should be aware of widely accepted standards and whether the organisation has adopted them.

Further References/Readings:

1. E-Commerce. Encyclopedia Britannica.
   http://www.britannica.com/EBchecked/topic/183748/e-commerce
2. E-Commerce and Public Key Infrastructure Audit/Assurance Program. Isaca
   http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/E-commerce-and-Public-Key-Infrastructure-PKI-Audit-Assurance-Program.aspx
3. Audit Trails in an E-commerce Environment
   http://www.isaca.org/Journal/Past-Issues/2002/Volume-5/Pages/Audit-Trails-in-an-E-commerce-Environment.aspx

[49] E-Commerce and Public Key Infrastructure Audit/Assurance Programme. Isaca, 2012.

APPENDIX I

GENERIC CRITICALITY ASSESSMENT CHECKLIST

Key to the checklist:

d. Weights have to be allocated to the Criteria question by the SAI. If required, the SAI may assign weights in consultation with the entity.If no weight have to be assigned, the SAI could give equal weight to all criteira questions, i.e., 1.
e. Figures in parenthesis are indicative scores for the responses.The scores indicated are between 1 to 5 with 1 indicating least risk area and 5 as high risk area. SAIs can adopt different scores as relevant to their scenario.
f. The criteria questions are not exhaustive. The SAIs can select criteria questions from the below table or develop criteria questions as per their requirement.
g. The information for the checklist should be collected for all organisations to be audited by the SAI. SAIs may endeavour to collect as much information as possible to make the scoring and comparisions relevant.
h. The SAI may decide to keep the scores and ranking confidential or share it with stakeholders as per their policy.

I. Name of IT System and Organisation:

	CRITERIA	WEIGHT	SCORE
	IT Governance		
1	**General state of computerisation in the entity. The entity has computerized**		
	All the business processes (5)		
	Most of the Business processes (4)		
	Only a few processes (3)		
	No business process (1)		
2	**The entity has an IT and related policies**		
	Yes (1)		
	Partially (3)		
	No (5)		
3	**The entity has**		
	Separate IT wing (2)		
	Has outsourced some IT functions (5)		
	Has outsourced IT facilities (5)		
4	**The entity has a**		
	Chief Information Officer (CIO) in charge of activities related to IT (1)		

	CRITERIA	WEIGHT	SCORE
	The entity has a sufficiently senior official in charge of activities related to IT in addition to his responsibilities (3)		
	Entity has a subordinate official in charge of activities related to IT (3)		
	The entity has no one designated to attend to activities related to IT (5)		
	Development, Acquisition and Outsourcing		
5	**The system was developed**		
	In-house with sufficient in house capacity (1)		
	In-house with insufficient in house capacity (5)		
	By a contractor/other Governmental agency (4)		
	A mix of in-house and outsource development (5)		
6	**The acquisition was made**		
	By the entity itself with sufficient capacity to make IT acquisitions (3)		
	By the entity itself with insufficient capacity to make IT acquisitions (5)		
	By utilising services of a consultant (4)		
7	**System documentation is**		
	Available (1)		
	Partially available (3)		
	Not available (5)		
8	**How often changes are made/warranted to the applications**		
	More than five times in a year (5)		
	Less than five times in a year and more than twice in a year (3)		
	Less than twice in a year (2)		
	Not even once in a year (1)		
	IT Operations and IS Security		
9	**Number of access points/ transaction locations/ users**		
	More than Y (5)		
	More than X, less than Y and more such levels, if required (3)		
	Less than X (1)		
	(Numbers X and Y to be decided by the SAI)		
10	**Network based system**		
	No network (1)		
	Local Area Network (LAN) (3)		
	Wide Area Network (WAN) (4)		
	Web based (5)		
11	**Number of locations** *(Threshold/Numbers for locations as X and Y to be decided by the SAI)*		
	Only one location (1)		
	More than one, less than X locations (3)		
	More than X locations (5)		
12	**Does the system make use of direct links to third parties e.g. EDI**		

	CRITERIA	WEIGHT	SCORE
	Yes (5)		
	No (1)		
13	**Number of end-users of the system** *(Threshold/Numbers for end-users X and Y to be decided by the SAI)*		
	Less than X (1)		
	More than X, less than Y and more such levels if required (3)		
	More than Y (5)		
14	**Does the entity maintain the data and application**		
	In house (1)		
	Partially in house and on outsourced facilities (3)		
	Hosted on outsourced facilities (5)		
15	**The system has been in operation for**		
	More than 10 years (1)		
	Between 5 and 10 years		
	Between 2 and 5 years		
	Less than 2 years (5)		
16	**Volume of data in the system is approximately (including offline data)**		
	More than 10 GB (5)		
	Between 2 GB and 10 GB		
	Less than 2 GB (1)		
	Financial Exposure		
17	**Investment made in the System** *(Threshold/Amounts $x and $Y levels to be decided by the SAI)*		
	Above $Y (5)		
	More than $X, Less than $Y (and more such levels, if required) (3)		
	Below $X (1)		
18	**Mode of financing of the system**		
	From internal resources (3)		
	From borrowings (4)		
	From loans from international organizations (5)		
19	**Recurring expenses on the system** *(Threshold/Amounts $x and $Y levels to be decided by the SAI)*		
	Above $Y (5)		
	More than $X, Less than $Y (and more such levels, if required) (3)		
	Below $X (1)		
	Functional Exposure / Usability of the System		
20	**The system is used for**		
	internal processes only (3)		
	external processes only (4)		
	Both internal and external processes (5)		
21	**Does the system provide citizen services?**		

	CRITERIA	WEIGHT	SCORE
	Yes (5)		
	No (3)		
	Internal control and Audit Assurances		
22	**Has a third party certification of the system been done**		
	Yes (1)		
	No (5)		
23	**Has the system been audited by IT Auditors of SAI**		
	3 years back (2)		
	5 years back (4)		
	Never (5)		
24	**Have other audit (financial/ compliance/ performance related) observations been made in previous audits**		
	Several recurring audit observations (5)		
	Few recurring audit observations (3)		
	No recurring audit observations (1)		
The list is not exhaustive. SAIs can identify their own such criterion over and above the list given above.			
	Total Score		

II. Ranking of IT Systems

Having completed the Criticality Assessment Checklist above, the IT Auditor can use the table below to summarize their assessment of the IT systems within the audit entity. This can be done by using the total scores generated from the checklist and deriving a category of risk (as per section III below) as well as a corresponding ranking.

Name of IT System	Total Score	Category of Risk	Rank

III. Category of Risk

Priority of IT System	Total Score Range*
A	L1-L2
B	>L2 and <L3
C	>L3 and <L4
D	> L4

*L1, L2, L3, L4 are score ranges to be decided by SAI to categorise the IT Systems

The above framework thus provides for categorising the IT systems and also ranking them for prioritising for audits. Category 'A' being the lowest risk, and category 'D' being the highest risk categories, respectively.

APPENDIX II

SUGGESTED MATRIX FOR AUDIT OF IT GOVERNANCE

Business Needs Identification, Direction & Monitoring	
Audit objective: Assess whether the organisation's leadership effectively directs, evaluates and monitors IT use in the organisation in order to fulfil the organisation's mission.	
AUDIT Issue 1: Defining IT requirements **How does the organisation identify and approve business and IT requirements?**	
Criteria: The organisation has a plan on how it identifies emerging business or IT needs and the Steering Committee approving requirements has sufficient information to make their decisions.	
Information Required	**Analysis Method(s)**
Requirements management process	Review of documents to ensure that new business requirements are identified and analysed according to the organisation's requirements management process.
Steering committee charter and operating principles including approval and rejection thresholds	Review of approved or rejected requirements to ensure that these are in accordance with accepted operating principles.
List of approved and rejected requirement	Interview management or others responsible for approving projects to ensure that they take into account the IT organisation's capabilities, skills, resources, and training, and the ability of the users to utilise the new tools and methods or procedures.
AUDIT Issue 2: Leadership **How does the leadership direct and monitor the performance of business and IT objectives on a periodic basis?**	
Criteria: Performance measures are established and the steering or equivalent high level committee conducts periodic reviews and meetings and takes appropriate action, or there is a reporting system to management that informs them of the status of key performance measures.	
Information Required	**Analysis Method(s)**
Performance measures for business and IT	Review sample management decision or memos to ensure that they are clear, well substantiated, and unaambiguous.
Periodic reports about project status	Review performance measures to ensure that they cover both business and IT systems.
Minutes from periodic reviews	Review project status reports (or other documentation that has the status of the project (meeting minutes, emails, etc.)) to ensure that it contains cost, schedule and performance indicators and variations from plan.
List of action items and their status etc	Review management actions items to ensure that they are assigned and tracked to closure and include lessons learned.
AUDIT Issue 3: IT Investments **How does the organisation manage IT investments?**	
Information Required	**Analysis Method(s)**
Investment management plan and procedures	Interview management to determine the organisation's investment management procedures.

Portfolio of IT projects Sample cost benefit analysis reports List of approved and rejected or deferred projects Project status reports for approved projects Sample post project evaluation reports	Review portfolio to assess whether projects have been prioritised according to approved criteria. Review status reports to see they provide cost and schedule tracking Review cost benefit analysis reports to assess that they are complete, reflect actual conditions and do not overstate the benefits or understate cost or schedule (utilise specialist services of economists or cost experts as needed). For projects in trouble, determine whether their methodology was suitable to the type of project and properly applied, and whether QA has been involved during the life cycle. Interview management to determine whether any projects have been terminated due to underachieving benefits or performance. Interview management to determine how the organisation makes decisions on building vs. acquiring (buying) solutions (for example, based on capability, skills, cost, risk, etc.).
Audit Conclusion: To be filled in by auditor	

IT Strategy	
Audit objective: Confirm whether there is an IT strategy in place, including an IT plan and the processes for the strategy's development, approval, and implementation and maintenance which is aligned with the organisation's strategies and objectives. The risks and resources while accomplishing IT objectives are effectively managed.	
AUDIT Issue 4: Quality of IT strategy **Does the organisation have an IT Strategy that serves to guide its IT functions?**	
Criteria: An organisational-level IT strategic plan exists, it translates business objectives into IT goals and requirements, addresses the needed IT resources to support the business, and it is reviewed and updated periodically.	
Information Required	**Analysis Method(s)**
IT Strategic Plan, or equivalent document Meeting minutes from IT and Organisation's Steering committee meetings.	Review of document. Interview business owners to determine if their needs are met by the IT organisation. Review periodic IT Committee and Organisational Steering Committee meeting minutes to ensure that business owners are represented and that strategic IT decisions are made at the Steering Committee level. Review the IT Strategy or interview management to determine resources' requirements and how they are determined and approved, who approves appropriate acquisition of tools and other resources (staff, contractors, skill via training, etc).
AUDIT Issue 5: Risk management **How does the organisation manage their risks?**	
Criteria The organisation has a risk management policy and plan, and has assigned sufficient resources to identify and manage risks.	
Information Required	**Analysis Method(s)**
Risk management plan List of risks (including IT) and mitigation strategies	Review risk management plan or other document to ensure that risk management responsibilities are clearly and unambiguously assigned. Review of documents to determine whether IT risks are part of the overall governance risk and compliance (GRC) framework.

