Guidance on Information Systems Performance Evaluations

INTOSAI WGITA Project

Guidance on Information Systems Performance Evaluations

Version 1.0

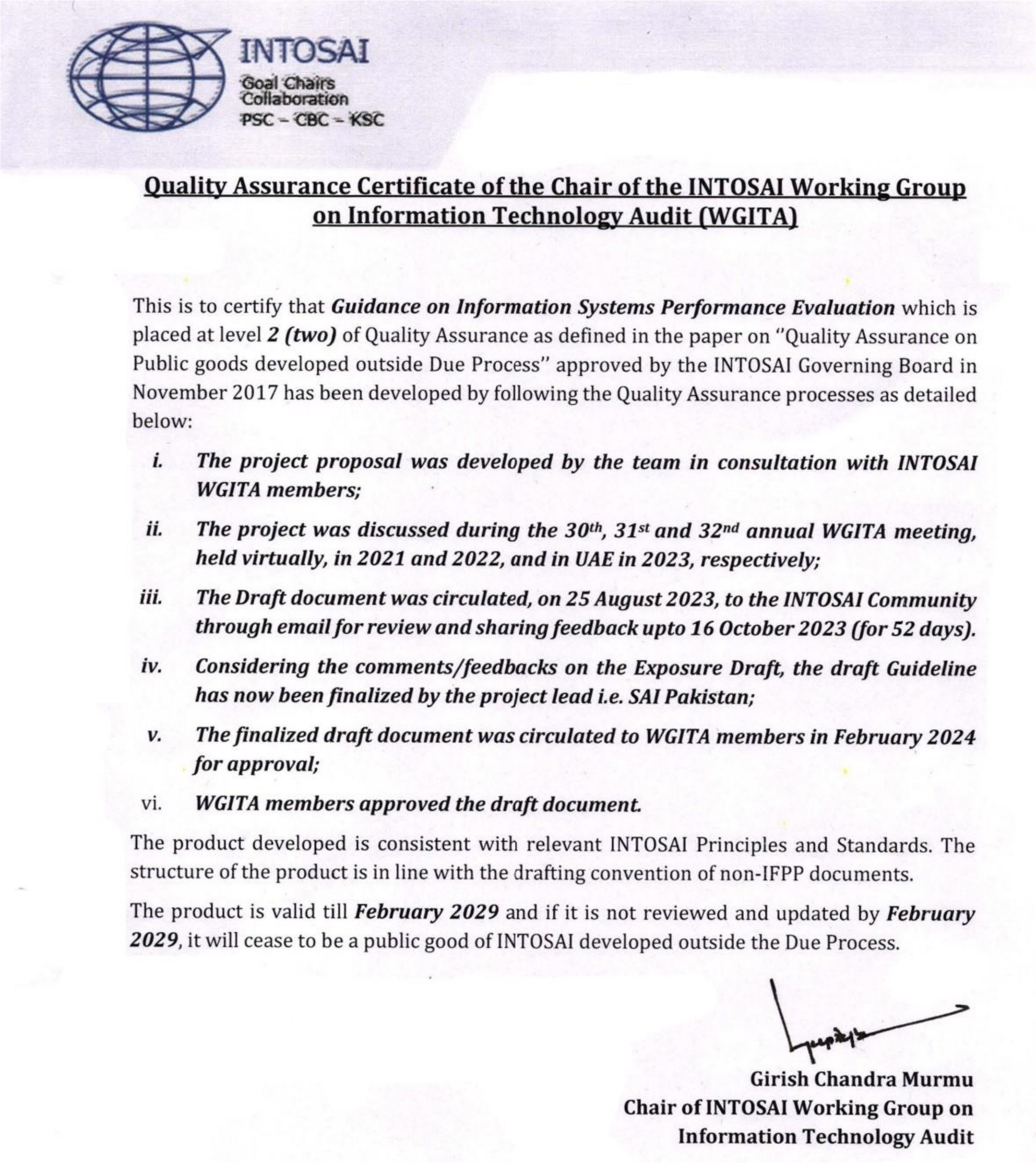
Compiled by:

Office of the Auditor General of Pakistan

(The Supreme Audit Institution of Pakistan)

Contact Info:

Address	Audit House, Constitution Avenue, Islamabad, Pakistan
Postal Code	44000
Phone	+ 92 51 922 4080
Website	www.agp.gov.pk
Email	saipak@comsats.net.pk



INTOSAI
Goal Chairs
Collaboration
PSC – CBC – KSC

Quality Assurance Certificate of the Chair of the INTOSAI Working Group on Information Technology Audit (WGITA)

