

Guidance on Audit of IT Management functions: IT Governance, Contracts & Sustainability

This Audit Practice Guide has been developed as a part of WGITA Work Plan with the engagement of nominated members from SAIs of Bangladesh, Ecuador, Qatar and the United States of America and led by SAI India.

INTOSAI Working
Group on IT Audit

CONTENTS

INTRODUCTION TO THE GUIDE	3
REVISION SCHEDULE:	4
ACKNOWLEDGEMENT:	4
CHAPTER 1 – AUDIT OF IT GOVERNANCE.....	5
SECTION A – IT GOVERNANCE AND RELATED RISKS	5
<i>A.1 Introduction.....</i>	<i>5</i>
<i>A.2 Key Elements of IT Governance for the Auditor.....</i>	<i>5</i>
A.2.1 Governance structures	5
A.2.2 IT Strategy	6
A.2.3 Entity Policies, procedures and processes	6
A.2.4 Control structure for IT infrastructure and services.....	7
A.2.5 People, Skills and Competencies	7
<i>A.3 Risks associated with inadequate IT Governance.....</i>	<i>8</i>
A. Fragmented IT structures and duplication	8
B. IT provides low contribution to business value	8
C. Ineffective or user-unfriendly IT systems	9
D. Ineffective IT resource management	9
E. Project failures.....	9
F. IT spending that is unknown, excessively high, or insufficient	10
G. Exposure to cybersecurity and privacy risks, such as data loss and security breaches	10
H. Poor public Service Delivery.....	10
I. Third party (vendor) dependency.....	11
J. Non-compliance with legal and regulatory requirements	11
SECTION B- INDICATIVE AUDIT PROGRAM FOR IT GOVERNANCE.....	12
SECTION C - AUDIT CASES ON RISKS RELATED TO IT GOVERNANCE AND REPORTED BEST PRACTICES	19
CHAPTER 2: AUDIT OF IT CONTRACT MANAGEMENT	26
SECTION A- RISKS ASSOCIATED WITH IT OUTSOURCING AND CLOUDSOURCING	26
<i>A.1 Introduction.....</i>	<i>26</i>
<i>A.2 Key Areas of IT contracts.....</i>	<i>26</i>
A.2.1 Application management:	26
A.2.1.1 Application Development:.....	26
A.2.1.2 Application maintenance and Production support:	27
A.2.2 Managed Services:	27
A.2.2.1 Management of IT infrastructure on premises	27
A.2.2.2 Data Centre Management.....	27
A.2.2.3 Management of Cloud-based deployment.....	28
A.2.3 Managed Security Services.....	28
A.2.4 Helpdesk Services.....	29
<i>A.3 Lifecycle of an IT Contract – Audit considerations.....</i>	<i>29</i>
A.3.1 Feasibility Assessment.....	29
A.3.2 Vendor Selection	30
A.3.2.1 Request For Proposal	30
A.3.2.2 Assessment of Bids.....	30
A.3.3 Legal and contractual obligations	30
A.3.4 Vendor Management	31
A.3.4.1 Transition management	31
A.3.4.2 Change Management	31
A.3.4.3 Service Level Monitoring	31

<i>A.4 Risks of IT contracting</i>	32
A. Information security and data privacy risks.....	32
B. Inaccurate assumptions and incorrect scoping of work	33
C. Lack of entity personnel prepared to manage Contracts	33
D. Retaining Business knowledge and strategic control	34
E. Vendor Failure to Deliver	34
F. External Risks	34
G. Vendor Lock in	34
SECTION B – INDICATIVE AUDIT PROGRAM ON IT CONTRACT MANAGEMENT (CSPs AND OTHER VENDORS)	36
SECTION C – AUDIT FINDINGS, RECOMMENDATIONS AND BEST PRACTICES IN IT OUTSOURCING	44
D. Retaining Business knowledge and strategic control.....	46
CHAPTER 3 – AUDIT OF IT SUSTAINABILITY	47
SECTION A – ELEMENTS AND RISKS RELATING TO IT SUSTAINABILITY	47
A.1 Introduction	47
A.2 Key Elements of IT Sustainability.....	47
A.2.1 Interoperability	47
A.2.2 Scalability	49
A.2.3 Adaptability	49
A.3 Governance Structure for IT sustainability	50
A.4 Risks to the audited entity.....	51
A. Hardware and Software risks	51
B. Human Resource risks	51
C. Vendor management and outsourcing.....	51
D. Governance (and top management commitment)	52
E. IT Security	52
SECTION 3B- INDICATIVE AUDIT PROGRAM FOR AUDIT OF IT SUSTAINABILITY	53

Introduction to the Guide

This practice guide aims to facilitate SAIs in carrying out IS Audit/ assurance engagements that focus on IT Governance, outsourcing (including Cloud services) and solution sustainability when public entities are either engaged in new IS implementations or considering outsourcing options or running legacy systems.

The guidance document is divided into three main Chapters. The first two Chapters build off the INTOSAI WGITA Handbook on IT Audit and the third is an independent development.

Chapter 1 addresses the important domain of audit of IT Governance – structures and processes in an audited entity/ a group of related entities - to determine the adequacy of leadership role that the Governance layer provides in steering technology adoption and Information Systems implementation in terms of Evaluating alternative proposals and strategic choices, Directing resources and strategy and Monitoring actions taken by the IT management roles.

This Chapter is divided into three Sections. Section 1A elaborates on risks that an entity faces when IT governance practices are inadequate. Section 1B provides an indicative Audit matrix for audit of this domain. Section 1C presents a set of audit findings, recommendations and best practices related to IT Governance noted in public audit engagements across the world.

Chapter 2 covers audit of IT Contract Management encompassing both outsourcing of specific IT functions and services at an audited entity and contracting Cloud Service Providers (CSPs).

Chapter 2 is divided into three Sections – Section 2A spells out the risks associated with contracting IT functions and cloudsourcing. The trend towards Cloudsourcing differs in public entities across legal jurisdictions and technological contexts, and ranges from zero adoption in some countries to a significant extent elsewhere. Audit of this domain would involve an assessment of controls relating to safeguarding business assets, data privacy, efficiency of core functions, service availability and continuity when a public entity engages a contractual entity for IS solutions for provisioning of infrastructure or services. Section 2B provides a fairly elaborate indicative Audit matrix for this domain of IT contract Management. The following Section, 2C presents a set of audit findings and recommendations related to IT contract management noted in public audit engagements across the world.

Chapter 3 seeks to address a relatively new domain for an IT Audit engagement in a public audit entity. This Chapter deals with questions of Sustainability in IT practices in a largely technological sense – in terms of interoperability of newly implemented systems, challenges that public entities face with legacy systems, significant vendor dependence, adaptability to new technology – and the like.

The Chapter on IT Sustainability is divided into two Sections. Section 3A covers risks that an entity faces when the IT Sustainability issues are not adequately addressed during design,

implementation or updation of systems. Section 3B presents an indicative Audit matrix for the Audit of IT Sustainability.

Revision Schedule:

This Practice Guide is intended to serve as a live document with a defined revision schedule of 3 years from the date of adoption and roll out, keeping pace with changing cloud service models, sustainability questions and findings from public audit engagements in the ensuing WGITA cycle.

Acknowledgement:

We wish to thank the SAIs of Ecuador, Qatar, USA and India for active participation of their nominated officials in creating this document and the WGITA secretariat for providing guidance and the CoP platform on the INTOSAI Community portal enabling close cooperation and sharing of documents and resources within the Project team.

Chapter 1 – Audit of IT Governance

Section A – IT Governance and related Risks

A.1 Introduction

A public entity needs to design and implement IT Governance in a manner that meets stakeholder needs, ensures that ongoing IT services and possible technology options are evaluated to better fit business goals; ensures that timely decisions are taken to direct IT spending ; and ensures performance and compliance are monitored against set objectives.

Specific arrangements for Governance of IT in a public entity vary on the basis of its size, nature and the entity's strategic dependence on IT. In most entities, governance is the responsibility of a designated set of senior management under the direction of the head of the entity. In smaller public entities distinct roles for Governance and Management of IT may not be clearly defined. However, a de facto top layer of Governance overseeing the functions of IT Management, evaluating proposals, considering options and directing the strategic path and resources for IT is important for the public entity to meet its functional role best.

The auditor needs to gain sufficient understanding of the design and implementation of IT Governance practices at the audited entity during the planning and initial phase of the engagement. A good knowledge of the possible risks that the entity faces when these practices are inadequate is a prerequisite for any IT audit engagement. Even if the audit assignment may not expressly cover IT Governance a lot of control weaknesses in any domain may have linkage with inadequate Governance mechanisms.

A.2 Key Elements of IT Governance for the Auditor

These are the factors that impact the strategic and operational alignment of IT to the entity's business or service goals.¹ Auditors need to understand and evaluate the different components of IT governance to determine whether the IT decisions, directions, resources, and performance monitoring support the organization's strategies and objectives. To carry out the assessment, the auditor needs to be aware of the risks associated with the inadequacy of each component in an entity.

A.2.1 Governance structures

An auditor needs to examine whether roles of various management and governance bodies within the entity are clearly defined and supported with enabling processes that facilitate decision making. For example, the entity needs to set up an IT Steering Committee or any equivalent body that includes members from top and senior

¹The key elements are supported by ISO 38500 with extensive use of its definitions and examples.

management, business as well as IT heads. The body should have the responsibility to examine business cases for IT services, decide on technology choices to support key business decisions, review availability of funds and take IT investment decisions with commitment of adequate resources. A separate Project Governance body may be entrusted with overseeing the processes of preparation of business case, solicitation and vendor engagement. Frequency of meetings of these bodies, kind of baseline information perused, projection of benefits, records of decisions taken and responses to questions raised can help the auditor in the assessment of the adequacy of functioning of the IT governance structures. Absence of these bodies critically impact transparency and accountability for IT decision making in a public entity.

A.2.2 IT Strategy

A business goal common to many public entities is to introduce or expand online services. The entity's legacy IT infrastructure and architecture may not be suited to make this transition. This business scenario would call for a clearly documented IT strategy that lays out a plan taking into consideration technology architecture, future capacity planning, investments, delivery model, as well as requirement of resources.² The auditor needs to examine whether such a strategy document or its equivalent components exist and whether it adequately meets the need for alignment between IT decisions, continuity of IT operations and the business goal of the public entity.

A.2.3 Entity Policies, procedures and processes

The auditor needs to access IT policy documents and determine whether they are approved by the IT Governance body, comply to Government regulations on security, standards, data protection, cloud services and the like and consistently facilitate achievement of entity business goals. These policies need to be supported by laying down detailed procedures and processes that would define how the work is to be accomplished and policy enforced. Areas that need well documented procedures include:

- Internal Control – that can be tracked through dashboards, management reports, logs, project updates and audit requirements
- Continuous identification, managing and review of IT risks by key stakeholders and adequate system of communication with Governance bodies to ensure stakeholder transparency

² ISO 38500.

- Access to data, handling and storage with specific provisions on handling sensitive data that has been collected to facilitate discharging of a public service. e.g.- patient records collected by a public funded health facility.
- HR practices that support IT strategy
- IS security procedures for protection of information assets

Auditor needs to check whether the policy and procedures are well communicated and understood by the stakeholders – including staff as well vendors for compliance. Further, the entity should be committing adequate resources in staff training and deploying those IT processes that bring maximum value to the public service that the entity is discharging.

A.2.4 Control structure for IT infrastructure and services

When auditing a large and complex public entity spread across geographical locations, the command and control structure for running and managing IT systems, services, virtual and physical networks, hosting applications, maintaining continuity of operations can be found to be divided into separate control centres focusing on specific tasks like managing special purpose software (viz. diagnostic tools in a Thermal power plant), network management, help desk operations, storage managements. Reporting requirements, dashboards and information periodically sent to the appropriate Governance layer by the control centre management needs to be examined and personnel interviewed to assess how the complex substructures are aligned to optimize resources within the entity.