Minutes of periodic risk assessment or other meeting if available.	Review meeting minutes to ensure that new risks are added and analysed as appropriate. Interview personnel responsible for risk management to determine whether the risks to be mitigated have appropriate cost estimates, and resources are allocated. Interview management or review minutes of meeting to determine that leadership is aware of both IT and other risks and monitors their status on a periodic basis.
Audit Conclusion: To be filled in by auditor	

Organisational Structures, Policy, & Procedures	
Audit objective: Ensure that there are organisational structures, policy, and procedures in place that enable the organisation to meet its mandate for business goals.	
AUDIT Issue 6: **Does the structure of the IT Organisation enable it to meet its IT Goals and business needs?**	
Criteria: The IT Organisation is positioned at a sufficiently high level within the organisation and its roles and responsibilities are clearly defined including those of the Chief Information Officer (CIO) or equivalent.	
Information Required	**Analysis Method(s)**
Overall organisation chart IT Organisational chart.	Review organisational charts to determine that the IT organisation is positioned at a strategic level (for example, there is a CIO who reports to or is a member of the Steering Committee). Review the IT organisation chart to determine that it is aligned to support the business (has a help desk, data base managers, maintenance personnel or contactors who help and facilitate IT operations).
AUDIT Issue 7: Policy and procedures **Has the organisation approved and is it using appropriate policies and procedures to guide its business and IT operations?**	
Criteria: The organisation documents, approves, and communicates appropriate policies and procedures to guide the business and IT operations in order to meet its mandate.	
Information Required	**Analysis Method(s)**
Organisational policies regarding: Human Resources including hiring and termination security, document retention, contracting and/or outsourcing, software development and/or acquisition, etc. Procedures for the selected policy areas Emails or other ways policy is communicated to appropriate users and stakeholders QA reports to management reporting on periodic policy and procedures compliance and other issues	Review policies to ensure they are approved and current. For example, review the Human Resources policy to determine that skill requirements are defined, and training is identified for new and other staff. Review initial and refresher training materials or other internal processes through which these policies and procedures are communicated within the organisation. Interview members of the quality assurance or other group that is responsible for enforcing policy's to see what they do to ensure compliance. Interview QA or compliance staff to determine how and when they report their results to senior management. Interview personnel responsible for compliance of policies and procedures to determine how often they report the results to senior management and how they solicit input on non-compliance anonymously or independently. Interview managers and users to understand their perception and attitude to the analysed policies and procedures. In case of frequent opinion: "Procedures are to complex" ask what and how they could be simplified. Review policy change control history to determine that policies are updated periodically or as needed.

Request changes to policy and or periodic review and results.	Review QA reports to ensure that they contain any policy or procedure compliance issues as appropriate. Review emails or other mechanisms (physical mail, training, etc) to ensure that policies are distributed to appropriate users and stakeholders when updated or on an as-needed basis. Review policies to determine adequacy by looking for (as an example): • Scope of policy and mandate. • Definition of roles and responsibilities. • Required resources and tools. • Linkage to procedures. • Rules to deal with non-compliance.
Audit Conclusion: To be filled in by auditor	

People & Resources

Audit objective: To assess whether sufficiently qualified/trained personnel are employed and that they have access to suitable resources that enable the organisation to met its business goals.

AUDIT Issue 8: HR and logistics

How does the organisation deal with meeting current and future people and resource requirements?

Criteria:

The organisation should have a plan to meet its current and future requirements for meeting business needs.

Information Required	**Analysis Method(s)**
Organisational policies regarding: Human Resources & Training IT Strategy or Strategic Plan Hiring & Training Plans.	Review policies to ensure they are approved and current. Review policies to ensure they require various groups (IT, quality assurance (QA), Business Users) to identify their current and future needs for personnel and resources. Review hiring and training plans to ensure that they reflect identified needs. For example, review the Human Resources policy to determine that skill requirements are defined, and training is identified for new and other staff. Interview HR or business managers to assess how they ensure critical positions are staffed during contingencies or extended absences. Review initial and refresher training materials or other internal processes through which these policies and procedures are communicated within the organisation. Review the IT Strategic plan to ensure that it contains people and resource requirements for current and future needs.

Audit Conclusion:

To be filled in by auditor

Risk Assessment and Compliance mechanisms

AUDIT Issue 9: Mechanism

How does the organisation ensure that it has an adequate and working compliance mechanism to ensure all policies and procedures are being followed?

Criteria:

The organisation has a mechanism (via a QA group, internal audit, or spot check, etc.) to ensure that all policies and procedures are being followed.

Information Required	Analysis Method(s)
Organisational policies & procedures (Security, SDLC, Training, etc) Organisation Chart Quality Assurance Plan Reports from compliance teams or groups Steering Committee Minutes	Select a sample of policies and organisational procedures to assess compliance. Interview management to determine who is responsible for ensuring compliance to the (audit selected) policies and associated procedures. Interview team or group responsible for compliance of above to determine how they accomplish their duties. Review reports from various compliance groups to see what they found, what actions they have taken and reported to management. Review steering committee minutes to see if high level compliance issues are discussed at this or at other meetings. Interview author(s) to determine reason for update to existing policies or procedures. Review past non-compliance issues and resolutions. Review training or other dissemination mechanisms (email, memo, notice) to see if non-compliance issues were addressed.
Audit Conclusion: To be filled in by auditor	
See Appendix III and Appendix IV respectively for audit matrices on Development and Acquisition and IT Operations	

APPENDIX III

SUGGESTED MATRIX FOR AUDIT OF DEVELOPMENT & ACQUISITION

Requirements Development & Management	
Audit objective: Assess how the organisation identifies, prioritises and manages their requirements for IT systems.	
AUDIT Issue 1: **How does the organisation identify user requirements for IT Systems?**	
Criteria: The organisation has a plan or procedures on how to collect, review, and catalog requirements for new or added functionality	
Information Required	**Analysis Method(s)**
Requirements' management plan or procedure Sample user submitted requirements Sample initial review	Review the requirements' management plan or procedures to ensure users, stakeholders, or other relevant users are involved in identifying requirements. In a major functionality enhancement development, user consultation and prototype development can be implemented in parallel. The information interchange between the business process owners and vendor/ IT organisation needs to be looked into. Review sample requirements to ensure that there is an initial review, and that similar or duplicate requirements are grouped.
AUDIT Issue 2: **How does the organisation analyse, prioritise, and manage user requirements?**	
Criteria: The organisation analyses, prioritises, and manages requirements to ensure that user needs are met in an optimum and cost effective manner	
Information Required	**Analysis Method(s)**
List of requirements Sample analysis of requirements Requirements traceability matrix Criteria for priority of requirements	Review requirements to determine that they include author, date, priority, cost, risk, and other elements. Review analysis of requirements or comments on requirements by business owners or stakeholders to determine that all views are solicited and summarised for appropriate analysis (accept, defer, reject, etc.) taken. Review traceability matrix to determine that approved requirements are assigned to either development or acquisition projects, and are tracked to closure when implemented. Review criteria for requirements priority to assess whether they include elements such as cost, business need, emergency issues, and new mandates.
Audit Conclusion: To be filled in by auditor	

Project Management & Control

Audit objective: Assess how the organisation manages and controls the development or acquisition of approved IT projects.

AUDIT Issue 3:
How does the organisation plan for the development or acquisition of IT projects?

Criteria:
The organisation has a project management plan or equivalent for each approved project that guides its execution

Information Required	Analysis Method(s)
Project management plan or equivalent	Review the requirements' management plan or equivalent to ensure that it contains the project description, scope, cost, schedule, risks, management structure and that it identifies stakeholders (internal or external). Review the plan to ensure that it has been approved by senior management and incorporates comments by stakeholder. Review the project's organisational chart to determine the roles of individuals who are responsible for quality assurance or testing, development, and installation of the system on organisations IT infrastructure, support group, etc. For acquisition projects, ensure that the plan or equivalent list of those who will be responsible for oversight of the contractor exists and review approvals given by responsible persons. Interview project managers to determine which SDLC method is being used for the development of the project.

AUDIT Issue 4:
How does the organisation control IT projects?

Criteria:
The organisation controls and tracks projects to ensure they meet their cost, schedule, and performance requirements.

Information Required	Analysis Method(s)
Project cost and schedule baselines	Compare project cost and schedule baselines with project status reports to assess deviations.
Project status reports Contractor status reports, SLA Results of reviews Action items	Interview project manager / review reports to determine whether appropriate corrective action was taken for major deviations. Interview project management team and review minutes of meetings with contractor to assess the frequency and effectiveness of monitoring the outsourced project activities. Review contractor SLA or contract to ensure that they are following the terms of the contract, for example, look for contractors conducting periodic reviews, providing status reports, tracking action items, conducting risk management activities in accordance to the contract. Interview contract officer at the organisation to determine how it manages the contractor if SLAs are not available.

Quality Assurance & Testing

Audit objective: Assess how the organisation ensures that IT projects under development or acquisition meet their quality goals.

AUDIT Issue 5:
Does the organisation have a quality assurance organisation and are their roles and responsibilities defined?

Criteria:
An established procedure for conducting quality assurance activities.

Information Required	Analysis Method(s)
Quality assurance policy or plan Quality assurance procedures Roles and responsibilities of the Quality Assurance group or individual(s) Quality assurance reports Project adopted SDLC	Review the quality assurance policy and/or plan to determine what group or individuals is responsible for conducting quality assurance activities for the project (for example, the Quality Assurance group should review documents to ensure they accurately reflect the requirements, review user manuals to ensure they are legible and do not contain missing elements or steps). Review the quality assurance procedures or interview quality assurance personnel to determine what activities they conduct (observe peer reviews, sit in on design or other reviews, etc.). Review reports from the quality assurance organisation to determine what they observed (whether the project team is following its project management plan, and the adopted SDLC and associated reviews etc.) to whom are issues reported.
AUDIT Issue 6: **How does the organisation plan for and conduct testing on IT systems?**	
Criteria: The organisation conducts test on IT systems and based on the results accepts or rejects the system.	
Information Required	**Analysis Method(s)**
Test plan Test schedule Test results Accept or reject criteria	Review test plans. Compare project cost and schedule baselines with project status reports to assess deviations, if any. Interview project manager / review reports to determine whether appropriate corrective action was taken for major deviations. Interview project management team and review minutes of meetings with contractor to assess the frequency and effectiveness of monitoring the outsourced project activities. Review contractor SLA or contract to ensure that they are following the terms of the contract, for example look for contractors conducting periodic reviews, providing status reports, tracking action items, conducting risk management activities in accordance to the contract. Interview contract officer at the organisation to determine how it manages the contractor if SLAs are not available.
Audit Conclusion: To be filled in by auditor.	

Solicitation
Audit objective: Assess how the organisation ensures that solicitation activities (set of tasks such as firming up the needs document, framing RFP, evaluating proposals, conducting pre-bid clarifications, designing and floating tender, evaluation, etc leading up to the award contract) are conducted in accordance with its adopted solicitation plan or procedure.
AUDIT Issue 7: **What is the plan or procedure for the conduct of solicitation activities?**
Criteria: Solicitation activities including vendor selection are conducted in accordance with the organisation's solicitation plan

Information Required	Analysis Method(s)
Solicitation plan or procedure Solicitation package User review of requirements User review of solicitation package Applicable laws that govern the conduct of solicitation.	Review the solicitation plan to ensure it covers areas such as user involvement, getting bids on a competitive basis, conducting market research prior to contract on areas as applicable, and that vendor selection is based on objective criteria. Interview key contracting personnel to assess how they ensure that the solicitation package is complete (for example, by getting users, stakeholders, experts as appropriate to review it). Interview users or business owners to ensure that they were consulted during the generation of requirements or approved the technical requirements of the solicitation and / or the final bid package. Interview contracting officer(s) to assess how they ensure that the solicitation process follows applicable laws and regulations.
AUDIT Issue 8: **What criteria does the organisation use in selecting a vendor?**	
Criteria: The organisation uses objective and published criteria for vendor selection for each.	
Information Required	**Analysis Method(s)**
Vendor selection criteria Vendors scoring matrix or equivalent.	Review the vendor selection criteria to ensure that it reflects the intent of the solicitation (for example, on a software contract, vendor selection should not include parameters not critical to the organisation). Interview key stakeholders to assess if they agree with the selection criteria. Review vendor scoring matrix or equivalent to confirm it is consistent with the selection criteria.
Audit Conclusion: To be filled in by auditor	

Configuration Management	
Audit objective: Assess how the organisation manages configurations of work products related to development and acquisition.	
AUDIT Issue 9: **What policy does the organisation use for configuration management?**	
Criteria: Configuration management activities are conducted according to the organisational policy or procedure.	
Information Required	**Analysis Method(s)**
Configuration management policy or procedures or equivalent.	Review the configuration management policy for adequacy by looking for (as an example): Scope of policy and mandate Definition of roles and responsibilities Required resources and tools Linkage to procedures Rules to deal with non-compliance. Interview personnel responsible for configuration management if there is no policy to assess how they ensure that their duties are uniformly carried out for the organisation.