This is to certify that ***Guidance on Information Systems Performance Evaluation*** which is placed at level ***2 (two)*** of Quality Assurance as defined in the paper on "Quality Assurance on Public goods developed outside Due Process" approved by the INTOSAI Governing Board in November 2017 has been developed by following the Quality Assurance processes as detailed below:

i. ***The project proposal was developed by the team in consultation with INTOSAI WGITA members;***

ii. ***The project was discussed during the 30th, 31st and 32nd annual WGITA meeting, held virtually, in 2021 and 2022, and in UAE in 2023, respectively;***

iii. ***The Draft document was circulated, on 25 August 2023, to the INTOSAI Community through email for review and sharing feedback upto 16 October 2023 (for 52 days).***

iv. ***Considering the comments/feedbacks on the Exposure Draft, the draft Guideline has now been finalized by the project lead i.e. SAI Pakistan;***

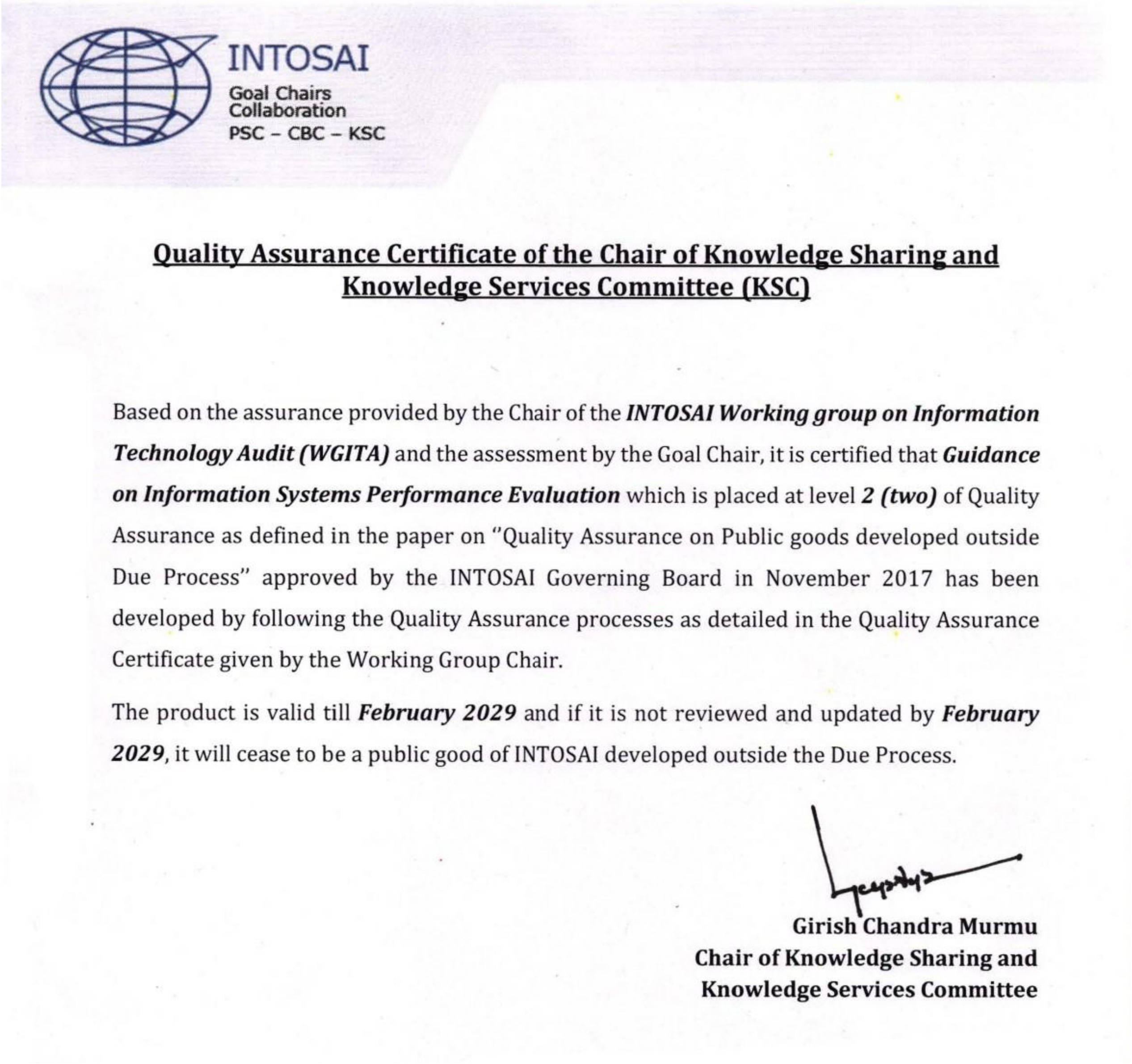
v. ***The finalized draft document was circulated to WGITA members in February 2024 for approval;***

vi. ***WGITA members approved the draft document.***

The product developed is consistent with relevant INTOSAI Principles and Standards. The structure of the product is in line with the drafting convention of non-IFPP documents.