A.2.5 People, Skills and Competencies

Going back to the example of a public entity initiating or expanding services online the single most important requirement for a public entity other than an IT strategy to realign IT infrastructure and services with the new business goals – is to identify competency gaps and taking appropriate measures to address staffing needs. Often competency gaps are underestimated, and adequate resources are not committed to manage new projects. When training plans are rolled out, the IT auditor needs to assess the adequacy of design, delivery and coverage of training programs to equip the existing workforce to use the new IT systems and reengineered business processes.

A public entity often lacks the readiness or ability to create new job roles and hire persons with required workforce plans even when skill limitations are recognised. These limitations could be beyond the control of the entity in question due to extant government regulations or dependence on separate hiring entities having other priorities. The auditor needs to appropriately weigh the circumstances in which the entity operates, examine what strategic measures the entity IT Governance bodies have taken to work around those limitations and make an assessment whether there is awareness of best approaches taken in similar entities – like engaging a vendor with appropriate technology

skills for a finite objective -and whether similar strategies could be applicable in the given scenario.

A.3 Risks associated with inadequate IT Governance

The continuous monitoring, analysis, and evaluation of metrics associated with IT governance initiatives require an independent and balanced view to facilitate improvement of IT processes. Seemingly compelling IT decisions taken by a public entity to improve services often fail to deliver the promised benefits due to inadequacies in the structure or elements of IT Governance discussed in the preceding sub Section. Auditor may find that either committed resources could not be made available in sync with the planned project path or the culture of exclusion of business heads, disengagement of head of entity from IT decision making or inadequate baseline data used by the public entity led to IT project activities occurring in a disjointed, inconsistent manner.

Audit can play a significant role in improving IT governance in a public entity by providing recommendations that mitigate risks associated with one or more elements of IT governance. The IT auditor needs to recognise the risks that result from the lack of proper IT governance – identify the key elements that are inadequate and make actionable recommendations. Common scenarios of substantiation of these risks would include :

A. Fragmented IT structures and duplication

Auditor may find that in large public entities that provide a large set of different services, the IT structure may have evolved in a manner that is highly fragmented across various Divisions and locations catering to distinct business needs. Much of the IT infrastructure and applications may have been commissioned at different periods in the past and large part of the decentralized spending is now on maintenance and continuity of operations which work in silos with little scope of sharing of information or operational infrastructure. Eg. The IT ecosystem of specific purpose software viz. vehicle registration in Transport department may have no interface with the Department's driver's license processing and renewal application. Auditor may examine how without adequate centralized authority and oversight, the entity draws assurance that investments in IT are being coordinated organization-wide, and that they provide an appropriate mix of capabilities that support mission needs while breaking silos and avoiding necessary duplication.

B. IT provides low contribution to business value

Auditor may notice a situation from internal reports, lessons learnt documentation, project status updates that major IT investments or continuation of legacy systems in a public entity adding little or no business value. Next step would be to try and identify the major conditions that resulted in such a scenario. In case of new acquisitions, interviewing IT heads at the entity may point to poor vendor delivery even when the real weakness may have been poor project

governance. Auditor needs to check the involvement of stakeholders in the IT decision making, the quality of management reporting to the Governance board on projects, adequacy of staff committed to the Project management structure, technology proposals made to Governance Board, adequacy of baseline data to identify primary causes of poor business value derived from IT.

C. Ineffective or user-unfriendly IT systems

Auditors may find that newly deployed entity-wide IT applications do not meet the complex functional requirements of the entity and result in out of scope, expensive change management requirements to address business needs that were being met better by a set of legacy systems that got replaced by the new deployment. This could happen either due to limited engagement of business process owners and users during the requirements definition, User Experience design or UAT³ stage or inadequate reporting of critical problems by the Project governance team to the IT governance body, in its haste to meet pre-approved Project milestones.

D. Ineffective IT resource management

The auditor may notice a number of individual public entities failing to move to common platforms developed for optimal use of Government IT spending although policy documents may envision such Whole of Government strategies. Individual entities may be constrained by operational requirements or lack of adequately IT-skilled human resources to be able to move into common platforms, data centers and continue to run legacy operations. These scenarios of suboptimal IT resource utilization may be common in public services – and can be addressed by appropriate stakeholder engagements, workforce planning and repurposing existing IT resources.

E. Project failures

Public IT projects often fail to deliver requisite functionality, align IT delivery with business goals, run into contractual, scope creep and change management issues that unduly extends development phases or fail to meet minimum security and architecture standards that are of ever increasing importance in a web-based service scenario in public entities. These projects may incur additional costs to maintain and administer non-standard systems and applications. Some entities reduce risk of Project failure in acquisition by undertaking extensive industry consultations, agile development methodology, taking demonstrations of prototypes, deferring upfront procurement of hardware and piloting rollouts in select locations

To assess causes of failure in IT projects or to draw assurance on well governed public IT projects in a public entity the auditor needs to access business cases and Detailed Project

³ User Acceptance Testing

Reports to understand what the project aims to deliver. The next requirement is to assess the quality of Project governance – in terms of commitment of resources, drawing up realistic milestones, estimation of technical resource requirement, engagement of business users to draw up Functional requirements and BPRs, if any. Auditor needs to assess the quality and frequency of progress tracking, identification of critical problems, their resolution proposals and what the Project governance team reports to the IT steering Committee or equivalent Governance body.

F. IT spending that is unknown, excessively high, or insufficient

These situations occur when a large public entity or multiple entities either have multiple cost centres responsible for spending on specific IT needs or maintenance – without a central Governance structure approving all IT spending or because business units within the entity not classifying IT-related costs appropriately. The IT auditor faced with such a scenario needs to assess the role played by the governance mechanism and adequacy of Management reporting to enable better visibility on IT investments. It would be important for the entity to reset its IT priorities, identify projects or legacy IT systems that aren't efficiently contributing to meeting them, and make top-management approved decisions based on the IT portfolio as a whole.

G. Exposure to cybersecurity and privacy risks, such as data loss and security breaches

The auditor needs to access policy documents, procedural requirements, user privilege matrices, access logs, log review reports, incident response reports and security architecture to draw assurance on the nature of leadership that the IT steering Committee or equivalent body provides in enforcing controls relating to cybersecurity -in an environment of increasing web based services provided by public entities. Security breaches carry the risks of misappropriation of assets, unauthorised disclosure of information, unauthorised access, disruption and information unavailability, misuse of information, noncompliance with personal data laws and regulations, and failure to recover from disasters. The auditor must examine whether the security policies, practices and training manuals clearly communicate the data protection priorities, available resources, reporting arrangements and overall tolerance of cybersecurity risks. These policies, inter alia, should include business continuity plans and procedures in the case of a disruptive cybersecurity attack.

H. Poor public Service Delivery

Auditor may find that the public entity has not made the best use of technology for its service delivery. While senior management may allude to lack of funds, this scenario is often triggered by a culture of inadequate IT planning. As a result, public services delivered by the entity fails to keep pace with citizen expectations. Auditor may examine whether the entity has periodically updated its IT strategy, considered technology options and created appropriate business cases to support IT decision making. It may also be examined if quality

of services delivered have been constrained by a lack of IT resources or the inability of the entity to repurpose 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 organisation.

I. Third party (vendor) dependency

If there are no proper policies controlling the acquisition and the outsourcing process for IT, the organization might face a situation where it depends completely on one vendor or contractor. Issues related to contract oversight are dealt with in detail in Chapter 2.

J. Non-compliance with legal and regulatory requirements

Citizens require increased assurance that public entities take implement adequate controls to ensure protection of personal data and conform to good governance⁴ practices in their operating environment. In an environment of integration between systems and data interchange e.g. Data collected through third party reporting mechanisms (eg banks, property registration Offices) by Tax Departments, stakeholders need assurance on the compliance mechanisms put in place by public entity governance bodies. In absence of suitable policies and procedures in a public entity, auditor may find that compliance to privacy, confidentiality, intellectual property and security requirements cannot be enforced.

⁴ For further reading on IT Governance and related risks see :

1. INTOSAI WGITA and IDI [Handbook on IT Audit for Supreme Audit Institutions](#) (2022 revision)
2. ISO/IEC 38503:2022 -Assessment of the Governance of IT <https://www.iso.org/obp/ui/#iso:std:iso-iec:38503:ed-1:v1:en>
3. ISACA, COBIT 2019 FRAMEWORK: *Governance and Management Objectives*, 2019
4. GAO- Federal CIOS -critical actions needed to address shortcomings, 2018
5. INTOSAI, *Governance Evaluation Techniques for Information Technology* (WGITA, 2016). <https://www.intosaicomunity.net/wgita/wp-content/uploads/2018/04/1.-Guide-on-IT-Governance-1.pdf>
6. GAO, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses*, [GAO-15-315](#) (Washington, D.C.: Mar. 31, 2015)
7. ISO/IEC 38500:2015, [Corporate Governance of Information Technology](#), Feb. 2015

Section B- Indicative Audit Program for IT Governance

Audit Focus Area: Governance Structures

Audit Objective: Assess whether there are appropriate IT Governance structures to enable the organization to deliver its IT objectives.

Audit Issue 1 – Elements of IT governance structures that evaluate, direct, and monitor the IT functions of the public entity

Criteria: IT Governance structures like that of the IT Steering Committee/ IT Strategic Committees which consists of members from the Top/Senior management are placed at a strategic level within the organization. Roles and responsibilities of such structures (Committees/Individual officials) are clearly defined including those of the Chief Information Officer, Chief Information Security Officer or equivalent.

Information Required	Analysis Method(s)
Organizational Chart	Review the overall Organizational chart to determine that the IT governance structures are positioned at a strategic level.
IT Organizational Chart	Review the IT Organizational Chart to determine if the IT governance structure is appropriately established with members from Top/Senior management.
The Steering Committee Constitutional documents/Equivalent documents	Review the documents constituting the IT governance committees to determine whether the roles and responsibilities have been clearly defined;
Minutes of Steering Committee meetings	Review the Minutes of the meetings to see, if the defined roles and responsibilities are being carried on by the structures, appropriately.
Audit Conclusion: To be filled in by auditor	

Audit Focus Area: IT Strategy

Audit Objective: Assess whether there is an IT strategy in place, which includes a strategic plan and processes to ensure alignment of the business objectives and IT objectives.

Audit Issue 2 –Alignment of IT strategy and service goals of a public entity

Criteria: An IT Strategy document is in place, which includes a strategic plan and processes, wherein the IT functions have been aligned with the business objectives. This document is reviewed and updated periodically.

Information Required	Analysis Method(s)
IT Strategy document (or equivalent) including the IT strategic plan	Review the document to determine if the IT goals are in alignment with the business goals.
Minutes of the meetings conducted by the IT Steering Committee or equivalent.	Review the minutes to determine that the business owners are sufficiently represented in the meetings. Review the documents to verify that strategic decisions are taken at the Strategic level only.
IT Budget/Project approval mechanism;	Review the IT Budget/Project approval processes to determine that IT Project approval procedures in place are unambiguous and involves all relevant stakeholders in the organization.
Business owners' requirements/proposals or equivalent.	Interview appropriate business owners to assess if their needs are met by the IT vertical.

Audit Conclusion:

To be filled in by auditor

Audit Focus Area: Policies, Procedures and Processes

Audit Objective 1: Assess whether the organization has appropriate, approved policies and procedures to guide its IT functions.

Audit Issue 3 – Are IT policies and procedures updated and current?

Criteria: The organization documents, approves and communicates appropriate IT policies and procedures to guide the IT functions.