AUDIT Issue 10: **What group or individual(s) are responsible for authorising changes and for final installation into the production environment?**	
Criteria: Only authorised and approved changes should be introduced into the production environment.	
Information Required	**Analysis Method(s)**
Group or individual responsible for authorising changes	Ensure that a group exists that authorises changes to the work product(s). The group could be the change control board or equivalent that reviews and approves changes.
Process for approval and introducing approved and tested changes to the production environment.	Interview personnel responsible for authorising introducing new software to the production environment to ensure that software has been tested (including regression testing with other systems if needed) meets the acceptance criteria, has appropriate documentation, and includes user training (if appropriate) prior to being introduced for business. Interview personnel responsible for authorising changes to the production system to determine how they control and prevent unauthorised changes to the system (for example, by controlling access to the production system, separating the production and development environments, etc.).
Audit Conclusion: To be filled in by auditor	

APPENDIX IV

SUGGESTED MATRIX FOR AUDIT OF IT OPERATIONS

<table>
<tr><th colspan="2">Service Management</th></tr>
<tr><td colspan="2">Audit Objective: To assess whether the IT organisation is actively monitoring IT operations against agreed-to internal Service Level Agreement or contract.</td></tr>
<tr><td colspan="2">Audit issue 1: Key parameters
What baseline service metrics are covered by the internal SLA between the business and the IT organisation?</td></tr>
<tr><td colspan="2">Criteria:
SLA Best practices – allocation of responsibilities between the business process owners and the IT support group, documented network management business objectives, service offerings and metrics, definition for problem types, help desk responsibilities.</td></tr>
<tr><td>Information Required
Entity's internal SLA between business owners and IT organisation.
• Help desk responsibilities
• Service reports generated
• User/ application response time.</td><td>Analysis methods
Review the SLA to find whether it contains appropriate elements – detailed and measurable service level objectives, systems and services covered, quality of service (QoS), services not covered, application level support and troubleshooting, system availability, help desk hours, response and resolution time dependent on severity classification of a problem, throughput, maintenance schedules etc.
Check whether data back-up and recovery practices are consistent with the entity's BCP standards.
Check if the Business Process Owners have signed on the agreement.
Interview sample of users to understand the level of awareness.</td></tr>
<tr><td colspan="2">Audit issue 2: Compliance
What mechanisms are in place to ensure that the SLA is adhered to consistently?</td></tr>
<tr><td colspan="2">Criteria:
SLA implemented, monitored and amended where necessary.</td></tr>
<tr><td>Information Required
The SLA parameters
Reporting timelines
Charts or graphs that show the success or failure of how these agreements are met over time
Periodic meeting documents that reviews the analysis of the baseline and trends</td><td>Analysis methods
Review the reports that the IT Organisation generates daily or over any other time interval. Check if all the indicators agreed upon are being monitored through the reports/trend graphs etc.
Review reports to examine what metrics are measured and reported to the management periodically.
Review documents to check whether the helpdesk activity reports are considered by the management and compared to resolution requests, and critical issues are noted for buying decisions and for periodic review of the SLA itself.
Interview IT organisation personnel and examine the nature of supervision of help desk personnel, the monitoring tools used, the support task prioritisation, gathering of baseline for network and application, data on response time, frequency of back-ups, testing of backed up data to verify compliance with SLA requirements.</td></tr>
</table>

Operational parameters - defect rates, help desk requests, other communication trails, response time, Time to implement new functionality, change documentation, serviced locations andincentive and penalty clauses (especially important if IT support services are outsourced).	Check what actions are taken by the IT unit, or in the case of an outsourced IT support group – by the organisation's management – if operational parameters are not in agreement with SLA requirements.
Audit issue 3: Effectiveness Does the management of IT services ensure satisfaction of business users and help meet business objectives of the organisation?	
Criteria: achievement of performance metrics that are aligned to business needs and goals.	
Information Required	**Analysis methods**
Help desk reports minutes of meetings between business stakeholders and IT organisation Agenda items for SLA review cycles.	Interview a sample of business users (at various levels) or conduct a satisfaction survey about the quality of services by the help desk and IT support group. Review help desk reports to check whether a significant proportion of critical service issues were prevented before being reported by users. Check whether the resolution time for reported issues was less than the parameters set in the SLA. Check whether SLA parameters were being reviewed by management periodically and examine QoS issues.
Audit Conclusion: To be filled in by auditor	

Capacity Management	
Audit Objective: Assess whether the IT organisation is ensuring that the system capacity and performance meets current and future business needs.	
Audit issue 4: Agreement on parameters Is there a documented agreement between the business and IT organisation that is used as the basis for selecting operational parameters for IT operations?	
Criteria: IT governance – track and monitor strategy implementation in terms of measurable metrics.	
Information Required	**Analysis methods**
Internal SLA, or other form of agreement IT operational parameters – processing resource availability, average system login time, % downtime, average system response time, etc.	Review the agreement or operating guidance that the IT group is using. Ensure that it is has been reviewed and signed by the relevant business users or senior executive management. Compare performance baseline parameters (viz. network resource availability, host response time) set by IT organisation with the Operating guidance set by Business process owners to verify that the IT organisation follows the operating guidance.

Audit issue 5: Monitoring Does the IT organisation collect and review system performance data on a real time/periodic basis for better alignment with business needs?	
Criteria: best practices by system/network administrators including performance base lining, collection of traffic and configuration information, system resource availability, observe traffic stats and trends, what-if analyses, and use of tools to pinpoint causes of performance deterioration.	
Information Required	**Analysis methods**
Reports, action items, help desk response time, and other metrics.	Use Compliance issue in SLA matrix. Pay special attention to all elements having impact on capacity, i.e. compare actual capacity metrics to the SLA requirements, etc.
Audit issue 6: Performance data analysis Is the performance data analysed and tuned for efficiency gains and avoidance of capacity constraints? If needed, has the IT organisation planned for and acquired additional resources to meet business needs? Does the IT organisation hire, train, or contract for staff as the business needs change?	
Criteria: parameters set in the agreement/operation guidebest practices in performance tuning (memory, optimisation of network response time, OS, I/O; efficient design of database schema, scheduling tasks according to priority and resource requirement, upgrade or tuning procedures set up to handle capacity issues on both a reactive and long-term basis).	
Information Required	**Analysis methods**
Reports, actions, status reports, performance metric graphs Minutes of meeting at the apex IT organisation level.	Review the reports that the IT Organisation generates daily or at other chosen time frame, look to see if it generates and analyses trend data, identifies bottlenecks to look for action items, and exception reporting for capacity issues. Compare to SLA requirements. Compare reports/trend patterns to verify procedural actions taken in response to the reports. Review minutes of meetings and find whether IT staffing issues, capacity problems and any additional resource needs are discussed and highlighted at the right time.
Audit Conclusion: To be filled in by auditor	

Problem & Incident Management	
Audit Objective: To evaluate the effectiveness of organisation's problem and incident management policies and procedures.	
Audit issue 7: Policy awareness Is there a documented incident response policy and are the business users aware of it?	
Criteria: Best practices in incident response.	
Information Required	**Analysis methods**
Entity's incident response policy Guidelines for communicating with outside parties regarding incidents.	Review the policy to find whether it contains appropriate stages – preparation, detection and analysis, containment and eradication, post-incident activity. Does type of activity depend on high incidence or level of incidents? Verify whether the policy assigns responsibility, scope and reporting requirements. Review the actual procedures by which the business users are made aware of the policy, and the nature of communication between the incidents response team and the business stakeholders. Interview a sample of business users across the organisation to get an assurance about the awareness of the incident response plan.

Audit issue 8: Skills set and resources Is there an adequately skilled incident response team with proper tools, resources and higher management support to handle incidents?	
Criteria: Incidents response best practices, NIST guidelines, as laid down in SLA	
Information required	**Analysis methods**
Incident response policy and plan Charter of the incident response team, composition and expertise SLA Incident response awareness training, upgrade strategy for skillsets of IRT staff List of logging tools and applications used for network monitoring and usage.	Look at whether the team has a charter to investigate incidents. Look for expertise in networks, operating systems, and security in the team members and how they conduct their work. Review the service desk procedures to check whether escalation procedures are laid down for incidents that cannot be resolved immediately in accordance to risk categories defined in the SLA. Review what actions have been taken in response to past incidents. Review case report(s) to check whether appropriate personnel were involved in investigating incidents. Check what incident management tools are being used – are they relevant for the organisation's needs? Verify whether the organisation has established logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.
Audit issue 9: Effectiveness of response Does the incidence response strategy result in effective response to incidents?	
Criteria: Incidents response best practices (COBIT 5 DSS domain, ITIL on Service support)	
Information required	**Analysis Methods**
Incident response action items, forms logs, etc. Periodic security awareness training Incident handling procedures – guidelines for prioritising incidents Case reports and action taken.	Check if an incident response/handling priority is assigned to each asset or service. Verify whether procedures provide for the capture and analysis of volatile[50] and static data in a timely manner. Verify whether the response team periodically makes users aware of policies and procedures regarding appropriate use of networks, systems, external media and applications. Review documents to find whether post-incident activities such as refresher training has been given to user groups to avoid costly recurrence of significant incidents. Look for whether source of incident was identified. Look for action taken. (Procedure change, reprimand, training, etc.). Check whether the incident response team records all resolved incidents in detail and review the information for possible update in the knowledge base.
Audit Conclusion: To be filled in by auditor	

[50] Volatile data are data that are overwritten or changed over time, where a snapshot cannot be obtained without capturing the information interactively, or by regularly scheduled data extracts.

Change Management

Audit Objective: Assess whether the entity has implemented a standardised procedure for controlling all changes to the core IT systems and applications.

Audit issue 10: Policy

Does the organisation have an approved Change management policy that contains the appropriate controls throughout the change cycle?

Criteria:

Best practices in change controls: Request for change- authentication- acceptance- prioritisation - change design -testing change- implementation- documentation

Information required	Analysis methods
Change management policy and procedures, process flow diagrams Change control board charter Timeline of policy review Change documentation: Change request, Change control testing procedures, quality assurance plan, test plan & procedures Change Management software reports and logs Minutes of meeting of the change control board Change management summary reports considered by the management.	Refer to general requirements for policy and procedures in IT Governance section. Review the change management policy document to verify whether procedures for initiation, review and approval of change are laid out along with mapping of responsibility for these tasks. Review the change control board charter to identify the allocation of responsibilities and responsibility levels. Interview personnel, observe actual practices and review documents to obtain assurance that change management procedures are followed: ask to see a change, trace change to operational environment, see that requisite procedures – e.g. management review and prioritisation – were followed, look for approvals and documentation. Look to see if internal QA has done an audit. Review if adequate review of logs and reports are done by the management where a change management software is used. Ensure that the access to production source library (e.g. Source code, configurations) is limited to CM staff, and the IT organisation is preventing unauthorised changes to the operational environment. Review documents, observe practices to ensure that business users are associated during testing of changes to ensure correctness. Ensure that program changes have appropriate sign-off by relevant business stakeholder before moving into production.

Audit issue 11: Fallback procedures

How does the IT organisation ensure that the organisation can revert back to a previous version if needed?

Criteria:

Change Management best practices – documentation on procedures and responsibilities for recovery of affected areas due to undesirable change impact.

Information Required	Analysis methods
Change management procedures Documentation on change tests and implementation Recovery documentation and configuration change logs Back-up and restore procedures	Review documentation, interview business users to find if unintended impacts of functionality changes/ enhancements have been addressed on priority, in line with business interests.