The product is valid till ***February 2029*** and if it is not reviewed and updated by ***February 2029***, it will cease to be a public good of INTOSAI developed outside the Due Process.

Girish Chandra Murmu
Chair of INTOSAI Working Group on
Information Technology Audit



INTOSAI
Goal Chairs
Collaboration
PSC – CBC – KSC

Quality Assurance Certificate of the Chair of Knowledge Sharing and Knowledge Services Committee (KSC)

Based on the assurance provided by the Chair of the ***INTOSAI Working group on Information Technology Audit (WGITA)*** and the assessment by the Goal Chair, it is certified that ***Guidance on Information Systems Performance Evaluation*** which is placed at level ***2 (two)*** of Quality Assurance as defined in the paper on "Quality Assurance on Public goods developed outside Due Process" approved by the INTOSAI Governing Board in November 2017 has been developed by following the Quality Assurance processes as detailed in the Quality Assurance Certificate given by the Working Group Chair.

The product is valid till ***February 2029*** and if it is not reviewed and updated by ***February 2029***, it will cease to be a public good of INTOSAI developed outside the Due Process.

Girish Chandra Murmu
Chair of Knowledge Sharing and
Knowledge Services Committee

TABLE OF CONTENTS

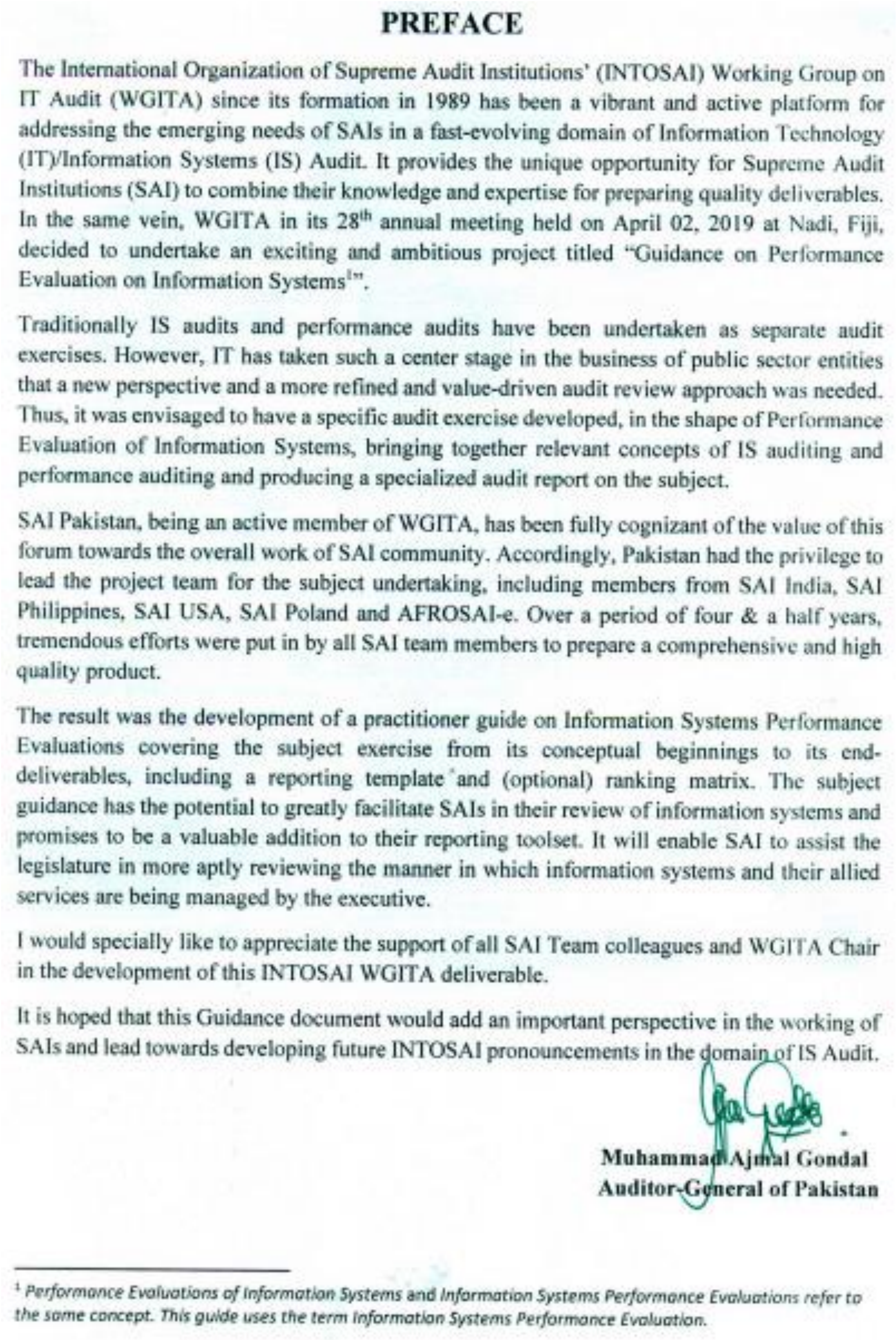
CHAPTER-4 IS Performance Evaluation Reporting