Information Required	Analysis Method(s)
IT policies like HR policy (for hiring IT personnel), termination security, software development/acquisition, IT security policy etc., Emails/Training materials whereby Policies are communicated.	Review the policy documents to verify if they are approved, current, complete and reflect the business needs of the entity Review the internal process documents to check if the policies have been appropriately communicated to the stakeholders. Review Policy change control history to determine that they are reviewed for necessary updates and periodic alignment with entity goals and regulatory requirements
Procedures for selected IT policy Emails/Training materials whereby procedures are communicated.	Review the internal process documents to check if the procedures have been appropriately communicated to the stake holders. Interview stakeholders to determine if the procedures are duly followed. Determine if the procedures are practicable to follow.

Audit Conclusion :

To be filled in by auditor

Audit Objective 2: Assess whether the organization has appropriate mechanisms in place to ensure compliance to the IT policies and procedures.

Audit Issue 4– Compliance to IT policies and procedures

Criteria: The organization has a compliance mechanism to ensure that all policies and procedures are followed by the users.

Information Required	Analysis Method(s)
IT policies, procedures, training materials communicating such policies and procedures	Select sample policies and procedures to assess compliance. Interview the compliance personnel to determine the compliance mechanism processes and their accomplishments.
Compliance reports, returns, MIS	Review compliance reports to check the non-compliances noticed and action taken thereon. Review steering committee meeting minutes to see if high level compliance issues are discussed at strategic level. Verify action taken against non-compliance has prevented recurrence. If not, analyse the reasons for the same. Verify if the action taken was sufficient to prevent recurrence.
Audit Conclusion : To be filled in by auditor	

Audit Objective 3 : Assess whether the IT Governance has ensured Compliance with legal and regulatory requirements with appropriate mechanisms in place.

Audit Issue 5 – Compliance to Legal and regulatory requirements

Criteria: Business and IT Legal and regulatory requirements

Information Required	Analysis Method(s)
Internal regulations related to job descriptions	Review to assess whether the internal regulations related to job descriptions are compliant with legal and regulatory requirements
Internal regulations related to IT security	Review to assess whether the internal regulations related to IT security are compliant with legal and regulatory requirements
Internal regulations related to Data privacy and employee verification procedures	Review to assess whether the internal regulations related to Data privacy and employee verification procedures are compliant with legal and regulatory requirements
Policy for communications and IT operations	Review to assess whether the policy for communication and IT operations are compliant with legal and regulatory requirements
Employees contract document	Review to assess whether the employee contract document (including non-disclosure clauses) is compliant with legal and regulatory requirements.

Audit Conclusion :

To be filled in by auditor

Audit Focus Area: Control structure for IT infrastructure and services

Audit Objective: Assess if the control structure for overall governance of IT infrastructure is fragmented, carrying risk of duplication and suboptimal resource use

Audit Issue 6– Control structures and IT infrastructures/services approval channels in place

Criteria: The organization has a centralized control structure and approval channel in place to ensure strategic decisions pertaining to IT infrastructure and services are taken at appropriate levels to optimize the use of IT resources.

Information Required	Analysis Method(s)
Organisational Chart and documents defining roles and responsibilities	Review the organizational chart and documents constituting the IT governance committees to determine whether the roles and responsibilities define the decision-making powers and the delegations thereto.
IT Budget/Project approval procedures, documents	Review the IT Budget/Project approval processes to determine that strategic and high level IT Budgets/Project approvals pertaining to IT infrastructure and Services are done at appropriate levels only.
Departmental IT structure and decisions taken	Interview a sample of key personnel across Departments/ location to determine the degree of harmonization and centralized control in decision making
Accounting reports for ICT expenditure made by Departments, Branch Offices	Check accounting entries re: IT maintenance expenses in field locations to examine whether all IT spending is tracked properly and available centrally to the IT Steering Committee
Audit Conclusion : To be filled in by auditor	

Audit Focus Area: People, Skills, and Competencies

Audit Objective: Assess whether sufficiently qualified and trained IT personnel are available to deliver the IT functions.

Audit Issue 7– Management of IT related Human resource requirements

Criteria: The organization has a plan to meet its current and future IT personnel requirements.

Information Required	Analysis Method(s)
IT Strategy	Review the IT strategy document to determine if it contains a strategy for ensuring present and future IT resource requirements, and where skill gaps are identified whether the entity strategically engages third party resources
HR and Training policy for IT personnel	<p>Review the policies to determine if they are approved, current and complete.</p> <p>Review the HR policy documents to check if the skill requirements are clearly defined,</p> <p>Review the IT training policy documents to check if the IT training requirements are clearly defined.</p>
Hiring plans	Check the staff hiring plans or plans for contractually engaging vendors' skillsets to verify if the plans are in sync with the IT strategy and current requirements.
IT Training plans	Check the IT training plans to verify if the plans are in sync with the IT strategy and current training needs.
Audit Conclusion : To be filled in by auditor	

Section C - Audit cases on Risks related to IT Governance and reported Best practices

Risk area	Audited finding	Report reference
A. Fragmented IT and duplication	A1.1 – Silo working can inhibit progress: There are boundaries between civil servants as well as systems. Sharing data is difficult and may be expensive and ultimately unsuccessful unless organisations understand each other’s data needs before they start commissioning technical solutions.	A1. Challenges-in-using-data-across-government, NAO, UK 2019⁵
	<p>A1.2 - A lack of standards across government has led to inconsistent ways of recording the same data. Audit found more than 20 ways of identifying individuals and businesses across 10 departments and agencies, with no standard format for recording data such as name, address and date of birth. This makes it difficult for government to maximise its data asset, for example by allowing thematic analysis across different sectors to help understand economic challenges or systemic problems.</p> <p>Audit has recommended that the government needs to Identify datasets that are critical to government functions, look at how to share them easily and examine how they can be enhanced by process improvement and automation. A new Data Strategy for the Government as a whole would be a good opportunity to include a clearly articulated plan of work to overcome barriers to effective use of data.</p>	
Risk area	Audited finding	Report reference
B. Low contribution to Business value	B1.1 Audit found that Although the Human Resources Information Technology (HRIT) investment was initiated about 12 years ago with the intent to consolidate, integrate, and modernize the department's human resources IT infrastructure, the Department of Homeland Security (DHS) has made very limited progress in achieving these goals. HRIT's minimally involved executive steering committee during a time	B1. Report on HR IT in Homeland Security, GAO US 2016⁶

⁵ <https://www.nao.org.uk/report/challenges-in-using-data-across-government/>

⁶ <https://www.gao.gov/products/gao-16-253>

	<p>when significant problems were occurring was a key factor in the lack of progress. DHS will be limited in efficiently tracking and reporting accurate, comprehensive performance and learning management data across the organization, and could risk further implementation delays.</p> <p>Audit recommended that the HRIT executive steering committee is consistently involved in overseeing and advising the investment</p>	
Risk area	Audited finding	Report reference
C. Ineffective or user-unfriendly system	<p>C1.1 – The newly introduced Service tax application (GST) rolled out by the Department was grossly inadequate to meet the intended objectives of a completely electronically driven System for administration of GST.</p> <p>The tax department did not enter into a formal agreement with the vendor that defined milestones for the project- and out of the few modules that were rolled out, many functionalities were incomplete. These resulted in ineffective tax administration and only 34 percent of the registered dealers under the previous tax regime (VAT) migrating to the new one.</p> <p>C1.2 - system was not user friendly to assist the taxation officials in ‘getting access to the taxpayer’s data’ with ease for carrying out the necessary functions of issuing notices etc. The database was not being updated in real time and the time lag made it unfriendly to the dealers as well as to the Department.</p> <p>Audit recommended that the entity undertake a comprehensive review of the backend application to overcome the systemic glitches and revamp the IT infrastructure of the tax Department to enable a successful IT driven tax administration.</p>	C1. Roll out of GST in Meghalaya state- SAI India 2020.⁷

⁷ <https://cag.gov.in/ag/meghalaya/en/audit-report/details/113861>

Risk area	Audited finding	Report reference
D. Ineffective IT resource management	D1.1 Since there is no single ICT development planning document in the ministries, which would define the directions, priorities and ICT tasks the overall goal of the ICT optimisation plan remains a challenge.	D1. Has Public Administration Used All Opportunities for Efficient Management of ICT Infrastructure? SAI Latvia 2019 ⁸
	<p>D1.2 In order to solve the problems of ICT resource management, the National ICT Architecture was developed in 2015. Audit found that regulations did not compel public institutions to use the common infrastructure of the national electronic communications service centre, which may stay unused after being set up with several million euros.</p> <p>Audit found that audited institutions do not assess alternative solutions for the provision of ICT services. It was noted that many institutions continued developing their own solutions in absence of a clear regulatory requirement to use a designated national IS integrator .</p> <p>Audit recommended that in order to ensure the application of the ICT management principles set out in regulatory enactments and policy planning documents in public institutions, the Ministry shall develop methodology and train ICT managers of public institutions to assess current situation in ICT provision and spending, identify opportunities for optimisation, and calculate financial gains from investments needed towards ICT optimisation.</p>	
Risk area	Audited finding	Report reference
E. Project failures	E1.1 Audit found that due to poor oversight by Public Services and Procurement Canada (PSPC), the Phoenix Pay System was implemented without critical pay processing functions; without having been fully tested; with significant security weaknesses that did not protect public servants' private information;	E1. Building and Implementing the Phoenix Pay System – OAG Canada , 2018⁹

⁸ <https://www.eurosa.org/en/databases/audits/Has-Public-Administration-Used-All-Opportunities-for-Efficient-Management-of-ICT-Infrastructure-00003/>

⁹ https://www.oag-bvg.gc.ca/internet/English/parl_oag_201805_01_e_43033.html

	without long term software support and without an adequate contingency plan in case of implementation failure	
	E1.2 PSPC did not fully consult and involve other departments and agencies to define user requirements for the development of Phoenix. Phoenix executives even cancelled piloting with one department before government-wide roll out.	
	E1.3 When faced with possible higher costs, the Department knowingly removed or deferred important system functions that could have ensured accurate processing and personal data protection. The Department chose not to report back to the Treasury Board the negative impact of such decisions on projected benefits or ask for more money to address the critical functions so that the project could be delivered as planned .	
	Audit recommended that for all government-wide IT projects, there should be mandatory independent reviews of the project's key decisions to proceed or not.	
Risk area	Audited finding	Report reference
F. Exposure to cybersecurity and privacy risks, such as data loss and security breaches	F1.1 Audit assessed that the audited regions are not protecting the access to IT systems and health data in a satisfactory manner. There are gaps in the regions' basic security measures against cyber-attacks – in terms of outdated OS used in two regions and almost all the approximately 27,000 staff employed by the other region having local administrator privileges.	F1. protection of IT systems and health data in three Danish regions. SAI Denmark 2017 ¹⁰
	F1.2 Audit noted that failure to log online activity or review where they exist - makes it difficult or impossible for the regions to detect and track cyber-attacks and abuse of user privileges.	
	F1.3 Audit found that the management of IT security to protect health data in South Denmark lack clear direction, and that an effective IT-security policy must be embedded in top management .	