Audit Issue 12: Emergency changes Are emergency changes controlled adequately when established change management procedures for defining, authorising, testing and documenting of changes cannot be followed?	
Information required	**Analysis Methods**
Emergency change control procedures Documentation of emergency changes that have been made during the audited period	Review the change management procedures to identify whether they contain a dedicated section and set of procedures to control emergency changes to the system. Ask for an example of an emergency change. Compare against documented procedure. Look for what testing was done prior to introduction into production environment. If documented procedure does not exist, ask how it knows what to do and who approves such changes. Examine whether emergency changes are approved by an appropriate member of the management before moving into production.
Audit Issue 13: Change closure and documentation Are there appropriate processes followed for the update of associated systems and user documentation after a change is implemented?	
Criteria: Change management best practices (e.g. COBIT 5-BAI domain, ITIL on Service support).	
Information required	**Analysis methods**
Process documentation of functionalities affected by change Established procedures for documentation.	Review documents to ensure comprehensiveness and consistency of changes implemented. Did operational procedures, configuration information, application documentation, help screens and training materials follow the same change management procedure, and were they considered to be an integral part of the change. Examine whether there is an appropriate retention period for change documentation and pre- and post-change system and user documentation. Examine what mechanisms exist to update business processes for changes in hardware or software to ensure that new or improved functionality is used.
Audit Conclusion: To be filled in by auditor	

APPENDIX V

SUGGESTED MATRIX FOR AUDIT OF OUTSOURCING

Outsourcing Policy	
Audit objective: To assess whether the agency has an adequate policy on outsourcing.	
AUDIT Issue 1: Key Elements of Outsourcing Policy Does the organisation have a policy on outsourcing?	
Criteria: Organisational policy on outsourcing	
Information Required	**Analysis Method(s)**
Policy Document Approval process for outsourcing of a function/ service List of outsourced functions/ services List of outsourced functions/ services with partial outsourcing Mode of service by the service provider Cost-benefit analysis on outsourcing of a function/ service List of outsourced service providers with locations Approval related documents for outsourced functions/ services Strategy to ensure continuity in case of takeover of the service provider by another organisation Information on any takeover of the service provider Monitoring documents/ reports.	Review policy to ensure it is approved. Review policy to check (for example) it contains information about organisation assets that can be outsourced or not, identifies the list of services/ functions that it may outsource. Review acquisition or outsourcing approval documents to ensure senior management are involved in the approval. Document review to assess that the organisation has identified the risks associated with respect to different modes of outsourcing and locations of outsourced service provider. Document review to verify whether the organisation is aware of risks associated with possibility of takeover of the service provider. Document review to verify whether the organisation has ensured that the business continuity, data rights, security, ownership and cost are embedded in the service agreement covering the case of takeover. Document review to assess that the policy includes identification of monitoring parameters for the outsourced functions and requires them to be included in the outsource agreement.
Audit Conclusion: To be filled in by auditor	

Solicitation
Audit objective: To assess whether the agency has a policy on how to manage solicitation.
AUDIT Issue2: Policy and Process of Solicitation • Does the organisation have a policy on acquisition? • Does the organisation have a definite process for identification and selection of the service provider? • Does the organisation have a process to ensure inclusion of user requirements into the Service Level Requirements/ contractual requirements? • Are the related decisions taken at appropriate levels?
Criteria: Provisions of organisation policy on Outsourcing and policy on IT services procurement dealing with solicitation and acquisition.

Information Required	Analysis Method(s)
Acquisition or equivalent Policy List of laws regulating the acquisition and outsourcing Selection process for identification and selection of a service provider List of outsourced functions/ services along with the service provider User requirements for the contracted or outsourced service Contract/ Service Level Agreement Approval related documents for selection of service provider.	Document review to assess that the organisation has a policy on solicitation or acquisition. Review policy to ensure it contains provisions for data requests from sub-contractors if the prime contractor has included sub-contractors as part of the proposal. Document review to assess that the policy on solicitation and acquisition complies to the laws on outsourcing and acquisition (review that it references to provides links to applicable laws and regulations) Review of selection process for compliance to the policy for each a sampling of contracts or outsourced service (review that the selection process is transparent, has objective criteria, the selection team is comprised of personnel who understand the requirements, is represented by contractual and legal personnel, and consult with users as appropriate for clarification). Ensure that the contractual requirements have been approved by users and relevant stakeholders. Meet with the contractual office to ensure that an appropriate level of management approved the solicitation and contract.
Audit Conclusion: To be filled in by auditor	

Vendor or Contractor Monitoring

Audit objective: To assess whether the organisation is managing the contractor or vendor and takes appropriate action when performance or quality deviates from established baselines.

AUDIT Issue3: Vendor Management

- Is there a contract with the service provider?
- Are Service Levels identified and agreed through a Service Level Agreement?
- Is there a monitoring arrangement (for services) with the service provider?
- Are the service levels ensured through this arrangement?
- Is appropriate action taken when service level agreement provisions are not met?

Criteria:

Provisions/ parameters defined in Service Level Agreement and the follow up actions by the organisation.

Information Required	Analysis Method(s)
Contract/ Service Level Agreement Approved schedules, baselines, cost and other technical parameters that define the product or service being acquired or outsourced Monitoring documents/ reports / meeting minutes of reviews conducted, action items, direction to vendor (task orders, statement of work, etc.) Impact assessment of deviations Action items or direction to vendor Action taken reports on deviations from service levels.	Document review to assess if a service level agreement has been established. Review of monitoring reports submitted by the contractor to ensure that they contain elements that are in the contract or SLA (cost, schedule, performance, risk, status, issues, and status of past action items or tasks). Review of monitoring reports to identify service deficiency/ deviation and assessment of impact due to the deficiencies/ deviations. Review of notices and action-taken reports for action taken to be commensurate with impact on business and contractual provisions.
Audit Conclusion: To be filled in by auditor	

Data Rights

Audit objective: To assess whether the organisation's data protection requirements are identified, and that they are part of the contractual requirements.

AUDIT Issue 4: Data protection and management of data

- Are the data protection and access rights built into the service contract?
- Is the data defined appropriately to cover the transaction data as well as the programs/ software supporting the data, as the case may be?
- Is there a mechanism to ensure that the data protection and security requirements as per the Service Level Agreement are being adopted and implemented by the service provider?

Criteria

Organisation's data protection and access rights requirements are levied on the contractor as appropriate.

Information Required	Analysis Method(s)
Organisation's Data Protection and access rights requirements	Document review on adequacy of data protection and access rights requirements/ definition of data.
Definition of data (for protection and access rights)	Document review of the contract with service provider to check for incorporation of Data Protection and access rights requirements.
Contract with the service provider	Document review of third party/ self audit reports.
List of data access records from the service provider	Document review of the monitoring reports, correspondence and incident handling reports to assess the follow-up activities by the organisation.
Reports of third party audits or self audits with recommendations and follow up on them	Review of the non-disclosure agreement to verify that all relevant information is covered.
Monitoring reports	Verify if the disclosure of information by outsourced agency is authorised.
Correspondence with the service provider on the subject	
Incident handling reports	
Non disclosure agreement with the outsourced agency	
List of information disclosed by the outsourced agency to third party / unrelated party(s).	

Audit Conclusion:

To be filled in by auditor

Overseas Service Provider

Audit objective: To determine if the organisation has strategy on contracting services to overseas vendors.

AUDIT Issue 5: Management of vendor who is overseas

Whether the organisation understands the issues involved in outsourcing to overseas agencies while outsourcing to overseas agencies?

Criteria:

Provisions of outsourcing policy related to outsourcing to overseas agencies.

Laws of land regulating business with overseas agencies.

Information Required	Analysis Method(s)
List of laws and regulations related to outsourcing services	Document Review to assess that the organisation has identified risks related to outsourcing to overseas service provider.
Information on any in-country presence of the service provider	Document review to assess the cost benefit analysis addressed the risks related to outsourcing to overseas service provider.
List of foreign offices of the organisation	Document review to assess that adequate background check on the service provider has been carried out.
List of laws and regulations regulating the service provider in their country	
Bilateral agreement between the country of organisation and the service provider facilitating outsourcing agreements	

Reports on vendor's past performance on delivery times and quality issues in Cost benefit analysis of indigenous and overseas service provider Outsourcing contract and Service Level Agreement Information on escrow amount/ financial guarantee related to performance List of deviations from the Service Level Agreement and outsourcing contract Monitoring and follow up reports on action taken on deviations by the service provider.	Document review to assess that a robust system is in place to ensure performance on Service Level Agreement and outsourcing contract. Document review to assess that any deviations from Service Level Agreement and the contract are followed up in a timely manner ensuring minimum downtime and loss to the organisation.
Audit Conclusion: To be filled in by auditor	

Retaining Business Knowledge/ Ownership of business process

Audit objective: To assess whether the agency retains business knowledge and ownership of business process(es).

AUDIT Issue 6: Policy on ownership of business knowledge and processes

- Is the business process ownership well delineated and documented?
- Is it ensured that the loss of business knowledge due to outsourcing does not occur?
- Is there capacity to conduct the outsourced services in house?
- Can business continuity be ensured if the vendor was unable to provide services at any point/ in future?

Criteria:

Organisations retain business knowledge and are able to continue operations in-house for mission critical function if contractors or vendors are unable to provide the service.

Retention of business process ownership.

Retention of business knowledge.

Performance vis a vis business continuity with respect to the service provider failing to provide service at any point.

Information Required	**Analysis Method(s)**
Identification of business processes, and critical skills that need to be retained in-house	Document review to assess that the ownership of the process, data and application software is retained by the organisation through adequate provisions in the contract.
Documentation of business processes	Document review to assess that the business knowledge in terms of data, application software, system design are well documented and that the staff is updated with these periodically through training etc.
Detailed system design document of outsourced service with the organisation	Document review to assess that the organisation and its staff are involved in any system updates carried out by the outsourced agency and the detailed system update documentation is provided to the organisation.
List of training of staff on the business processes, system design, data, application software	Document review to assess that there are no incidents or disputes with the service provider with respect to ownership of system and data.
Incident reports/ correspondence related to stoppage of service/ dispute with the service provider, including those related to ownership of system/ data	Review meeting minutes with the contractor to ensure that if there are any high level risks they are jointly managed and tracked to ensure continuity of operations.
Meeting minutes with contractor.	
Audit Conclusion: To be filled in by auditor	

Cost control and management

Audit objective: To assess whether the organisation has ensured most economical cost through the life cycle of the outsourced contract.

AUDIT Issue7: Cost benefit Assessment

- Have all the costs (including future costs) for outsourcing been identified?
- Has due cost-benefit analysis been carried out and best option been chosen?
- Are there specific responsibilities on the organisation in the outsourcing, and do they have critical cost elements/ impacts built in?
- Are additional costs or escalated costs being charged to the agency?

Criteria:

The cost benefit analysis is realistic and is the basis on which the programme is managed and controlled.

Information Required	Analysis Method(s)
Initial cost benefit analysis	Document review to assess that all costs have been identified by the organisation, reviewed and approved by relevant stakeholders.
Estimated cost of outsourced contract	Document review of the selection and approval process.
Selection process of the service provider vis a vis cost element	Document review to assess that all costs are reflected in the contract and that there are no hidden costs including any future costs.
Approval process documents related to selection	Review that all costs are subject to cost-benefit analysis before commitment by the organisation.
Instances of additional costs/ escalation of costs by the service provider	Review and comparison of estimated vs. actual expenditures on the contract.
Service Level Agreement and contract	Review of expenditure vis a vis the available budget.
Monitoring reports with respect to specific function/ activity for which escalation / addition of cost is being sought	Review of the performance of service provider on specific activity/ function for which change in cost is sought through monitoring reports and assess the need for such change.
Action documents on requests for additional costs/ escalation of costs by service provider.	Review of action by organisation on additional costs/ escalation of costs by service provider.

Audit Conclusion:

To be filled in by auditor:

Service Level Agreement

Audit Objective: To assess whether the agency has developed the Service Level Agreement detailing all its requirements and is actively monitoring the vendor against the agreement.