¹⁰ <https://www.eurosai.org/en/databases/audits/Report-on-the-protection-of-IT-systems-and-health-data-in-three-Danish-regions/>

	Audit recommended that regions should put in place basic IT security measures in combination with management and control of user privileges to reduce the risk of compromising the regions' IT systems and data considerably.	
Risk area	Audited finding	Report reference
G. IT spending that is unknown, excessively high, or insufficient to meet organizational goals	G1.1 GAO reviewed Office of Management and Budget and 26 agencies, covering years 2010 through 2017. It reported that Federal legacy IT investments are becoming increasingly obsolete: many use outdated software languages and hardware parts that are unsupported. Agencies reported using several systems that have components that are, in some cases, at least 50 years old. For example, Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation's nuclear forces. The Audit reported that although OMB has initiated a plan to modernize, retire, and replace legacy IT systems, the government runs the risk of maintaining systems that have outlived their effectiveness till a policy is finalized and executed.	G1- Legacy IT Risks, US GAO, 2016¹¹
	G1.2 Audit identified examples of legacy systems across the federal government that agencies report are 30 years or older and use obsolete software or hardware and identifies those that do not have specific plans with time frames to modernize or replace these investments. Audit recommended the entity to develop a goal for spending measure and finalize guidance to identify and prioritize legacy IT needing to be modernized or replaced.	
	G2.1 In this follow up Audit, GAO reported that out of 10 critical Fed IT legacy systems only seven had documented plans for modernization. Among the latter, only two plans included all elements of best practices covering milestones, workplans and plans for disposing the legacy systems.	G2-Modernization Plans for Critical Legacy Systems -GAO 2021¹²

¹¹ <https://www.gao.gov/products/gao-16-696t>

¹² <https://www.gao.gov/products/gao-21-524t>

Best Practice Issue	Audit Observation	Report reference
1.Stakeholder engagement in complex IT procurement	<p>1a.1 The Audited entity subdivided megaprojects into smaller ones where possible and made good progress on consulting early and often with end users and private sector suppliers to gather their input on IT solutions. The entity adopted a number of agile procurement practices. In particular, procuring organizations started with pilot projects, had live demonstrations and more testing to evaluate potential solutions, and added more flexibility with shorter contracts and multiple qualified suppliers.</p>	<p>1a. Procuring Complex Information Technology Solutions-OAG Canada 2021¹³</p>
	<p>1a.2 The procurement team also designed the contract to commit less time and funding upfront and to keep 3 qualified suppliers engaged after choosing a preferred supplier. Audit noted that subdividing large IT initiatives into smaller projects, where possible, can reduce the risk of failure by incorporating early learning, while keeping multiple suppliers engaged can make it easier to rely on a back-up provider if the selected one fails to deliver.</p>	
	<p>1a.3 Procurement teams also engaged private sector suppliers early in the procurement process in an effort to create clearer solicitation documents. They invited suppliers to industry days, assessed their qualifications, and held one-on-one meetings and group sessions with them. The teams also adopted innovative techniques for evaluating proposals, such as requiring live demonstrations and testing products early in the evaluation process to make sure that the proposed product could perform key functions to meet business needs.</p>	
	<p>1a.4 Audit interviewed suppliers for their perspectives on how the federal organizations used agile procurement practices. They were told that agile procurement was far more interactive and transparent, which was beneficial for meeting business outcomes.</p>	

¹³ https://www.oag-bvg.gc.ca/internet/English/parl_oag_202102_01_e_43747.html

2. Project for Centralisation of Support Services	2a.1 Audit concluded that centralisation of support services of state authorities has generally been successful, quality of accounting improved, and became more effective.	2a. Centralisation of Support Services of State Authorities SAI Estonia 2018 ¹⁴
	2a.2 Transitioning to a common information system was the main lever that enabled making financial, personnel and wage accounting more effective and reduction of staffing requirements.	
	<p>2a.3 Implementation of a web-based reporting environment (SAP BO) has created opportunities for obtaining information necessary for management. This enables easy access to financial and personnel data regarding the area of government, and availability of information can be made simpler as a result of improving the skills of users.</p> <p>-Audit recommended that Minister of Public Administration should in cooperation with local governments analyse and assess whether a similar model could also be implemented to improve the quality of financial, personnel and salary accounting of local governments and making it more effective.</p>	

¹⁴ <https://www.eurosai.org/en/databases/audits/Centralisation-of-support-services-of-state-authorities/>

Chapter 2: Audit of IT Contract management

Section A- Risks associated with IT Outsourcing and Cloudsourcing

A.1 Introduction

Around the globe, contracting IT services from vendors as well as Cloud Service Providers (CSPs) is increasingly an opportunity to add value, tap into a resource base and/or mitigate risk. Outsourcing is the process of contracting out one or more elements of operations to a supplier of services outside of the organisation's management structure. Access to skilled personnel, advanced technology infrastructures, flexibility, rapid scaling and cost savings are the driving forces behind contracting IT services. A contract is entered into at an agreed fixed or 'pay per use' pricing model or a combination with a third-party provider or CSP to provide the service.

The benefits of IT contracting are accompanied by the need to manage the complexities, risk, and challenges that come with it. Auditors, therefore, can help organizations with a comprehensive review of its IT contracting operations, identify risks, provide recommendations to better manage the risks, and also evaluate the outsourcing activity's compliance with applicable laws and regulations. The auditor's engagement can be relevant right from the pre-transition stage to the entire lifespan of the IT contract agreement. Taxpayers need assurance that public entities carry out proper feasibility studies before contracting, select vendors in a transparent manner, transition internal operations smoothly, take care to protect citizens' personal data, and do not lose strategic control over core services, intellectual property and information assets. It is therefore important that the audit of an IT contract in a public entity is taken up in a timely manner to help avoid contract failure.

A.2 Key Areas of IT contracts

To start with the Auditor needs to know the nature of service for which a public entity has contracted a CSP or an IT vendor. This could include one or many elements of following operations:

- Application development and maintenance
- Data centre management
- Network and IT infrastructure management
- Security management
- Helpdesk services
- Website hosting
- IT project management support, GRC and other consulting services

A.2.1 Application management:

A.2.1.1 Application Development:

Application management can be in the form of application development, software maintenance, and production support. Where core functions of a public entity is taken to a digital platform, custom-built application development is common. The auditor needs to examine the documents generated as a part of the functional and technical requirements generation process. The work statement as part of terms of contract should be defined clearly from the beginning, as well as the final stages of the development phase for which the service provider is responsible. In case the entity chooses a cloud native application development process the delivery risks, access rights, acceptable downtime etc need to be factored in. The entity and vendor need to agree on milestones, timelines, deliverables and

process of user acceptance. Code review¹⁵, test plans and results need to be designed and documented at each stage of the development process. A public entity may also acquire an application as a Commercial -of-the Shelf (COTS) product with minimal customisation or access a 'Software-as a-Service' offering from a Cloud Service provider to meet a specific core or support business process

Especially in case of a bespoke development, the auditor must ensure that access control and segregation is maintained during development and testing, and that the entity's project management team is actively involved in the review process. Where the scope of application development includes integration of external applications e.g. A new tax application needs to fetch data from vehicle registration system of another entity – the auditor needs to ensure that the test result reviews validate the integration's completeness and accuracy, and back out procedures and conditions are defined adequately. Besides, in many countries it is mandatory to have third party security certifications for roll out and running of e-governance IT applications. For audit engagements in these countries, the auditor needs to check the scope, periodicity, results of and action taken on the security audit reports.

A.2.1.2 Application maintenance and Production support:

In case of post roll-out application maintenance or production support, the auditor needs to draw assurance that the entity has defined the Service expectations adequately in terms of expected Turnaround time (TAT) with response and resolution parameters for each class of service. The auditor needs to ensure there is adequate tracking and monitoring of SLA compliance by the entity, examine the efficiency of the monitoring process and verify that the system's performance is measured.

A.2.2 Managed Services:

Many public entities have been contracting out support IT functions like infrastructure, data centre and security services management. While traditionally managed services were limited to on-premises or co-located data centres for physical set-up and security, some public entities are now making a paradigm shift by choosing Cloud¹⁶ based deployment and management of IT applications.

A.2.2.1 Management of IT infrastructure on premises

Public entities contract services of a vendor for managing performance and maintaining infrastructure on premises, troubleshooting errors, maintaining databases, providing backing up and restoration services, performing downtime analyses and the like. For on premise services, the auditor should examine whether all service requests to the vendor are being formally communicated and Turnaround times are clearly agreed upon.

A.2.2.2 Data Centre Management

In many countries, public IT systems are mandated to be hosted and run from designated Data Centre facilities where all support services of Hardware, software and OS planning, procurement, installation, configuration and maintenance, server capacity management and load balancing, are run by the state designated facility. In case the auditor finds that the entity owned compute, storage and networking assets are placed and managed by a third party at a privately owned facility (Co-

¹⁵ Code reviews- plans and systems for code review for debugging etc differ as per the Software Development methodology. In the traditional 'waterfall' methodology, these were done by peers and specialists of the development team while in agile development, code reviews are embedded into agile sprints and iterations.

¹⁶ For a brief on Cloud service models see WGITA IDI IT Audit Handbook (2022 version)

located with other customers) the auditor needs to determine whether the vendor has adequate capacity (infrastructure, financial, and technical) to host outsourced services, whether physical segregation of entity systems and data is ensured and the service provider has adequate back up capacity to ensure the organisation's infrastructure and network availability.

A.2.2.3 Management of Cloud-based deployment

Advantages of a cloud-based deployment of an IT application are well-known. It offers scalability in the solutioning and provides flexibility in payment terms (converting CapEx to OpEx). However, in case of cloud deployment, the controls of the public entity over the underlying infrastructure and technical aspects are limited.

Depending on the mode of cloud-deployment, the nature of services being availed also varies. For example, in case of 'Infrastructure as a Service' and 'Platform as a Service' deployments, the public entity no more owns the major computing, storage and network assets but continues to control the application, OS and data assets. Provisioning of compute and storage capacity, and their continuous monitoring becomes part of the CSP's responsibility. Similarly, in 'Software as a Service', some of the application components (e.g., Identity and Access Management, SMS and Email Services) are offered off-the-shelf. Many of these software services are owned by third parties (other than the Cloud Service Provider). The engagement between the public entity and the third parties are governed largely by the CSP's terms.

Thus, Cloud-based deployment brings in some inherent Governance and Security issues. Therefore, in Cloud based deployment, the auditor must ensure that the contract terms clearly define the shared responsibilities of the CSP and the public entity, physical locations of hosting production and back up environments, logical segregation of virtual computing environment, standard security configurations of the CSP meet the minimum security requirements of entity information assets, and CSP's responsibilities for return and removal of client information assets in case of termination.

Further, the agreement should clearly state that the cloud service provider would provide the information and technical support that are necessary to meet the public entity's requirements. When the information security controls provided by the cloud service provider are pre-set and cannot be changed by the cloud service customer, the cloud service customer may need to implement additional controls of its own to mitigate risks.

A.2.2.4 Composite contracts

While undertaking IT projects with largescale implementations a public entity often finds it beneficial to choose composite contracts with a single vendor that contracting separately for each component in order to minimise risks of coordination between delivery of component services. Eg. The Data centre may not be functional while the application is developed, or, infrastructure is procured upfront but the application is not even ready for the first stage of 'Go Live'. Such composite contracts may include Application development as well as infrastructure management and Data Centre services.

A.2.3 Managed Security Services

Depending on the nature of business and scale of IT operations, a public entity may contract a vendor for overseeing IT security over its entire IT infrastructure, data assets, and user management activities. The scope of security services may range from end to end security architecture design and support (design, implementation and technical support for a large and complex entity) to specific security functions on particular systems (e.g., firewall monitoring, content filtering, virus protection, intrusion

detection and response, and network vulnerability assessments). The Auditor needs to assess the exercise undertaken by the entity to assess its overall security requirements and how frequently it is done. It may be checked whether access privileges granted to Service monitoring team and the team's skillsets are commensurate to the services rendered. Moreover, the auditor needs to peruse MSS monitoring reports – viz. vulnerability assessments, intrusion detection logs, proposed mitigation procedures and review what timely action is taken by the entity management to ensure the security, confidentiality, and availability of data assets and systems.

When a public entity contracts the use of CSPs, additional security controls that need to be enforced include non-disclosure of sensitive data, clarity on what constitutes a breach of security and how the CSP will notify the entity of a breach, use of compatible cryptographic controls tested on data in transit and at rest, right to access incident logs, audit trails and security testing reports, and appropriate identity and access management.

A.2.4 Helpdesk Services

Any of the maintenance services, such as troubleshooting problems, production support, and infrastructure management, can be categorized as a help desk service. Under this arrangement, the service provider's personnel support the organisation through various IT problems either onsite (i.e., at the organisation's premises) or offsite (i.e., from the service provider's premises). TATs (i.e., responses and resolutions) are then defined for each level of service.

Auditor needs to examine what procedures are in place to evaluate the Help Desk Services and whether the entity uses performance results in terms of response and resolution for service tickets generated as one of the core criteria for ongoing vendor evaluation. Audit should also determine whether periodic status reports were submitted to the organisation and issues and improvement action items were documented.

A.3 Lifecycle of an IT Contract – Audit considerations

Outsourcing and cloud governance is at the heart of the IT contracting model. Within the outsourcing life cycle, governance involves the development of processes which bring together the appropriate level of management from both the organisation and the service provider(s) to create a formal and transparent working relationship on an ongoing basis. This is arguably an area that organizations underestimate most frequently in terms of time and investment and the structural architecture necessary to manage accountability. The auditor needs to have good knowledge of the control concerns along the entire lifecycle of an IT services contract that a public entity engages in.

A.3.1 Feasibility Assessment

The feasibility phase deals with the formalization of the IT outsourcing strategy. During this phase, a public entity should assess the outsourcing options, and identify the services and locations from where they can be operated. It is important for the auditor to examine whether the entity properly evaluated all financial, operational, and legal considerations before embarking on the IT outsourcing partnership, and whether the assumptions made in the business case documents were validated by baseline data.

A.3.2 Vendor Selection

Vendor selection begins with a formal project management structure on behalf of the entity, that has the authority to lay down a detailed scope of work in terms of application, infrastructure, and type of service that is expected to be outsourced.

A.3.2.1 Request For Proposal

The auditor needs to ascertain whether the scope of work is documented formally in terms of a Request For Proposal that, inter alia, includes the functional and technical requirements, a milestone-based plan, contractual obligations of contracting parties, planned contract duration, requisite skillsets, templates for proposals, draft legal terms of service, and indicative payment terms and schedule. Auditor needs to examine whether a robust and transparent selection criteria has been put in place. To facilitate such a criteria setting, the RFP document should spell out a list of parameters and weighting to be considered for vendor selection that reflects the entity's outsourcing requirements and business criticality of the services proposed to be contracted. Parameter considerations could include the use of global delivery centres, and minimum level of IT outsourcing experience in specific kinds of environments. The attributes may include referrals, market knowledge, competitor insight, and consultant recommendations.

A.3.2.2 Assessment of Bids

The auditor needs to examine the bid evaluation process not only in terms of its transparency but also for objectivity of technical criteria. E.g. The vendor qualification criteria spelt out in the RFP should consider details such as the vendor's size, stability, experience, location, infrastructure, level of process quality, and skill sets. Further, an exhaustive list of vendor information requirements with values attached to each parameter that can be used during the final selection round. Such information requirements on the part of the bidders facilitate selection of vendors for IT contracts in terms of a Quality cum Cost Based Selection (QCBS) method. Commonly used technical parameters include vendor's background and statement of experience, use of operation and risk management frameworks and relevant certifications, compliance with intellectual property rights; Project-specific approach and methodology, including allocation of resources, and organisation references including information on transitioning success.

A.3.3 Legal and contractual obligations

IT contracting arrangements involve a range of legal and contractual issues. Unless the scope of work spelt out by the public entity is supported by a well-written contract, management and operational activities may not be properly incentivised/ penalised. The auditor may examine whether Service levels and incentives – outlined in terms of minimum performance benchmarks and metrics (relating to service quality, system availability, and response times) are part of the contract agreement. Appropriate terms covering Data protection, privacy, and intellectual property need to be included

Contracts should cover pricing issues such as changes in service scope, agreed pricing parameters, and procedures to accelerate the resolution of pricing disagreements. In situations where the vendor hires a third party (i.e., a sub-service provider) to deliver services, the entity needs to include in the contract how service quality will be managed, and any entity performance risks. Further, rules and procedures should define and create ownership rights when new value is created from an outsourcing activity. Dispute resolution mechanisms, right to audit and conditions for termination should be clearly set. A good practice in some countries is to establish a standard template of contractual requirements that

public entities need to follow when contracting IT services. In an audit engagement involving vendor selection in IT contracting the auditor should identify whether a checklist exists that consists of the legal and contractual factors agreed on by the public entity and service provider that help to determine the vendor's compliance with each of these factors.

A.3.4 Vendor Management

When the audit engagement commences after the IT contract is already in operation, the key areas of audit consideration are the effectiveness of transition management, Change management and service level monitoring by the entity.

A.3.4.1 Transition management

Transitioning or migration involves the transfer and custodianship of information assets to the vendor. Although transition plans are the responsibility of the organisation, they usually are delegated to vendors. Migration activities typically involve two stages - planning and knowledge transfer. The auditor needs to examine whether the entity developed a formal migration strategy, including the costs and timelines for each significant milestone in the migration plan. As part of the transition strategy, the entity and service provider should agree on the migration mode viz. a complete transfer or all activities or a gradual rollout of functions based on a prioritization scheme. The auditor must verify if the strategy assigned specific resources and budgets for each step of the migration phase.

Auditor may also assess whether the knowledge transfer plan requires the organisation and service provider to identify and document all the necessary information (e.g., technical, business, process, and background information) so that the transfer process has the least impact possible on the service quality of the outsourced activity. The plan elements should cover security, business continuity planning, disaster recovery, connectivity adaptations, and data protection activities needed during transition along with responsibilities of contracting parties. Additionally, the auditor may identify if attrition affected the transfer phase in terms of operation, and how effectively the entity project management team controlled the communication and review process with the vendor.

A.3.4.2 Change Management

Application maintenance addresses ongoing change management activities and the implementation of new software releases. Auditor needs to assess whether the entity has implemented appropriate change controls that involve authorizations of change requests, reviews, approvals, timelines, documentation, and testing, as well as assessments of changes on other IT components and implementation protocols. Best practices in change management require an evaluation of changes on other IT processes like security incidents and service availability. Auditors need to verify whether a proper change control process exists to ensure that only approved changes are carried out by the service provider.

A.3.4.3 Service Level Monitoring

One of the most critical IT contract management elements is the definition of service-level targets, that need to be achieved by the vendor. Auditor must examine the SLA and the compliance controls implemented by the entity. The SLA should describe:

- The service's objectives and scope.
- Performance metrics and corresponding service levels against each metric, including:
 - Volume (i.e., the number of maintenance requests per month and lines of code).

- Availability (i.e., availability of provided services for a specific period of time).
- Quality (i.e., the number of production failures per month, deliverables rejected).
- Responsiveness (time needed for an enhancement or to resolve production problems).
- Efficiency (i.e., the number of programs supported per person, rework rates).
- Frequency definitions to measure performance (e.g., monthly, quarterly, etc.) and other informal contract performance reviews through regular progress meetings and reports.
- Payments based on SLA performance.
- Definition of clauses that stipulate the availability of the contract's renegotiation for non-achievement of SLAs.

The organisation should install a process that allows monitoring of results and performance in order to draw conclusions. Auditor must evaluate whether the key areas defined in the SLA are aligned with the benefits identified in the business case, periodic pre-defined assessment reports from the service provider are based on the key areas in the SLA, whether there exists a process of independent validation of assessment reports, formal review meetings are recorded, adequate actions are taken on reported deviations and any changes in terms of SLA are approved appropriately.

A.4 Risks of IT contracting

Public entities getting into contracting of IT services need to adopt appropriate risk mitigating strategy to reputational damage and handle impediments to the effective use of third parties and CSPs in the delivery of entity business.

The following key risks need to be considered within the IT contracting life cycle in order to devise the appropriate measures:

A. *Information security and data privacy risks*

When contracting with any service entity, it completely or partially exposes its business assets to an outsider. That is why it is important to pay attention to privacy, intellectual property, and data protection. Proper security requirements can be set out on the basis of a rigorous risk -assessment exercise undertaken by the public entity when IT operations are outsourced.

In case cloud computing services are contracted, there are added security concerns depending on the CSP service and deployment model chosen. the additional security risks include :

- I. A greater dependency on third parties, which can lead to increased risk due to
 - vulnerabilities in external interfaces,
 - aggregated data centres, (shared infrastructure)
 - reliance on independent assurance processes, and
 - organisations no longer owning the data or overseeing the controls used by third parties; often security controls of a CSP are pre-set and the public entity cannot change them as per its requirements.
- II. The increased complexity of compliance with laws and regulations, with effects on
 - a greater magnitude of privacy risk,
 - the trans-border flow of personally identifiable information, and
 - contractual compliance;

- III. A reliance on the internet as the primary conduit to the enterprise's data, which introduces
 - security issues associated with a public environment and
 - internet connectivity and availability issues;
- IV. The dynamic nature of cloud computing, including the possibility that
 - the location of processing facilities may change according to load balancing,
 - processing facilities may be located across international boundaries or high seismic risk zones
 - operating facilities may be shared with competitors, and
 - legal issues (liability, ownership, etc.) relating to differing laws in hosting countries may put data at risk;
- V. Cloud governance risks such as
 - a loss of IT governance and control by the organisation when using cloud services,
 - less reactivity of the client's command compared to the internal provision of the service, and
 - a lack of internal support due to organisational culture and the customer perception of greater risks associated with cloud services; and
- VI. Audit-related risks such as
 - the inability to access system and security logs from third parties,
 - the loss or incomplete provision of information from the provider to the customer relating to security incidents and the provision of audit trails, and
 - the absence of log data isolation among different clients or other log data leaks.

B. Inaccurate assumptions and incorrect scoping of work

Cost savings and competitive advantage projected in outsourcing proposals are based on assumptions and scope of work. If outsourcing contracts inappropriately or incorrectly detail work specifications, contract duration or payment terms - vendors may be tempted to behave opportunistically. This has become a major obstacle for IT organisations that are surprised that the price was not "fixed" (e.g., for cloud computing resources) or that the vendor expects to be paid for incremental scope changes. Additionally, organisations often create overly optimistic or unrealistic business cases that can cause significant scope creep throughout integration of outsourced services.

C. Lack of entity personnel prepared to manage Contracts

Organizations tend to underestimate the set of outsourcing governance processes and the staff required to manage the demand and integration as well as monitoring and steering of the provider. This often results in an overly optimistic or unrealistic business case. The organisation must prepare and maintain qualified personnel able to carry out the correct management of outsourcing contracts. If it does not have enough qualified personnel, during the entire contract execution, the audited organisation may make overpayments to the vendor or not obtain the expected results or outsourcing fail completely. In addition, it is in organisations best interest to create a competitive environment for contracts in which suppliers are constantly being evaluated and maximised. Following areas need to be focused upon:

- I. Poor visibility of individual contract performance, lack of contract management skills, service levels/key performance indicators (KPIs) poorly defined and not measured or monitored. This

results in the inability to effectively manage and monitor service quality, price and delivery in line with outsourcing objectives. Lack of 'right to audit' clause in contracts or 'right to audit' not exercised so no evaluation and monitoring of the third-party provider can take place.

- II. Choosing outsourced IT services means the entity does not get much, if any, insight into the team members of the vendor. Therefore, it's important to verify the knowledge and experience of the outsourced IT firm as a whole. Look for case studies, call references, etc.

D. Retaining Business knowledge and strategic control

A core business process that was previously executed by the in-house team when outsourced to external agencies may leave a public entity with little to no control over it. When mismanaged by the service provider, it can affect the quality of the public service. e.g. A state transport agency contracting out the service scheduling platform to an IT vendor may face severe service disruptions if the platform fails to deliver suitably or vendor is unable to control high turnover of personnel. If this scenario takes place years into the contract, resumption of quality services may take a long time as entity IT team would have been repurposed. It is important for the entity to understand strategic importance of select services and contract arrangements around knowledge management and intellectual property.