AUDIT Issue 8: Adequacy of Service Level Agreement

- Is a service level agreement agreed to between the organisation and the service provider?
- Is the service level agreement detailed enough to identify all roles and responsibilities between the organisation and the service provider?
- Is the service level agreement implemented diligently?
- Does the organisation have a mechanism to monitor the implementation of the service level agreement?
- Is there a mechanism available to address exceptions to the service level agreement?

Criteria:

The service level agreement is the basis for monitoring and controlling the contractor or vendor against technical and other requirements.

Information Required	Analysis Method(s)
Service level agreement or contract	Document review to assess that all user requirements are translated to service level requirements.
Technical and other requirements (list of services that will be performed by the vendor)	Document review to assess that the roles and responsibilities of the organisation and the service provider are clearly identified and delineated.

List of responsibilities of organisation and vendor Baselines for the services that will be measured, measurement period, duration, location, and reporting timelines (defect rates, response time, help desk staffing hours, etc.) Periodic vendor performance status reports.	Document review to assess that the parameters for performance levels are clearly identified and included in the service level agreement. Document review to assess that the service level monitoring mechanism is established and agreed to between the organisation and service provider. Review vendors status reports to assess that the parameters in the SLA are being reported on by the contractor and reviewed by appropriate personnel within the organisation. Assessment of compliance to SLA technical parameters and baselines. Verify the action taken by the organisation for deviations from service level agreement.
Audit Conclusion: To be filled in by auditor:	

Security	
Audit objective: To assess whether the security requirements are addressed in outsourcing and being complied with.	
AUDIT Issue 9: Response to security requirements • Have the security requirements been identified by the organisation with respect to outsourcing? • Is there a mechanism ensuring that the security requirements of the organisation are addressed by the service provider? • Does the organisation have a mechanism to monitor compliance to security requirements by the service provider?	
Criteria: The organisation's pertinent security requirements are levied on the contractor as appropriate.	
Information Required	**Analysis Method(s)**
Organisation security policy Outsourcing Contract Service Level Agreement Inventory of data, application software and hardware with the service provider Inventory of back up data files and application software with the service provider Access control logs of the data files, application software as well as hardware at the outsourced location Security plan for the back-up site and disaster recovery site Monitoring reports with respect to security issues Correspondence between organisation and service provider with respect to security issues.	Document review to assess that the security requirements have been identified by the organisation and built into the outsourcing contract or SLA. Verify if the organisation has the inventory of data files, application software. Verify that the organisation monitors/ is aware that status of data files, application software and hardware are preserved during the back up and data recovery process carried out by the outsourced agency. Verify if the organisation has assurance on authorisation of any change in data, application software and hardware by the outsourced agency. Verify if the organisation has an assurance on the access to the data, application software and hardware at the outsourced location through study of access logs (physical and logical). Verify if the organisation has assurance on security mechanisms put in place by the service provider. Verify if the organisation receives regular reports and acts on the information in the monitoring reports.
Audit Conclusion To be filled in by auditor:	

Back-up and disaster recovery for outsourced services	
Audit objective: To assess whether outsourced services adhere to business continuity and disaster recovery plans as required in the contract or service level agreement.	
AUDIT Issue 10: Backup and Recovery Procedures Is the vendor meeting the requirements of the contract or SLA for BCP and DRP?	
Criteria: Contractual or service level agreement for BCP and DRP at the vendor.	
Information Required	**Analysis Method(s)**
Contract or SLA Internal Audit or third party certification of BCP and DRP readiness of the vendor Periodic reports of BCP / DRP testing or updates.	Review contract or SLA to ensure that the vendor is required to ensure BCP and DRP on the outsourced data, applications and services. Review contract or SLA to ensure that the vendor is to provide independent or internal audit reports that confirm that BCP/DRP activities are in place and that the vendor tests their procedures periodically. Review submitted reports from the vendor to ensure that testing has been conducted in accordance with the conditions of the contract and /or SLA. Review periodic reports to ensure that the procedures have been updated if needed.
Audit Conclusion To be filled in by auditor:	

APPENDIX VI

SUGGESTED MATRIX FOR AUDIT OF BCP/DRP

Business Continuity Policy	
Audit objective: To assess whether there is an effective business continuity policy in the organisation.	
AUDIT Issue 1: Policy Does the organisation have a contingency plan and policy for business continuity?	
Criteria: The organisation has a published/ approved and adopted contingency plan and has a policy in place that comprehensively covers all areas of contingency operations and clearly identifies training requirements and testing schedules.	
Information Required	**Analysis Method(s)**
Business Continuity Policy Document	Document review for assessing that the policy is consistent with the organisation's overall IT policies.
IT Policy Document Approval process for adoption of business policy objectives	Document review to assess that the policy addresses requirements of business continuity by defining organisation's contingency objectives, organisational framework and responsibilities for contingency planning.
Correspondence and minutes of meetings related to business continuity	Review or interview personnel to determine how often the policy is updated if conditions change. Review policy to determine who approved it and when was it last distributed / interview a sample of business users to assess if the policy has been sufficiently communicated within the organisation.
Audit Conclusion: To be filled in by auditor	

Organisation of Business Continuity Function	
Audit objective: To assess whether an adequate business continuity team is in place.	
AUDIT Issue 2: Business Continuity Function Is there a business continuity team or equivalent function in place?	
Criteria: Coverage of all critical areas of the organisation in the team. Roles and responsibility requirements for the team members.	
Information Required	**Analysis Method(s)**
Organisation chart of organisation	Document review / Interview relevant staff to assess that all critical areas of organisation are represented in the business continuity team or equivalent
Organisation chart of business continuity team Role/ responsibility description of the business continuity team members	Document review to assess that there is adequate ownership and assignment of business continuity responsibility on the senior management. For example, has the management identified the level and urgency of recovery, and is this reflected in the policy? Document review to assess that all critical departments have assigned team members for disaster recovery and their roles are clearly laid out.
Correspondence / meeting minutes on issues of business continuity Business continuity plan	Interview a sample staff in business continuity team / equivalent to assess that they are aware of their roles for business continuity for each critical business unit/ department.

Audit Conclusion: To be filled in by auditor

Business Impact Assessment

Audit objective: To assess whether the business impact assessment and risk assessment have been completed and a risk management system is in place.

AUDIT Issue 3: Risk Assessment

Have business impact analysis and risk assessments been carried out and critical data, application software, operations and resources been identified and prioritised?

Criteria:

Enterprise Risk Management framework or equivalent

Business Continuity Policy or equivlent

Completion of the Business Impact Assessment and identification of critical data, application software, operations and resources.

Information Required	Analysis Method(s)
Risk Assessment report(s)	Document review to assess that the risk assessment was carried out, probable threats and their impacts are identified.
Business impact assessment report(s)	Document review to assess that all functional areas were considered in the risk assessment and impact assessment.
List of critical data, application software, operations and resources for each function	Document review to assess that the impact analysis evaluated the impact of any disruption in relation to time and other related resources and systems.
List of residual risks	Document review to assess that the decision on residual risks were taken at appropriate level.
List of related stakeholders	Document review to assess that the organisation has determined RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) for each critical application.
Review report(s) on risk and business impact assessment	Document review to assess that the RTOs and RPOs are practical and reasonable for each application and line of business or function.
Enterprise risk assessment policy/ framework	Document review to assess that the senior management involvement/ approval.
Minutes of meetings on risk assessment and business impact assessment.	Document review to assess that relevant stakeholders were involved in risk identification and impact assessment.

Audit Conclusion: To be filled in by auditor

AUDIT Issue 4: Risk Management

Is a risk management process (including mitigation and tracking, etc.) in place and have emergency processing priorities been established?

Criteria:

Coverage of the risk management process vis a vis risk assessment and business impact assessment.

Risks and emergencies are promptly addressed as per organisation's agreed parameters.

Information Required	Analysis Method(s)
Risk Management process document	Document review to assess that the risk management process addresses all high priority items.
Risk Assessment and Business Impact Assessment Report(s)	Interview and document review to assess that all relevant personnel, including senior management are aware of their role and responsibilities and carry them out.
List of all relevant personnel, members of the BCP team with roles and responsibilities	Document review to assess that the residual risks do not have material impact on the organisation.
List of prioritized items for emergency process	

List of residual risks identified List of instances of emergency process being invoked Emergency process/ response reports.	Document review and observation to assess that the emergency instances are adequately handled. Document review to assess impact of the emergency. Review meeting minutes or list of risks to determine that risks have been assigned, mitigation activities defined, and that risks are tracked periodically and status updated.
Audit Conclusion: To be filled in by auditor	

Disaster Recovery Plan	
Audit objective: To assess whether the Business Continuity Plan includes back-up and recovery plans for hardware, data, application software and data centre (recovery) and has been suitably implemented?	
AUDIT Issue 5: Back-up Procedures Have the data and program back-up procedures been devised and implemented effectively?	
Criteria: Established criticality of applications and functions as per Organisation's Business Impact Assessment. Determined periodicity of back-ups. Documented back-up and recovery plans.	
Information Required	**Analysis Method(s)**
Back up plans and procedures for the hardware, data, application software Back-up logs/ Version logs Roles and responsibilities for back-up List of storage locations and periodicity Retention schedule Security arrangement for back-up site Disaster logs Roles and responsibilities for recovery activities Training records of responsible personnel Impact assessment of disasters Report on disaster recovery activities.	Document review to assess that the back-up plan includes all critical hardware, data, application software. Document review to assess that detailed back-up procedures have been devised. Document review to assess that the back-up plan is adequately implemented. Analysis of logs to assess the back-up is taken at determined timelines and are retained for the specified time period. Verify that the right version of back up is available. Document review to assess the adequacy of back-up location and the mode of transport of back up files etc to the back-up location. Verify that the security, logical or physical is adequate for the back-up site. Verify that the back-up files can be used for recovery. Document review to assess that back-up procedures are implemented minimising loss of time and resources. Document review to assess that detailed recovery procedure has been devised and includes resetting of system parameters, installation of patches, establishing the configuration settings, availability of the system documentation and operating procedures, reinstallation of application and system software, availability of most recent backup, and testing of system. Document review to assess that recovery procedures are implemented minimising loss of time and resources. Document review/ Interview staff to assess that the relevant staff have been trained on the back-up and recovery procedures.
Audit Conclusion: To be filled in by auditor	

Environment Control

Audit objective: To assess whether the organisation has suitable environment control at back-up sites.

AUDIT Issue 6: Control Mechanisms

Has an environment control mechanism been devised and put in place at the back-up site.

Criteria:

Environment control parameters in the environment control mechanism.

Information Required	Analysis Method(s)
Environment Control programme List of probable environment hazards identified during risk assessment with locations (risk assessment document) List of environment mitigating steps undertaken.	Document Review , observation, walk through of procedues to assess that: • Un-interrupted power supply is available. • Adequate fire protection system is put in place. • Humidity, temperature and voltage are controlled within limits. • Adequate flood protection system is put in place. • Environment controls are as per the regulations. • Environment control measures are conveyed to and adhered to by all concerned staff.

Audit Conclusion:

To be filled in by auditor

Documentation

Audit objective: The business continuity plan is adequately documented to conduct effective interim business activities and recovery procedures after a business interruption.

AUDIT Issue 7: Documented plans for back up and recovery procedures, roles and responsibilities

Does the organisation have a documented disaster recovery plan that is readily available for back-up and recovery?

Criteria:

Availability and currency of the business continuity and disaster recovery plan

Information Required	Analysis Method(s)
Business continuity plan	Document review to assess the currency of the business continuity plan.
Disaster recovery plan	Document review to assess the currency of the disaster recovery plan
Version/ currency of business continuity and disaster recovery plan	Verify if the latest version of business continuity plan and the disaster recovery plan are communicated to all concerned.
Distribution list of business continuity and disaster recovery plans to all concerned.	Determine if the business continuity and disaster recovery plan documents are available at off-site to be available in case of a disaster.
	Verify that roles and responsibilites of back-up and disaster recovery team/ related staff are clearly listed out.
	Interview a sample of staff to assess whether disaster recovery procedures are known and understood.