E. Vendor Failure to Deliver

If the outsourcing process is not implemented correctly, there is a high likelihood that the system or services being acquired may not meet user needs in terms of functionality or timeliness. There is a good possibility that the outsourcing provider may not be familiar with the know-how of business processes like in-house employees do. Misunderstanding the business requirements, and absence of an appropriate engagement between organisation and vendor may lead to designing of faulty product and may require significant re-work. A poor contract, flawed system of vendor selection, unclear milestones, and unfavourable market conditions are some of the common reasons for vendor failure.

F. External Risks

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

G. Vendor Lock in

Vendor lock is an issue that occurs in outsourcing when finding a new vendor or moving operations in-house becomes too expensive. Vendor lock-in is usually the result of proprietary technologies by the service provider that are incompatible with those of competitors. This can be especially troublesome in a cloud environment, where moving data to a different type of environment may require reformatting the data. In addition, organisations may become dependent on the software they are using with a specific cloud provider and will not easily be able to change vendors. Organisations

can reduce the risk of vendor lock by choosing cloud services or OEM components wisely, ensuring that the data can be easily transferred, and using different cloud services across multiple providers. To minimise this risk, Contract RFPs may include conditions that each OEM component should follow open¹⁷ standards. The auditor needs to verify that the RFP conditions did not promote exclusivity in selection of application components.

The consequences of poor contract management¹⁸ are service failure or delay, additional costs that may not represent value for money to the taxpayer, and reputational damage for the public entity. The auditor must aim to add value by drawing an assurance on the quality and effectiveness of the contract management controls. The auditor needs to understand how the risks are jointly shared between the public entity and the service providers, what are the various security and compliance standards and to what extent (s)he can rely on the work of independent service auditors and specialists, ensure that the level of audit coverage is commensurate with the scale, nature and number of contracts. It is important not to rely on a purely systems-based approach, but to complement this with an element of substantive testing to test the consequences of any control failure. Where there are several layers of assurance on a large-scale project with many contractors with complex interfaces it is important to ensure that assurance is coordinated properly so that audit does not hamper the progress of the project. However, the auditors need to communicate the IT contract audit findings in a way that is understood and taken seriously by the organization.

¹⁷ open standard software is defined as software that follows the guidelines laid down to keep technologies “open”. These guidelines allow free sharing of all data types with perfect fidelity. Open standards help avoid vendor lock-in and thereby, enhance interoperability. See Chapter on IT sustainability.

¹⁸ For further reading on IT Contracts and cloud service models see

1. WGITA IT Audit Handbook (2022 revision)
2. NIST publication on Cloud computing security risks, <https://www.nist.gov/publications/cloud-computing-security-foundations-and-challenges-chapter-14-cloud-computing-security>

Section B – Indicative Audit Program on IT Contract management (CSPs and other vendors)

IT Outsourcing and Cloud Governance

Audit Objective: To assess whether the entity leadership sets the direction and effectively monitors the adoption and use of cloud computing/ IT outsourcing in the organisation

Audit Issue 1 – Key elements of outsourcing and cloud governance

Does the entity have a clearly defined strategy/policy for cloud/outsourcing?

Does it promote an effective working relationship between the public entity and IT service vendors?

Was a robust cost benefit analysis made as a part of feasibility assessment?

Criteria:

- ICT strategy of the public entity
- Government regulations on use of IT vendors and CSPs,

Information Required	Analysis Method(s)
Entity ICT strategy	Verify whether the approved ICT strategy identifies IT needs and processes that can be contracted out or taken to CSPs
Government guidelines on IT contracting /CSPs	Review the entity's cloudsourcing strategy and procedures laid down to ensure they are in compliance with government's cloud regulations ?
Risk assessment documentation for outsourcing/ cloud initiatives	Examine whether the financial risks (complex supplier relationships in cloudsourcing models), operational risks (of data leakage or service disruption) are properly understood and documented
List of IT services identified for contracting	Examine the nature of senior management approval.
Business case for Cloud computing/ IT outsourcing	Verify adequacy of business case (including accuracy of cost estimates and assumptions used) in support of the entity business and IT strategy

Financial approval process	Interview key relevant management personnel to examine whether the move from a Capex to an Opex model of financing (in case of Cloud services) have been understood and adequately discussed and provided for by the entity leadership
Project Governance structure	Review the Project management set up, reporting relationships, meeting schedules with contract partners, escalation matrices, dispute resolution procedure to determine whether roles and responsibilities of contracting parties are clear -to facilitate an effective working relationship
Key Performance Indicators for IT contract management including cloud contracts	Review the formal process of development of suitable KPIs. Obtain evidence of cloud initiatives being monitored by top management (e.g. key performance indicators, regular risk and benefits assessment, etc.)
Audit Conclusion : To be filled in by auditor	

Value assessment – Costs & benefits in contracting Cloud services/IT vendors

Audit Objective : To ensure the adequacy of the cost-benefit analysis made in the Business case document in terms of actual baseline data and considering intangibles like data access and hosting locations

Audit issue 2 – Elements of the Cost Benefit Assessment

Have all the Data elements on users, peak loads, O&M Costs, Development and Testing set ups, Resource engagement requirements been captured correctly?

Does engagement of CSPs/ IT Vendors bring in specific additional responsibilities to the entity and have them been adequately factored into costing?

Criteria:

- Industry benchmark data on CSP engagement costs for the service and deployment model
- Model Business case templates published by Government, if available

Information required	Analysis Method(s)
Initial Cost Benefit analysis and CSP offerings	Document review to assess that all costs have been identified by the organisation, reviewed and approved by relevant stakeholders – and are supported by work specifications in reasonable detail Review to assess whether the risks of hosting information assets at

	<p>overseas locations have been considered, and whether data residency clauses could be enforced</p> <p>examine how the entity has spread out costs of infrastructure and other services over the Lifecycle of the engagement/ cloud adoption and check that no hidden costs including future costs have been missed</p>
Weightage on financial terms in proposed bid process	Review terms of weightage in the bid process (in case of proposed QCBS bid model) and justification for such weighting
Instances of Cost escalation clauses/ additional costs invoked by the CSP/vendor	Review of specific activity/ change management function for which change in cost is sought through monitoring reports and assess the need for such change.
Entity response to such requests	Review of action taken by public entity on additional costs/ escalation of costs levied by service provider.
Audit Conclusion: To be filled by Auditor	

Vendor selection – Contract and regulatory issues

Audit Objective: To ensure that the entity has appropriately documented its requirements and examined proposals from prospective vendors in a fair and objective manner to safeguard its interests, and in compliance with government regulations

Audit Issue 3 – Elements of the Solicitation exercise

Did the project involve business process owners to frame the Functional Requirement specifications (FRS)?
Did the entity adopt adequate tech criteria for identification and selection of vendor?
Has the RFP included suitable technical requirements that minimize risk of vendor lock-in?

Criteria :

- Entity policy on IT Outsourcing/ Cloud sourcing
- Government approved templates for RFP for IT Outsourcing/ Engagement of Cloud services
- List of Government approved IT vendors and Cloud service Providers
- Bid document templates cleared by entity's legal function
- Technical criteria listed in model IT Contract agreements issued by Government

Information Required	Analysis Method(s)
Request for Proposal or equivalent Bid Document	<p>Review technical, financial, eligibility criteria and weighting to ensure that the selection process establishes adequate competition, requirements are clearly stated; evaluation parameters represent business criticality and impact of the contract.</p> <p>Examine compliance with government requirements on open standards, security testing, data privacy, territorial data hosting requirements, as applicable</p> <p>Ensure that Service levels and incentives – outlined in terms of minimum performance benchmarks and metrics are part of the draft contract agreement.</p> <p>In case of solicitation for renewal of an IT services contract, review the terms of eligibility, experience and major technical requirements to ensure that undue advantage is not extended to the existing vendor, and that the public entity protects itself from the risk of Vendor lock-in</p>
Contractual terms on ownership of data and access -when engaging CSPs	<p>Review to ensure that while the entity agrees to the CSP's governance and security standards, it retains the right to access third party security testing reports and actions taken, ownership of Intellectual property, as well access to entity data assets throughout the engagement term</p> <p>Ensure that draft contract as per Bid document clearly includes service requirements, payment terms, penal clauses, right to change CSP, termination and Exit strategy safeguarding the business continuity of the entity</p> <p>Ensure that the entity has included conditions that each OEM component should follow open standards and has not promoted exclusivity in application components. Further, examine if the bidder has been asked to list alternative to the proposed components</p>
Pre-Bid meeting minutes and clarifications issued	Ensure that technical and financial matters raised by prospective vendors/ Cloud Service providers are adequately considered and addressed to protect the interests of the entity.
Skill certifications of entity project team and project documents	Interview project management team to ensure that they understand the project requirements, consult users to seek clarification, acquired the capacity to evaluate Cloud service options aimed at the public sector, and obtains inputs from contractual and legal personnel
Technical evaluation parameters	Review technical evaluation parameters to ensure that the entity provides adequate weightage to vendor/CSP's other engagements, demonstration of capabilities through making prototypes, adequacy of skilled resources to be committed to the contract

	engagement, use of standard tools and test platforms, use of global delivery centres, and robustness of business continuity plans.
Audit Conclusion : To be filled in by auditor	
Vendor Management – transition, Change management and Service monitoring	
Audit Objective: To assess whether the entity is managing the Cloud service/ IT contract in line with its operational goals and has implemented adequate controls to manage transition and change risks	
Audit Issue 4 : Operation of the Service Level Agreement Is the transition plan effective ? Are all changes controlled ? Is the SLA implemented diligently? Does the entity engage adequate skillsets to manage a Cloud/ IT Outsourcing contract ?	
Criteria: Provisions/ parameters defined in Service Level Agreement Contract agreement with CSP/ IT service vendor	
Information Required	Analysis Method(s)
Transition strategy or equivalent plan	Review the document to ensure that migration is done as per service prioritization strategy; and costs and timelines for each significant milestone are clearly stated Ensure that plan lists responsibilities of contracting parties and covers security, business continuity planning, disaster recovery, connectivity adaptations, and data protection activities
Change Control board charter, CM procedures, job tickets, resolution and change documentation, test results, acceptance criteria and QA documents	Ensure that change requests are authorized by process owners, reviewed and approved by project team, timelines agreed upon Ensure that the changes made are documented with version control, fully tested and implementation approved by the entity Project team against acceptance criteria
Contract agreement	Review contract to ensure that the entity and vendor has agreed on key milestones, timelines, deliverables and process of user acceptance. Ensure user acceptance requires test plans, cases, and results to be documented and shared with the entity

(additional terms in CSP contracts)	<p>Ensure that access to source code in the event of financial insolvency of the outsourcer should is specified</p> <p>Right to Audit the CSP or suitable access to third party Audit procedures of the provider are ensured</p> <p>Ensure that conditions for exit management along with clear responsibilities for return and removal of client information assets in case of termination of contract with CSP are provided</p>
SLA document – service baselines, reporting formats and helpdesk hours	Review SLA document with CSP/ IT services vendor to ensure that full description of services for the contract duration, payment terms, escalation matrices, response and resolution log requirements are clearly defined
List of IT tools/ Enterprise Monitoring Solutions used for service monitoring	Review the list and implementation status of these tools to ensure that the entity is in a position to obtain regular reporting on the service parameters agreed upon
service monitoring reports, resource use dashboards	<p>Review to ensure adequate mechanisms are in place to generate exception reports for each period covering service quality, uptime, Turnaround time, log of secondary operation centre, outages, data breach etc. as per the parameters and terms of SLA.</p> <p>Check whether penal action is taken in cases of deviation as per contract</p>
Contract agreement terms in system integration contract with IT services vendor	<p>Where system integration with external applications and data structures are involved, evaluation parameters should consider system interdependence, infrastructure capability and capacity planning for added infrastructure.</p> <p>Ensure that Back out procedures and conditions are defined adequately for system and integration failures</p>
Entity IT staff skillsets, and training plans	Review available skillsets and training plans, interview IT managers to obtain assurance that the entity has a well-documented plan to identify needs and accordingly create and enhance capacity to manage Cloud/IT contracts
Project resource plan for Cloud engagements and list of staff engaged	Compare with actual deployment to ensure entity is committing adequate resources to manage the CSP engagement/ IT outsourcing arrangement (viz. dedicated entity team for a Development contract on Agile methodology)
<p>Audit Conclusion:</p> <p>To be filled in by auditor</p>	

Information Security, data access, hosting and Protection of Personal Data

Audit Objective : To assess whether the security , access and privacy requirements are addressed in the cloud computing arrangement and are being complied with.