Audit Conclusion:

To be filled in by auditor

Testing the BCP/DRP

Audit objective: To assess whether the business continuity disaster recovery procedures have been tested.

AUDIT Issue 8: Trials

Has the organisation tested its BC and DR procedures, and what changes (if any) have been made as a result of the test?

Criteria:

The organisation should test its documented BCP and DRP procedures via drills or mock-ups to ensure that they work in actual conditions. Personnel involved in ensuring continuity should be aware of their roles.

Information Required	Analysis Method(s)
BC and DR procedures & Test procedures List of items for which business continuity/ disaster recovery plan has to be tested Frequency of testing of business continuity plan and disaster recovery plan List of tests conducted List of test criteria like RTOs and RPOs etc List of testing methods employed Test results & actions taken or test recommendations Follow up action on test results.	Document review to assess whether all relevant items are covered for testing. Document review to assess whether the tests are conducted are right intervals, in time. Document review to assess that the tests were conducted against identified criteria. Document review to assess that the tests were conducted using appropriate testing methods. Document review to assess that the recommendations are conveyed to appropriate authorities for follow-up. Document review to assess that the test recommendations are adequately followed up and the business continuity plan or the disaster recovery plan are adequately updated.
Audit Conclusion: To be filled in by auditor	

Security

Audit objective: To assess whether business continuity plan and disaster recovery plan ensure security of data, application software, hardware and data center.

AUDIT Issue 9: Efficiency of Security Indicators

To determine whether the data, application software, hardware and data centre are secured appropriately during the back-up disaster recovery procedures?

Criteria:

Security baselines for the organisation like procedures laid down in the IT security policy and disaster recovery plans

Information Required	Analysis Method(s)
Inventory of data, application software and hardware Inventory of back-up data files and application software Access control logs of the data files, application software as well as hardware Security plan for the back-up site and disaster recovery site.	Verify if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process. Verify if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software. Verify if there has been any breach of security through examination of access control logs (physical and logical).
Audit Conclusion To be filled in by auditor:	

Back-up and disaster recovery for outsourced services

Audit objective: To assess whether outsourced services adhere to business continuity and disaster recovery plans.

AUDIT Issue 10: To determine whether the outsourced service provider ensures adoption of the organisation's business continuity plan and disaster recovery plan.

Criteria:

Security baselines for the organisation like procedures laid down in the IT security policy and disaster recovery plans.

Information Required	Analysis Method(s)
Inventory of data, application software and hardware of the organisation with the outsourced agency Inventory of back-up data files and application software of the organisation with the outsourced agency Access control logs of the data files, application software as well as hardware with the outsourced agency Test results of back-up plan and disaster recovery plan at the outsourced agency Security plan for the back-up site and disaster recovery site at the outsourced agency site Strategy to ensure continuity in case of takeover of the service provider by another organisation Information on any takeover of the service provider.	Verify if the organisation verifies if the number and status of data files, application software and hardware are preserved during the back-up and data recovery process at the outsourced agency. Verify if the organisation verifies if the data, application software and hardware have undergone any change during the process of back-up or disaster recovery through study of control totals on number of records and size of files related to data and application software at the outsourced agency. Verify if the organisation verifies if there has been any breach of security through examination of access control logs (physical and logical). Verify if the organisation verifies that the testing of back-up and disaster recovery is ensured at the outsourced agency. Verify whether the organisation is aware of the risks associated with possibility of takeover of the service provider. Verify whether the organisation has ensured that the Business Continuity is embedded in the service agreement.
Audit Conclusion To be filled in by auditor:	

APPENDIX VII

SUGGESTED MATRIX FOR AUDIT OF INFORMATION SECURITY

Risk Assessment	
Audit Objective: To ensure that all risks associated with information security have been identified and an appropriate risk mitigation strategy is put in place.	
Audit Issue 1: Assessment Mechanism Does the organisation has an effective and well-documented information security risk assessment mechanism?	
Criteria: Internal policy, procedures or regulations reflect organisation's preparedness to manage critical risks	
Information Required IS Security Policy Formal procedures of risks management System configuration documentation.	**Analysis Method(s)** Analyse risk management policy, risk assessment documents and interview top management and operational level to: • understand the real role of the organisation in risk assessment procedures. • identify who are involved in assessing risks. • find out the mechanism's operational costs. • verify whether risk assessment is performed and documented on a regular basis, or whenever the conditions change. • check if the current system configuration is documented, including links to other systems. • check if the documentation contain descriptions of key risks for the organisation's system, business, and infrastructure? In the case of lack of the formal procedures and documents on risk assessment, do not underestimate controls that are embedded within the operation procedures of the organisation – verify if the compensatory control mechanism embedded within operations is effective. This can be seen by walk through of a sample of operations etc.
Audit Issue 2: Coverage Does the risk assessment cover all important internal and external risks? Are possible effects and impact of Information Security breaches assessed?	
Criteria: All the significant risks are identified and assessed properly (best practices in risk assessment[51]).	
Information Required Documented Risk Assessments Risk register Incident handling reports.	**Analysis Method(s)** Review documents to check if the risk assessment performed by the audited organisation was based on sufficiently comprehensive information. Check whether data and reports were obtained from the organisation's incident management system. (Support your analysis with results of Analysis Methods of IT Operations focused on Incident Management system, esp. if the information security incident handling forms a system separated from a general incident management system.) ***Validation Test 1:*** Security audit trails: Determine if security audit trails capture user identification (ID), type of event, data and time, success or failure indication, origination of event, and the identity or the name of the affected object

[51] ISO 27005 information security risk management, ISACA RiskIT Framework, COSO Enterprise Risk Management Framework.

	Interview relevant personnel to verify whether there is a standard re-assessment of risk whenever the organisation plans to roll out new information systems, upgrades, and new versions. Check the risk assessment design for completeness, relevancy, timeliness and measurability. Check if consequences of infrastructure inoperability is considered while assigning risk categories. Verify documents to see if a business impact analysis is done for the consequences of critical information becoming unavailable, corrupted, inappropriately compromised or lost. Review incidence response reports and earlier risk documents/ registers to examine whether the risk assessment methodology has been effective in the past.
Audit Issue 3: Mitigation Are significant risks mitigated in effective and efficient way?	
Criteria: Adequate risk mitigation practices are in place.	
Information Required Problem/incident handling reports Periodic activity reports.	**Analysis Method(s)** Review incident handling reports and check whether appropriate procedures were in place to prevent, detect and control security risks identified in the risk assessment document. In organisations that do not follow a well-defined risk assessment mechanism, determine what compensatory control exist. Analyse if any serious security incidents occurred in relation to risks that might have been mitigated better with a properly working risk assessment mechanism, vis-à-vis existing compensatory controls. Take into account that problem/incident reports may be incomplete in some cases. Nevertheless, important events may be reflected directly or indirectly in other documents, as e.g. annual activity reports or other periodic reports.
Audit Conclusion: To be filled by the auditor	

Information Security Policy	
Audit Objective: To assess whether there is adequate strategic direction and support for information security in terms of a security policy, its coverage, organisation-wide awareness and compliance.	
Audit Issue 4: Information Security Policy Does the organisation possess an Information Security Policy? Is it properly implemented and documented? Does it form a consistent and robust IT security plan?	
Criteria: The organisation's information security policy covers all operational risks and is able to reasonably protect all business critical information assets from loss, damage or abuse.[52]	
Information Required IT Strategy Legal acts defining information security requirements Formal and written information security policy	**Analysis Method(s)** Check the document to examine whether IT Strategy adequately highlights the critical role of Information Security. Also refer and use the *IT Governance* matrix for *IT Strategy*. In the absence of a written IT strategy, interview top management, middle level management and staff to see what is their understanding of the strategic role of Information security. Assess compliance of the organisation's *IT Strategy and Information Security Policy* external compliance requirements

[52] See ISO 27000 series Information Security Management System and other internal policy, procedures or applicable regulations.

Organisation structure and its job description Contractual arrangements with external parties IT Security Plan.	Compare policy goals and security procedures to determine the effectiveness of integration of information security requirements into the IT security plan (charter, framework, manual etc.). Verify whether it is regularly reviewed at appropriate management levels. Examine coverage of the IT security plan and check whether it considers IT tactical plans, data classification, technology standards, security and control policies and risk management. Check if the IT security plan identifies: Roles and responsibilities (board, executive management, line management, staff members and all users of the enterprise IT infrastructure), Staffing requirements, Security awareness and training; Enforcement practices; and the need for investments in required security resources. Review and analyse the charter to verify that it refers to the organisational risk appetite relative to information security, and that the charter clearly includes scope and objectives of the security management function. Check security incident reports and follow-up documents to find what actions the organisation takes when individuals violate the security policy. Check the incident reports to identify the number of Information Security breaches by employees or external parties in given period to assess effectiveness of the policy.
Audit Issue 5: Confidentiality Has the organisation confidentiality requirements or non-disclosure agreements that appropriately reflect the need for protecting information? Do the policies secure information in the organisation's relation with external parties?	
Criteria: The organisation's information security policy is able to protect all confidential information related to internal stakeholders and third parties	
Information Required	**Analysis Method(s)**
External and internal regulations concerning confidential and classified information. Eg, Non-disclosure clauses for employees. Contractual arrangements with external parties Information security policy IT Security Plan.	Check procedural measures taken by the organisation to comply with the confidentiality requirements. Where access to confidentiality breach cases are restricted to special law procedures and specialised agencies only, base your opinion on their reports and recommendations to the organisation's management – if available. Review contractual arrangements with external parties or contractors. Do they involve granting and invoking access, processing, communicating or managing organisational information assets? Check whether the contractual terms and obligations define the security restrictions and obligations that control how contractors will use organisation's assets and access information systems and services. Check whether any information security breaches were committed by contractors. Check management action on such breaches.
Audit Conclusion	

Organization of IT Security	
Audit objective: To ensure the secure operation of IT processing facilities.	
Audit Issue 6: Structure Does the auditee have clear organisation of IT security? Are security roles and responsibilities defined with regard to information security policy?	
Criteria: Documented and clear IT roles and responsibilities relating to Information Security Policy[53]	
Information Required	**Analysis Method(s)**
IT Organisation structure Internal regulations related to IS security Job descriptions Minutes of relevant bodies' meetings.	Determine if the responsibility for IT security is formally and clearly stated. Check whether a process exists to prioritise proposed security initiatives, including required levels of policies, standards and procedures. Check how senior management maintains an appropriate level of interest in information security within the organisation.
Audit Issue 7: Coordination How does the organisation coordinate information security activities from different parts of organisation?	
Criteria: No responsibility conflicts, disharmony nor "no-man's land" in Information Security activities[54]	
Information Required	**Analysis Method(s)**
Legal requirements concerning classified information Organisation structure Internal regulations related to IS security Minutes of meeting of IT security committee Failure reports.	Check documents, observe practices and interview personnel to verify whether there are inherent conflicts/ overlaps/ gaps between security procedures followed by employees in different departments/ units. Check operational workflow procedures to identify if some information is transmitted to external parties out of control of responsible units/employees. Check if higher level managers are aware of coordination problems and whether they supervise inspections and coordinating activities. Review processes to check whether there is any established procedure for management to authorize new information processing facilities.
Audit Conclusion To be filled by auditor	

Communications & Operations Management	
Audit objective: To ensure that internal and external communication is secure.	
Audit Issue 8: Policy and procedures Are policy and procedures adequate for safe and efficient internal and external communication?	
Criteria: The policy and procedures form stable management environment for internal and external communication[55]	
Information Required	**Analysis Method(s)**
Formal and written policy for communications and IT operations Documentations of operational procedures.	Check whether the policies and procedures of the organisation embrace communication with citizens, mass media, and external organisations. Verify how the organisation documents its operating procedures and makes them available to all users. Interview a sample set of users at different levels to examine whether the procedures for data handling are well known by employees. Check how often the communication and data handling procedures are reviewed and updated.