Audit Issue 5 – Effectiveness of security and privacy controls

Does the entity recognise elements of security responsibility that are shared between the entity and CSP?

How does the public entity monitor the CSP's compliance to its security and privacy requirements ?

Are data protection and access rights built into the contract?

Has the public entity revised its security procedures and artefacts in line with Cloud adoption

Criteria :

- **Entity security and privacy requirements as mandated by law.**
- **Data classification as per sensitivity**
- **Data residency regulations by Government**
- **Cloud security and privacy good practices**

Information Required	Analysis Method(s)
Entity security policy and IT service contract with CSP/vendor	<p>Ensure entity policy defines procedures for acceptable use, information classification, third-party access, data transmission, remote data access, and user authentication policies along with a mechanism for periodic review of user privileges</p> <p>Review to examine that entity security requirements like third party testing, right to audit, maintenance of evidence and logs are embedded into the contract – the vendor does not have access privilege to entity data and is obliged to protect data from unauthorized access. security testing.</p> <p>The contract should clearly define what constitutes a breach of security (eg. Invalid access attempts to sensitive assets) and how the CSP will notify the entity of a breach</p> <p>All reporting requirements and issues around ownership of data must be specified in the contract</p>
Government legislations on data residency, protection and hosting	<p>Check contract for compliance to hosting locations. Further, the public entity should implement cryptographic controls for its use of cloud services. These controls should be tested both on data in transit and at rest.</p>

Data Classification based on sensitivity	<p>Ensure that the highly sensitive data elements (top secret and secret) are given additional protection and the controls installed are shared with the entity along with periodic access logs and incidence reports</p> <p>Ensure that the CSP/ vendor maintains related certification for handling top secret workloads throughout the contract duration</p>
Inventory of information assets for which the CSP/ vendor acts as a custodian	<p>Verify if the entity maintains a list of info assets – applications, data files, identity and access management software licenses, etc which are hosted at the vendor/ CSP's production and back up locations</p> <p>Verify whether the CSP/ vendor shares user and data access logs on a regular basis and whether the public entity can draw an assurance on the access to the data, application software and hardware at the outsourced location through study of access logs</p>
Policy on Segregation controls in virtual computing environments	The cloud service provider should enforce appropriate logical segregation of public entity's data, virtualized applications, operating systems, storage, and network for the separation of resources used by cloud service customers in multi-tenant environments.
Security incident reports on designated systems and data files Terms of SLA that define incidents (data breaches, security violations) and events (suspicious activities) and the responsibilities of parties and actions to be taken	<p>Contract should enforce the service provider/ CSP's obligation to provide documentation of service monitoring capabilities and deliver regular reports on security incidents and events on predefined set of highly sensitive assets.</p> <p>To draw assurance on how the entity ensures suitable actions are taken the auditor may pick a sample of incidents and determine that the service provider notified the entity on a timely basis within scope of the contract, remediation was timely based on the scope and risk of the incident, the issue was escalated within the service provider's hierarchy issue was resolved and reported to entity project management team.</p>
List of specific purpose software and additional security requirements	Review security requirements of specific purpose software (Eg- access control in e-procurement software may require that Tender evaluation committee cannot view bid values) and ensure that these are complied
Business continuity plans and DR drill reports	The contract must ensure that the Business continuity and recovery objectives are clearly defined and DR drills are scheduled notified and undertaken as per agreement
Audit Conclusion: To be filled in by auditor	

Section C – Audit findings and recommendations in IT Outsourcing

Risk Area	Audit Findings	Reference Report
A. Information Security Risks	<p>A1.1 Audit found that five audited authorities having outsourced IT systems failed to maintain adequate controls within the systems. Report noted examples of serious IT security incidents in the companies providing IT services to the government. The entities could have refined security requirements by considering different technical layers of the outsourced systems and components and placing emphasis on access controls and logging.</p> <p>A1.2 Audit also found the scope of the guidelines put in place for the vendors to be vague. A defined set of vendor obligations to ensure security of systems/services and adherence to the latest Government guidelines needs to be made part of contracts. Further, some of the authorities need to acquaint themselves with the areas of IT security covered by their suppliers' auditor's reports.</p> <p>A1.3 Audit identified the lack of appropriate risk assessment being conducted as a major concern. Appropriate risk assessment would ensure that the authorities would be in a better position to define their security requirements. In the report that evaluated six different government IT systems spreading over five authorities, only one department had conducted risk assessment appropriately.</p>	<p>A1. Management of IT security in systems outsourced to external suppliers</p> <p>-Rigsrevisionen/SAI Denmark¹⁹, November 2016</p>
B. Inaccurate assumptions and	<p>B1.1 Audit found that to implement the 1BestariNET project for developing ICT infrastructure across 10000 schools in Malaysia,</p>	<p>B1. Implementation of 1BestariNET</p>

¹⁹ <https://uk.rigsrevisionen.dk/audits-reports-archive/2016/nov/report-on-management-of-it-security-in-systems-outsourced-to-external-suppliers>

<p>incorrect scoping of work</p>	<p>the Board went for an open tender process. However, the project implementation was not successful due to the inadequacy of the tender.</p> <p>B1.2 Audit recommended that department should ensure that contents of the contract documents are in proper order and any errors such as duration of contracts and the terms of payment are rectified before signing of the contract to ensure optimal utilisation of resources.</p>	<p>- NAD Malaysia, 2013 Annual Report (Series 3)</p>
<p>C. Lack of specialized personnel</p>	<p>C1.1 Audit identified that a key factor in the failure to deliver by Central ICT programmes was due to a lack of specialist skills and experience.</p> <p>C1.2 Audit found that many government agencies failed to assess the skills required to deliver ICT programmes at the start of the process leading to significant amounts of skill gap. Audit recommended the need for a skill assessment at the onset of any project to ensure that not just personnel but also financials can be in place.</p> <p>C1.3 Government, to bridge the existing skill gap went in for short-term contracts without effective knowledge transfer plans in place. Further, over-reliance on these short-term contracts and the finances required to implement them were also identified by audit as not promising.</p> <p>C1.4 Audit identified that the Central government recruitment is constrained by the public sector pay-scales which are not at par with that offered by private sector firms.</p> <p>C1.5 While Audit accepted that the Central Government's idea to develop a Digital Transformation Service, which would act as a central resource pool, has merit, it also warned the need to have necessary checks in place while establishing the Service.</p>	<p>C1. Managing ICT Contracts in Central Government</p> <p>- SAI Scotland, June 2015²⁰</p>

²⁰ https://www.audit-scotland.gov.uk/docs/central/2015/nr_150618_ict_contracts.pdf

<p>D. Retaining Business knowledge and strategic control</p>	<p>D1.1.Audit reported that that the decision to outsource critical IT infrastructure operations services is a matter of significance, because the purpose of the government ownership of Energinet is to ensure government control with critical infrastructure, and because the operation of critical IT infrastructure is essential for the security of supply.</p> <p>D1.2 The ministry did not have opportunity to assess Energinet's outsourcing project separately before the tender process was started. Further, audit detected serious breaches of security in connection with the outsourcing, and the entity had not addressed these.</p> <p>D1.3 Audit concluded that Energinet's basis for decision and implementation of the outsourcing is worthy of criticism. The consequence is that the outsourcing risks compromise the security of supply of electricity and gas.</p>	<p>D1. Energinet's outsourcing of Critical IT infrastructure – SAI Denmark 2021²¹</p>
<p>E. ineffective formulation of strategic IT plans</p>	<p>B1.1 Audit found that the system for identifying critical information resources of the state was not sufficiently effective. These assessments lacked objectivity which impeded the implementation of the processes.</p> <p>B1.2 Audit stressed on the need for management of IT resources to be in line with the best practices of the current times. This stemmed from the audit finding that the IT planning process was not sustainable due to the high number of strategic documents in place and a lack of systematic approach. This scenario could lead to unprepared IT development plans with no detailed implementation procedures identified.</p>	<p>B1. Management of Critical State Information Resources</p> <p>- NAO Lithuania, June 2018</p>

²¹ <https://uk.rigsrevisionen.dk/Media/637878689388619078/14-2021-UK.pdf>

Chapter 3 – Audit of IT Sustainability

Section A – Elements and risks relating to IT Sustainability

A.1 Introduction

New technology brings both opportunities and risks, and one such predominant risk facing traditional firms today is failing to ensure long term IT sustainability, in the wake of disruptive technologies. Organizations need to embrace innovation, foster cultural change and embark on digital transformation programs designed to become ever more nimble and keep pace with the rapidly changing business environment.

The term “IT sustainability” can be defined as the ability of an organization to continue their digital business operations in a secure manner without being affected by changes in technology, service integrators, and availability of human resource, in the long-term. IT Sustainability is a wider concept which also includes Business continuity.

The auditor has a crucial role in adding value to public entities by reviewing their choices of new technology options, safeguarding their intellectual property and information assets and champion digital transformation of public services by identifying, documenting and disseminating best practices technology led operations

A.2 Key Elements of IT Sustainability

The key elements of IT sustainability of a public entity are inter-operability, scalability and adaptability of the entity and its personnel to new and emerging hardware and software technologies, and appropriate Governance mechanisms that promote sustainable IT.

A.2.1 Interoperability

The ISO/IEC 2382 Information Technology Vocabulary defines interoperability as the “capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.” (ISO, 2000)

Interoperability²² is the property that allows for the unrestricted sharing of resources between different systems. This can refer to the ability to share data between different components or machines, both via software and hardware, or it can be defined as the exchange of information and resources between different computers through local area networks (LANs) or wide area networks (WANs).

²² <https://www.techopedia.com/definition/631/interoperability>

Broadly speaking, Interoperability is the ability of different systems, devices, applications or products to connect and communicate in a coordinated way, without effort from the end user. Functions of interoperable components include data access, data transmission and cross-organizational collaboration regardless of its developer or origin. Similar to compatibility, interoperability helps organizations achieve higher efficiency and a more holistic view of information.

Interconnected systems can vary in degree of interoperability. Types²³ of interoperability include:

Syntactic interoperability: Systems that can communicate successfully through compatible formats and protocols. Tools that facilitate syntactic interoperability are recognized formatting standards (such as XML and JSON) or Application Programming Interfaces (APIs) . This is also sometimes referred to as structural interoperability.

Semantic interoperability : This is the ability of systems to exchange and accurately interpret information automatically. Semantic interoperability is achieved when the structure and codification of data is uniform among all systems involved.

Cross-domain or cross-organization interoperability: This refers to the standardization of practices, policies, foundations and requirements of disparate systems. Rather than relating to the mechanisms behind data exchange, this type only focuses on the non-technical aspects of an interoperable organization.

Data exchange between applications, databases and IT systems is crucial for the growth of modern technology, such as the IoT. Approaches to improving or achieving interoperability include conducting compatibility tests, engineering products with a common standard and using the same technology, coding language or syntax across multiple systems when appropriate.