[53] See ISO 27000 series

[54] See ISO 27000 series Information Security Management System

[55] See following standards: : ISO-27002, S15-IT Control (ISACA Standard), COBIT

Audit Issue 9: Network control How does the organisation manage and control information in the network?	
Criteria: Network operations are managed and performed in safe and effective way[56]	
Information Required	**Analysis Method(s)**
Information restriction policy Network Admin Logs/ Registers Results of the logs analysis User Acceptance Test Report Service Level Agreement(s) Information available to the public or found in the web pages.	Check what tools are used for network monitoring and analysis. verify whether users and IT systems of the audited organisation are protected against spam. Check whether Intrusion Detection System configurations and logs are analysed by appropriate personnel to ensure security of information from hacking attacks and malware intrusions. Verify whether the attacks (failed and effective ones) are analyzed and reported. Check the statistics of spam, hacking and malware attacks. Inquire how the organisation provides secure transmission of transactions passing over public networks. Eg. Circulating/ notifying operating procedures to users for e-commerce/ online transactions. Review policies to verify whether data transmission outside the organisation requires an encrypted format prior to transmission. Inquire whether information security policies have been implemented in accordance to the sensitivity classification of organisation's data (e.g., confidential, sensitive). Through enquiry determine whether the client utilises cryptography for sensitive information processing. If so, conduct a validation testing. **Control Validation Testing Procedures** ***Validation Test 1:*** Operating effectiveness of cryptographic controls: Determine: • the existence of processes for the key management life cycle. • key destruction. • segregation of duties for the authorised key custodians.
Audit Issue 10: Configuration Management Are the IT resource settings/ applications under appropriate configuration control?	
Criteria: Clear and well-managed configuration system that supports Information Security in communication and operations.	
Information Required	**Analysis Method(s)**
Policy and procedures referring to configuration matters in operations area Configuration lists/ library.	Review role matrices to determine who is responsible for administering the configuration, and what the scope of the configuration control in operations is. Check how it is registered, controlled and updated. Verify if any problems occurred in the past because of configuration discrepancies. If so, interview managers to check what procedures have been implemented to configuration changes
Audit Conclusion To be filled in by the auditor	

[56] *ibid*

Assets Management	
Audit objective: To encourage appropriate protection of IT assets.	
Audit Issue 11: Assets Management Does organisation have an appropriate asset management system that supports its Information Security?	
Criteria: Ensuring appropriate protection of information assets (Ref: ISO 2700 series Information Security Management System, COBIT, and other internal policy, procedures or regulations applied).	
Information Required	**Analysis Method(s)**
Asset management policy Asset Classification Information classification Asset disposal procedures Financial audit reports (if they refer to assets and inventories).	Review policy to check if there is an acceptable use policy for IT hardware and software (Example, laptops may be used for personal use if it does not interfere with official business). Check whether the asset database is up-to-date. Check inventory records to verify whether assets are categorised in terms of value, sensitivity, or other categories. Review procedures for assets disposal and the level of supervision mandated. Check the authorisation requirement for any disposal or re-use of equipment. Inquire persons and check provisions that ensure data is erased prior to disposal or re-use of equipment.
Audit Conclusion	

Human Resources Security	
Audit objective: To ensure that all employees (including contractors and any user of sensitive data) are qualified for data handling and understand their roles and responsibilities, and that access is removed once employment/ contract is terminated.	
Audit Issue 12: Staff Awareness and Responsibility Are employees aware of their roles and responsibilities with respect to their duties and security responsibilities?	
Criteria: Professionlly trained staff in guarding information security	
Information Required • HR Policy and recruitment procedures • Information Security policy and procedures • Competency Standard for IT Personnel • Individual assessment reports • Security incident reports (including violation of code of ethics or code of conduct) • Security Awareness Campaign • User Management Roles and Responsibilities.	**Analysis Method(s)**[57] Inspect hiring documentation for a representative sample of IT staff members to evaluate whether background checks have been completed and evaluated. Inspect selection criteria for performance of security clearance background checks. The role of each position must be clear. Supervision activities should be run to check adherence to management policies and procedures, the code of ethics, and professional practices. Check if roles thay are critical for Information Security are clearly defined and documented. Employees and third parties assigned such roles should know their responsibilities with respect to protecting the organisational information assets, including electronic data, IS infrastructures, and documents. Review for appropriate definition of critical roles, for which security clearance checks are required. This should apply to employees, contractors and vendors. Check for appropriate Segregation of Duties between IT security management and Operations. Check if the policy of IT personnel placement, transfer and rotation, as well as employee termination is clear to reduce dependence on the individual. Verify what knowledge transfer mechanisms are followed.

[57] Human resources *vis-à-vis* Information Security is one of key topics in other sections including *IT Governance*, and portions of this Audit Matrix such as *Information Security Policy* (awareness, responsibility, top-down information flow, sanctions) and/or *Access Control* (individual user rights).]

Audit Issue 13: Training Is training in Ind\formation Security procedures effective in enhancing staff's professional skills in guarding the same ?	
Criteria: Conduct, Scope and Periodicity of Orgnisational Training for Information Security.	
Information Required	**Analysis Method(s)**
Training schedule Results of ending tests Evaluation of training effectiveness.	Assess the training effectiveness measurement process, if any, to confirm that the critical IT security training and awareness requirements are included. Inspect IT security training programme content for completeness and appropriateness. Inspect delivery mechanisms to determine whether the information is delivered to all users of IT resources, including consultants, contractors, and temporary staff members and, where applicable, customers and suppliers. Inspect training programme content to determine if all internal control frameworks and security requirements are included based on the organisation's security policies and internal controls (e.g., impact of non-adherence to security requirements, appropriate use of company resources and facilities, incident handling, employee responsibility for information security). Inquire whether and confirm that training materials and programmes have been reviewed regularly for adequacy. Inspect the policy for determining training requirements. Confirm that the training policy ensures that the organisation's critical requirements are reflected in training and awareness programmes. Interview staff to asess whether they have undergone the organisational training and whether responsibilites in maintaining information security and condfidentiality are clearly understood by them.
Audit Conclusion	

Physical Security	
Audit objective: To prevent theft or damage of IT hardware, unauthorized access, and copying or viewing of sensitive information.	
Audit Issue 14: Premises safety Are the buildings and grounds of the organisation secured against physical and environmental risks?	
Criteria: Ensure that physical and environmental security stays in compliance with the safety requirements and sensitivity classification of IT assets.	
Information Required	**Analysis Method(s)**
Network diagram Site Security Plan Periodical physical testing report Reports by relevant services (eg. Fire dept).	Analyse what the audited organisation's primary physical security controls are. Check if they match the up-to-date risk analysis. Review location and physical precautionary measures for key elements of IT infrastructure. Check what environmental controls are in place (fire extinguisher, alarm, power systems, etc). Verify if recommendations by relevant services (esp. firemen, housing inspection, disaster prevention) been implemented. (For security plans relating to disasters, refer to BCP and DRP section of this Handbook).

Audit Issue 15: Physical access How the organisation ensures that only authorised personnel access the facility?	
Criteria: Security measures are put in place by the organisation to ensure no unauthorised physical access to critical IT facilites (server rooms, data storage etc)	
Information Required	**Analysis Method(s)**
Layout of IT hardware installation Site Security Plan Devices configuration Periodical physical testing report Incident reports.	Review security instructions, network diagram and related documents and check how the organisation controls access to sensitive areas of its premises. Review and observe the in/out traffic and how the physical security system works. Determine what means are used. Obtain policies and procedures as they relate to facility security (gates, badges, turnstiles, guards, barriers, key and card reader access etc.) and determine if those procedures account for proper identification and authentication. Check who maintains and controls the allocations of access control to the sensitive locations. Find if the level of management is sufficient for Information Security. Find if access to secure areas /secure rooms/ server locations is restricted. Select a sample of users/employees and determine if their access to facilities is appropriate, based upon their job responsibilities. Verify if incidents are reported to an incidents/problems management system. Find if they are analysed and lessons learnt.
Audit Issue 16: Intrusion defense. Whether the organisation has a policy on intrusion detection and follows it	
Criteria: Procedure to comabt intrusions as laid down in Organisation's Internal Security Policy	
Information Required	**Analysis Method(s)**
Site Security Plan Devices configuration Incident reports.	Inquire how the organisation's security unit knows that an intrusion has occurred to secure locations. Check instructions to find out the Process for handling an intrusion to a secure space or building. Check incident reports to identify whether intrusion was detected early. Check if the organisation have a clear desk or clean screen policy to prevent unauthorised access.
Audit Conclusion.	

Access Control	
Audit objective: To ensure that only authorised users have access to relevant information	
Audit Issue 17: Access policy Does the organisation have clear and efficient policy on access control?	
Criteria: The Access Policy gives sound basis for control of relevant information distribution.	
Information Required	**Analysis Method(s)**
Access Policy and procedures List of users Access control list/ matrix.	Analyse Access Policy and procedures to ensure that employee duties and areas of responsibility are separated in order to reduce opportunities for unauthorised access and privilege approval. ***Validation Test:*** Operating effectiveness of authorisation of user access to the LAN (not separate testing of user access to applications should be done in conjunction with application reviews).

	Select a sample of user and system accounts to determine existence (access control software maybe used) of the following: • clearly defined requested role and/or privileges mapped to job functions. • business justification for access. • data owner and management authorisation (i.e. signatures/ written approvals). • Business/risk justification and management approval for non-standard requests. • Access requested is commensurate with job function/role and required segregation of duties.
Audit Issue 18: Privileges management. Is process for granting and revoking access control to employees and contractors safe and effective?	
Criteria: The Information Security function monitors user account management operations on a timely basis and reports the operating efficiency and effectiveness.	
Information Required Access control procedures Sample of employees' transfers and terminations.	**Analysis Method(s)** Check procedures to determine how often the various accesses and privileges that employees or users have in the organisation are reviewed. **Check how the privileges that are granted to an employee are confirmed (Examples include asking the supervisor, area manager, group, etc.)** Interview sample of users and check instructions to verify how the users are informed about their responsibility for protecting sensitive information or assets when the access is granted to them. Determine whether the organisation's security practices require users and system processes to be uniquely identifiable and systems to be configured to enforce authentication before access is granted, and that such control mechanisms are utilised for controlling logical access across all users, system processes and IT resources. Analyse other than password privileges, e.g. how it is checked that a user does indeed have sufficient access and privileges to the requested resource? (Examples include access from secure location, hardware tokens or fingerprint readers, etc.) ***Validation Test 1:*** Operating effectiveness of transfers and terminations: Obtain from HR a sample of employee transfers and terminations and, through review of system account profiles and/or CAATs (e.g. ACL, IDEA) determine if access has been appropriately altered and/or revoked in a timely manner. ***Validation Test 2:*** Password management: Verify that the quality requirements for passwords are defined and enforced by the network management system and/or operating systems based on local requirements/ organisation policy or best practice.
Audit Conclusion	

IT Systems Acquisition, Development and Maintenance is in Appendix III

Business Continuity Management is in Appendix VI

APPENDIX VIII

SUGGESTED MATRIX FOR AUDIT OF APPLICATIONS CONTROLS

<table>
<tr><th colspan="2">Input</th></tr>
<tr><td colspan="2">Audit objective: To assess whether valid data is being entered into the application by authorised personnel.</td></tr>
<tr><td colspan="2">AUDIT Issue 1: Validation of inputs
Does the application have adequate input validation controls?</td></tr>
<tr><td colspan="2">Criteria:
Several good practices provide basis for criteria of good inout validation controls, e.g.
validation rules are comprehensive ,documented and implemented into the application entry interfaces; different methods and interfaces for data entry are documented; invalid data is properly rejected by the application; the validation criteria is updated in a timely, appropriate and authorised manner; there are compensating controls such as logs and authorisation rules in case of the possibility of overriding input controls; and there are proper controls and documentation for the application interfaces.</td></tr>
<tr><td>Information Required
Business requirements and rules
Data input types
Legal and external compliance requirements
Structure of data interfaces with other applications
System flow diagrams
User manuals
Validation rules</td><td>Analysis Method(s)
Analyse business rules, requirements, application documentation and inquire business process owners to determine which validation rules should be assured in the business process being assessed. Check if these validation rules were proper designed and documented. Verify whether the validation controls for data input are being enforced: observing application users into real action; running the application in a testing environment and testing different interfaces for data entry; and analysing data records stored in the database through the use of CAATs.
Obtain functional description for each class of input and design information on transaction data entry. Inspect the functionality and design for the presence of timely and complete checks and error messages. If possible, observe transaction data entry.
Assess whether validation criteria and parameters on input data match business rules and enforce rejection of unmatched input types. In case of online processing systems, verify that invalid data is rejected or edited on entry and test the logic checks/calculation checks performed. Database operatives (such as *, =, or, select) should be disallowed as valid input, as they can be used to disrupt or retrieve information from the database.
Inquire managers about whether validation criteria and parameters on input data are periodically reviewed, confirmed and updated in a timely, appropriate and authorised manner. Assurance could be obtained through documentation review, code analysis or interviews.
Inquire and check documentation in order to verify the possibility of overriding input data control validations and controls. Verify if the override actions are being properly logged and reviewed for appropriateness. Check whether authority to override is restricted to only supervisory staff and to a limited number of situations. Inspect error corrections, entry overrides and other documents to verify that the procedures are followed.
Determine which interfaces exist with the application. These interfaces could be in the form of real-time data transmission or periodic transmission of data files via batch processes. Review system flow diagrams and system code, and interview the application developers or administrator to obtain information on interfaces and controls over them. E.g.: Control totals from interface transmissions. E.g., Hash[58].</td></tr>
</table>

AUDIT Issue 2: Is management of source documents, data collection and entry adequate?	
Criteria: Data preparation procedures are documented and understood by users; there is appropriate logging and records of the source documents received until their disposal; there is assignment of unique and sequential numbers to each transaction and original source documents are retained for the time required by legal standards or policies.	
Information Required	**Analysis Method(s)**
Classes of source documents Entity's criteria for timeliness, completeness and accuracy of source documents Data preparation procedures Data interfaces with other applications Document retention policies System flow diagrams	Inspect and observe creation and documentation of data preparation procedures, and inquire whether and confirm that procedures are understood and the correct source media are used. Assess whether the Data Processing group (DP) or equivalent group maintains a log of all the user departments' source documents received and their final disposal. Verify the existence of a system of reconciliation of record counts with user department groups. Verify that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management. Inspect whether critical source documents are pre-numbered and how out-of-sequence numbers are identified and taken into account. Identify and review out-of-sequence numbers, gaps and duplicates using automated tools (CAATs). Verify if there is assignment of unique and sequential numbers to each transaction preventing duplication. Enquire responsible personnel about retention policies. Verify how these policies are ensured. A sample of system records might be checked against its source documents.
AUDIT Issue 3: Does the application have adequate procedures for error handling?	
Criteria: There is a system of clear and compact error messages communicating the problems so that immediate corrective action can be taken for each type of error. Errors are corrected or appropriately overridden before processing transactions. Logs are reviewed periodically and necessary corrective action is taken.	
Information Required	**Analysis Method(s)**
Error types and messages Log review procedures Policies and procedures for dealing with rejected data Suspense file review procedures	Discuss the application's error and exception handling with the developer and/or administrator. Inquire whether and confirm that policies and procedures exist for handling transactions that fail edit and validation checks. Verify whether the system provides error messages for every type of error (field level or transaction level) not meeting the edit validation. Verify how the application behaves if data is rejected by the input controls. Check whether the data items are recorded or if they are automatically written in a suspense file. Check if the automated suspense file includes codes indicating error types, date and time of entry and identify the person entering data. Evaluate if there are procedures for reviewing and correcting data in the suspense file before processing it again. Assess whether an escalation procedure is in place when error rates are too high and corrective action is taken. Ask managers about the existence of procedures for periodically reviewing the log. Verify whether the procedures include the initiation of corrective measures. Obtain evidence – either documental or digital – that the log is being periodically reviewed.

[58] PC Magazine Encyclopaedia, from http://www.pcmag.com/encyclopedia/term/44130/hash-total:
A method for ensuring the accuracy of processed data. It is a total of several fields of data in a file, including fields not normally used in calculations, such as account number. At various stages in the processing, the hash total is recalculated and compared with the original. If any data has been lost or changed, a mismatch signals an error

AUDIT Issue 4: How data entry authorisation into the application is being managed?	
Criteria: Authorisation levels for transactions were established and are enforced by proper controls; there is proper segregate of duties for data entry; and there are compensating controls in place for those cases in which segregation of duties is not possible.	
Information Required	**Analysis Method(s)**
Legal and external compliance requirements Business requirements and rules User manuals	Inquire whether and confirm that the design of the system provides for the use of preapproved authorisation lists. Verify, through inspection of authorisation lists, that authorisation levels are properly defined for each group of transactions. Assess whether authorisation rules for data input, editing, acceptance, rejection and override for major classes of transactions are well designed and documented. Observe that authorisation levels are properly applied running the application in a testing environment. Verify, through the use of CAATs or embedded audit modules, that the authorisation records present in the database are compliant to the authorisation rules defined. Determine if a separation of duties (SOD) table exists, and review for adequate separation of key duties/ job functions and permitted transactions, then, look into list of users and user-specific access privileges. Assess whether segregation of duties ensures that the person keying the data is not also responsible for verification of document. Verify the adoption of compensating controls in cases which SOD was not feasible.

Processing	
Audit objective: To assess whether the application ensures data integrity, validity and reliability throughout the transaction processing cycle.	
AUDIT Issue 5: Are the business processes rules and requirements properly mapped into the application?	
Criteria: Application transactions run accordingly to the expected behaviour.	
Information Required	**Analysis Method(s)**
Application documentation Business rules and requirements Data flow chart Highly critical transactions list Source code	Identify the executable programs in the application from a study of the data flow chart and match them with defined and established business process rules. Review the application documentation to verify that it is applicable and suitable for the task. Where appropriate for critical transactions, review the code to confirm that controls in the tools and applications operate as designed. Reprocess a representative sample to verify that automated tools operate as intended. For highly critical transactions, set up a test system that operates like the live system. Process transactions in the test system to ensure that valid transactions are processed appropriately and in a timely fashion.
AUDIT Issue 6: Do the application controls ensure the integrity and completeness of its transactions?	
Criteria: The application does correctly identify transactional errors. Data integrity is maintained even during unexpected interruptions to transaction processing. There is an adequate mechanism for handling processing errors, review of suspense files and clearance.	

Information Required	Analysis Method(s)
Application design documentation Business rules and requirements Out-of-balance reports Reconciliations Report review procedures Suspense files	Assess whether the application has adequate validity checks in place to ensure processing integrity. Inspect the functionality and design for the presence of sequence and duplication errors, referential integrity checks, control, and hash totals[59]. Inspect reconciliations and other documents to verify whether input counts are coherent with output counts to ensure completeness of data processing. Trace transactions through the process to verify that reconciliations effectively determine whether file totals match or the out-of-balance condition is reported. Inquire whether control files are used to record transaction counts and monetary values, and that the values are compared after posting. Verify that reports are generated identifying out-of-balance conditions and that the reports are reviewed, approved and distributed to the appropriate personnel. Take a sample of data input transactions. Use appropriate automated analysis and search tools to identify cases where errors were identified erroneously and cases where errors were not detected. Inquire whether and confirm that utilities are used, where possible, to automatically maintain the integrity of data during unexpected interruptions in data processing. Inspect the audit trail and other documents, plans, policies and procedures to verify that system capabilities are effectively designed to automatically maintain data integrity. Inspect the functional description and design information on transaction data entry to verify whether transactions failing validation routines are posted to suspense files. Verify that suspense files are correctly and consistently produced and that users are informed of transactions posted to suspense accounts. For a sample of transaction systems, verify that suspense accounts and suspense files for transactions failing validation routines contain only recent errors. Confirm that older failing transactions have been appropriately remediated.

Output

Audit objective: Assess whether application assures that output information is complete and accurate before further use and that it is properly protected.

AUDIT Issue 7:
Does the application have controls to ensure completeness and accuracy of its output?

Criteria:
Procedures have been designed to ensure that the completeness and accuracy of application output are validated prior to the output being used for subsequent processing, including use in end-user processing; tracking of application output is properly enabled; output is reviewed for reasonableness and accuracy; and completeness and accuracy controls are effective.

Information Required	Analysis Method(s)
Completeness and accuracy controls Methods for balancing and reconciliation List of electronic outputs / reports Sample of electronic output	Obtain a list of all electronic outputs that are reused in end-user applications. Verify that the electronic output is tested for completeness and accuracy before the output is reused and reprocessed. Examine the balancing and reconciliation of output as established by documented methods. Select a representative sample of electronic output, and trace selected documents through the process to ensure that completeness and accuracy are verified before other operations are performed. Re-perform completeness and accuracy tests to validate that they are effective. Examine if each output product contains processing program name or number; title or description; processing period covered; user name and location; date and time prepared; and security classification. Select a representative sample of output reports, and test the reasonableness and accuracy of the output. Verify that potential errors are reported and centrally logged.

[59] F/N: *ibid*

AUDIT Issue 8: Is the output data properly protected?	
Criteria: Output is handled in line with the applicable confidentiality classification; distribution of outputs/ reports are appropriately controlled.	
Information Required	**Analysis Method(s)**
Output handling and retention procedures Information classification policies	Review output handling and retention procedures for privacy and security. Assess whether procedures have been defined that require the logging of potential errors and their resolution prior to distribution of the reports. Examine the system of reconciliation of output batch control totals with input batch control totals before release of reports establishing data integrity. Check if there are documented procedures for labeling sensitive application output and, where required, sending sensitive output to special access-controlled output devices. Review the distribution methods of sensitive information and verify that the mechanisms correctly enforce pre-established access rights.

Application Security

Audit objective: Assess whether application's information is properly secured against misuse.

AUDIT Issue 9: Do the traceability mechanisms of the application are sufficient for its purpose?	
Criteria: There are audit trails that capture edits, overrides, and authorisation logs to critical transactions; the audit trails are periodically reviewed to monitor unusual activity; the audit trail is adequately maintained and protected; and unique and sequential numbers or identifiers are assigned to every transaction.	
Information Required	**Analysis Method(s)**
Audit trail structure and documentation Override policies Review procedures System flowcharts	Obtain documentation and assess the design, implementation, access and review of audit trails. Inspect the audit trail structure and other documents to verify that the audit trail is designed effectively. Inquire who can disable or delete the audit trails. Inspect the audit trail, other documents, plans, policies and procedures to verify that adjustments, overrides and high-value transactions are designed effectively to be promptly reviewed in detail. Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to verify that periodic review and maintenance of the audit trail effectively detects unusual activity and supervisor reviews are effective. Inquire how the access to the audit trail is restricted. Examine access rights and access logs to the audit trail files. Verify whether only restrict and authorised personnel have access to the audit trail. Assess if the audit trail is protected against privileged modifications. Verify, where possible, using automated evidence collection, if unique identifiers are being assigned to each transaction.
AUDIT Issue 10: Is the application data properly protected?	
For physical and logical access control refer to Appendix VII on Information Security. For disaster recovery planning refer to Appendix VI on BCP/DRP	

INTOSAI Working Group on IT Audit
c/o CAG of India
Pocket-9, DDU Marg,
New Delhi- 110124, India

www.intosaiitaudit.org

INTOSAI Development Initiative (IDI)
c/o Riksrevisjonen
Pilestredet 42
Postboks 8130 Dep.
N-0032 Oslo, Norway
www.idi.no