In sum, the benefits of interoperability are:

- Lower costs associated with interoperable systems as fewer resources and additional maintenance is required.
- Easy access to information could be provided to all stakeholders.
- Quality of data is improved as more sources can be brought together.
- Minimizes time needed to process data, thus increasing organizational efficiency.

²³ <https://searchapparchitecture.techtarget.com/definition/interoperability>

A.2.2 Scalability

Scalability²⁴ is the measure of a system's ability to increase or decrease in performance and cost in response to changes in application and system processing demands. Examples would include how well a hardware system performs when the number of users is increased, how well a database withstands growing numbers of queries, or how well an operating system performs on different classes of hardware. Enterprises that are growing rapidly should pay special attention to scalability when evaluating hardware and software.

Scalable software can remain stable while adapting to changes, upgrades, overhauls, and resource reduction.

Scalability includes

- planning functionality i.e., the kinds of functions that need to be integrated into the software
- the storage requirements i.e., the type of storage environment or database suitable for accessing data, keeping in mind business growth and data volumes.
- Software development and maintenance i.e., developing the software in an environment and platform which is simple and would be available for a period of time, thereby ensuring continuity as well as easy maintenance.

This will mitigate the risk of adaptability i.e. the extent to which a software system can function usefully in a changing business environment.

Apart from the considerations of technical scalability, public entities also deploy innovative contractual mechanisms to manage the needs of scalability.

A.2.3 Adaptability

The ability to adapt to technological changes has emerged as a new paradigm for successful business operations. Adaptability means how quickly organizations adjust their business processes to emerging technologies to achieve their business goals. It includes the ability of the organisation and its personnel to comprehend and adopt new technological changes with minimum disruptions to the business operations.

²⁴ <https://www.gartner.com/en/information-technology/glossary/scalability>

A.3 Governance Structure for IT sustainability

Although the Interoperability and Scalability pillars of IT sustainability may have to be considered at the inception phase of an IT Project, the Adaptability aspect is to be deliberated for the whole organization periodically.

The organizations should have an IT Strategic plan in place. An effective IT Strategic plan clearly defines an IT organization's mission and requirements, and it translates that mission into long- and short-range actionable goals. The assessment of all IT assets (including IT applications, hardware, software, networks etc.) vis-à-vis the technological risks. Further, the IT assets should be assigned a priority value based on their importance for the organization. The priority value may not be driven entirely by the cost of IT asset.

All technical assets have finite lifespan due to continuous advances in the IT world. The underlying technologies of any IT application faces obsolescence with passage of time. Similarly, the OEM products and services have fixed dates for going out-of-support. Operating with technologically obsolete IT assets have implications on both interoperability and scalability. For example, the new hardware may not support the technical architecture of old applications.

Thus, the IT Strategy plan should include as assessment of its existing assets, their lifespan along with factors contributing to obsolescence. An annual working plan may be prepared to replace the old IT assets by factoring in the time and efforts required for their replacement.

Introducing a new IT application requires changes in organization culture, training of personnel. The human resources aspect of introducing a new IT application should also be considered in the IT plan.

Further, a sound Exit management strategy for each asset is a must for keeping up with up-to-date technologies.

In addition to the maintaining existing IT assets, the IT Strategy plan should be future-looking. The plan should continuously strive for replacing low-level repetitive functions and standardizing its processes through the introduction of IT applications. The plan should capture the improvement to be brought out by introduction of an IT application in objective terms.

The organization should have a Governance structure in place to periodically review these plans. Audit should check whether these plans are updated periodically, and if the Governance structure is effective. It should see if the other resources (financial and HR) are also aligned as per the IT plan. Further, Audit should see if the assessment of IT assets vis-à-vis technological obsolescence in the IT plan is proper, and if the organization is operating in with obsolete technologies.

A.4 Risks to the audited entity

While all organizations manage Sustainability risk to some degree, it is always a prudent policy that public entities become aware of IT sustainability issues and develop, implement and continuously improve a risk framework. The purpose of this exercise is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture. The predominant IT Sustainability risks are detailed below:

A. Hardware and Software risks

The hardware, software (and network) technologies adopted by the organisation should be interoperable and scalable. Failure to manage scalability risk can result in service failures or performance degradations due to lack of capacity; break down of the architecture under increased workloads, leading to an inability to support usage spikes or new business solutions etc.,

Similarly, failure to ensure inter-operability of the hardware software (and network) technologies, may hinder the faster adaptability of the organisation to the business competitive requirements in the external environment. This may result in reduction of business productivity and non-achievement of the business goals.

B. Human Resource risks

IT sustainability of an organisation includes the availability of suitable human resource to enable the adaptation of new technologies. An agile workforce with the capability to absorb and learn new technologies is essential to ensure faster adaptation of new technologies in organisational processes, thereby enabling achievement of business goals. Public entities should strategically manage workforce agility risks by transferring some of the risks through outsourcing arrangements and bringing suitable skilled resources that can deliver the learning needed for the adaptability.

C. Vendor management and outsourcing

IT outsourcing is most often aimed at allowing the entity's management to concentrate their efforts on core business activities and may also be driven by the need to reduce running costs or lack of requisite skill sets within the entity. Sustainability of the outsourced vendors is not within the control of the business organisation but with the outsourced agency and the agency industry. Non – Sustainability of the outsourced vendors may reduce the efficiency of the organisation or at its worst, leave the organisation unable to continue its business operations.

An outsourcing policy which has incorporated sustainability features, ensures that proposals for out-sourcing operations, and/or functions, database are developed and implemented in a sustainable manner.

D. Governance (and top management commitment)

IT Governance and management of the public entity, if devoid of Sustainability controls, puts the organisation to sustainability risk of being less or not adaptable to the emergent technologies thereby reducing the competitive edge. By placing Sustainability controls the IT Governance and Management of an organisation enables appropriate control environment to achievement of business goals. Sustainability concerns should be reflected by the tone at the top. This helps incorporating Sustainability controls in various policies, procedures and processes of the organisation. Sustainability risk management and ensuring its ongoing effectiveness require strong and continued commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels. Sustainability²⁵ controls should be reflected in the IT strategy, IT policies like risk management, HR policy, IT security policy etc.

E. IT Security

As technology grows in sophistication new vulnerabilities are created at a faster pace, and the organisation needs to learn to recognize potential threats in all shapes and forms. The increased use of mobile devices and cloud technology presents a new challenge for organizations trying to secure organisation's information assets. Non-Sustainability of the security controls placed in the IT environment will not only result in loss and damage of the information assets but also in non-achievement of business goals.

²⁵ **References**

<https://searchapparchitecture.techtarget.com/definition/interoperability>

<https://fullscale.io/blog/what-is-software-scalability/>

<https://www.panorama-consulting.com/why-cybersecurity-requires-a-change-management-plan/#:~:text=A%20Change%20Management%20Plan%20for%20Cybersecurity&text=Cybersecurity%20is%20a%20continuous%20battle,employee%20clicks%20a%20phishing%20link>

WGITA IDI IT Audit Handbook

ISO_IEC 27005 – IS Risk Management

ISO-IEC 31000 Risk Management

ISO-IEC 27031 BCP

Section 3B- Indicative Audit Program for Audit of IT Sustainability

Focus Area: Inter – Operability	
Audit Objective: Assess whether the software/hardware technologies and specifications selected are inter-operable to support the business objectives and growth for the foreseeable future and capable of keeping pace with new technological changes?	
Audit Issue 1 – Addressing Inter-Operability of IT systems - How does the entity identify and ensure inter-operability while choosing IT application platforms?	
Criteria: The public entity ensures that all the IT applications, services, infrastructure are inter-operable.	
Information Required	Analysis Method(s)
IT Strategy, IT plans, equivalent documents	Review the IT Strategy to determine if 'Inter-operability' is identified as a technology driver. Review whether the strategy identifies key IT applications -both internal and external to the entity where interoperability is envisaged in the future.
IT purchase policies, software/hardware policies or equivalent documents	Review and identify elements in the policies to verify if inter-operability is a parameter while making IT choices/decisions.
Relevant Steering Committee meeting minutes	Review the rationale behind the IT purchase decisions made by the Steering Committee and analyze if 'Inter-operability' was given due importance as a vital parameter for making IT choices.
Request for Proposal documents, Pre-bid Meeting documents	Review the documents to verify if the entity has ensured that the IT purchase decisions are made considering inter-operability as an essential criterion.
Meetings with IT management personnel; Incident management reports	Interview the IT management personnel including the IT security team and determine the importance placed by the personnel on 'inter-operability'.

	Interview the IT security personnel to determine instances where they experienced difficulties in containing security concerns because of non-interoperability.
Meetings with System administrators	Interview the System administrators to determine how far the existing applications, services and infrastructure is inter-operable.
Audit Conclusion : To be filled in by auditor	
Audit Issue 2 – Addressing Inter-Operability of technologies in outsourcing – Whether and how the entity ensures interoperability in outsourcing contracts?	
Criteria : The organisation ensures inter-operability of technologies while outsourcing	
Information Required	Analysis Method(s)
Request for Proposals for Outsourcing of IT services	Review the documents to determine whether the RFP clearly mentioned 'inter-operability' as an essential criteria.
Pre-bid meetings, Vendor meeting minutes/equivalent documents	Review the discussion notes to determine whether there was clarity regarding 'inter-operability' as a mandatory element.
Outsourcing contracts	Determine presence of vendor-lock in clauses.
User – Surveys, Feedback/equivalent documents	Review the user surveys on outsourced services and verify if there are indicators of issues because of vendor-lock in. Interview the IT service users to check if there are any issues because of non-interoperability of technologies.
Audit Conclusion: To be filled in by auditor	

Focus Area: Scalability

Audit Objective: Assess whether the public entity ensures that the Information Systems are Scalable and Adaptable.

Audit Issue 3 – How does the organisation identify and ensure the scalability of its Information systems?

Criteria : The organisation ensures that the IT systems are scalable.

Information Required	Analysis Method(s)
Request for Proposals for IT services/applications/ infrastructure	Review the documents to determine whether the requests for proposal clearly mentioned 'scalability' as an essential criteria and whether the scalability requirements were clearly enlisted.
Pre-bid meetings, Vendor meeting minutes/equivalent documents	Review the discussion notes to determine whether there was clarity regarding 'scalability' as a mandatory element.
Outsourcing contracts	Review the documents to determine there are appropriate clauses regarding scalability.
User – Surveys, Feedback/equivalent documents	Review the user surveys on outsourced services and verify if there are indicators of issues because of vendor-lock in. Interview the IT service users to check if there are any issues because of non-interoperability of technologies.
User requests / Service requests	Analyze the Service requests to determine if there are any requests for scalability of the hardware/software; and whether the request was addressed appropriately.
Audit Conclusion : To be filled in by auditor	

Focus area: Adaptability

Audit Objective 1 : Assess whether the IT governance and management structure, is adaptable.

Audit Issue 4 – How does the organisation addresses issues pertaining to IT Sustainability in its IT Governance and management mechanisms.

Criteria : The IT governance and management of the organisation has mechanisms in place to ensure adaptability.

Information Required	Analysis Method(s)
IT Strategic Plan	Review of IT Plans to analyse whether the top management is aware of IT Sustainability issues and attendant risks
IT Steering Committee meetings Minutes	<p>Review the documents to identify the tone at the top, regarding IT sustainability. Determine how often emerging technologies form part of their agenda.</p> <p>Verify if the IT governance bodies are aware of and constantly keeping track of emerging technologies which may add value to the business needs.</p>
IT Security committee minutes	Review the IT security committee meetings to determine how the security risks pertaining to the emerging technologies are identified, assessed and dealt with.
Risk Management Plan and minutes of meetings	Review of risk management plan to determine whether the risks on account of changing technology and attendant vulnerabilities are being addressed
Quality Assurance Plan and meetings	Review of Quality Assurance plan and minutes to determine whether there is deviation from quality parameters on account of technology changes
Audit Conclusion : To be filled in by auditor	