CHAPTER-5 Survey on IS Performance Evaluations

ABBREVIATIONS AND ACRONYMS

AAPSI	Agency Action Plan and Status of Implementation
AFROSAI	African Organization of Supreme Audit Institutions
AI	Artificial Intelligence
BCP	Business Continuity Planning
BIA	Business Impact Assessment
CAATs	Computer Assisted Audit Techniques
CISA	Certified Information Systems Auditor
COBIT	Control Objectives for Information and Related Technology
COTS	Commercial Off-the-Shelf Software
DLs	Driving Licenses
DOD	Department of Defense
DPR	Detailed Project Report
DR	Disaster Recovery
DRP	Disaster Recovery Planning
ERP	Enterprise Resource Planning
FY	Financial Year
GAO	Government Accountability Office
GIS	Geographical Information System
GUID	Guidance
IDI	INTOSAI Development Initiative
IFPP	INTOSAI Framework of Professional Pronouncements
INTOSAI	International Organization of Supreme Audit Institutions
ITIL	Information Technology Infrastructure Library
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISSAI	International Standards of Supreme Audit Institutions
ISPE	Information Systems Performance Evaluations
IS	Information Systems
IT	Information Technology
ITAF	Information Technology Assurance Framework
KPI	Key Performance Indicators

OLA	Operational Level Agreement
O&M	Operation and Maintenance
OMB	Office of Management and Budget
PE	Performance Evaluation
PID	Project Initiation Document
SAIs	Supreme Audit Institutions
SLAs	Service Level Agreements
SNGPL	Sui Northern Gas Pipelines Limited
TCO	Total Cost of Ownership
TOR	Terms of Reference
UNCTAD	United Nations Conference On Trade And Development
UNSDGs	United Nations Sustainable Development Goals
USD	United States Dollar
WBS	Work Breakdown Structure
WGITA	INTOSAI Working Group on IT Audit



PREFACE

The International Organization of Supreme Audit Institutions' (INTOSAI) Working Group on IT Audit (WGITA) since its formation in 1989 has been a vibrant and active platform for addressing the emerging needs of SAIs in a fast-evolving domain of Information Technology (IT)/Information Systems (IS) Audit. It provides the unique opportunity for Supreme Audit Institutions (SAI) to combine their knowledge and expertise for preparing quality deliverables. In the same vein, WGITA in its 28th annual meeting held on April 02, 2019 at Nadi, Fiji, decided to undertake an exciting and ambitious project titled "Guidance on Performance Evaluation on Information Systems[1]".

Traditionally IS audits and performance audits have been undertaken as separate audit exercises. However, IT has taken such a center stage in the business of public sector entities that a new perspective and a more refined and value-driven audit review approach was needed. Thus, it was envisaged to have a specific audit exercise developed, in the shape of Performance Evaluation of Information Systems, bringing together relevant concepts of IS auditing and performance auditing and producing a specialized audit report on the subject.

SAI Pakistan, being an active member of WGITA, has been fully cognizant of the value of this forum towards the overall work of SAI community. Accordingly, Pakistan had the privilege to lead the project team for the subject undertaking, including members from SAI India, SAI Philippines, SAI USA, SAI Poland and AFROSAI-e. Over a period of four & a half years, tremendous efforts were put in by all SAI team members to prepare a comprehensive and high quality product.

The result was the development of a practitioner guide on Information Systems Performance Evaluations covering the subject exercise from its conceptual beginnings to its end-deliverables, including a reporting template and (optional) ranking matrix. The subject guidance has the potential to greatly facilitate SAIs in their review of information systems and promises to be a valuable addition to their reporting toolset. It will enable SAI to assist the legislature in more aptly reviewing the manner in which information systems and their allied services are being managed by the executive.

I would specially like to appreciate the support of all SAI Team colleagues and WGITA Chair in the development of this INTOSAI WGITA deliverable.

It is hoped that this Guidance document would add an important perspective in the working of SAIs and lead towards developing future INTOSAI pronouncements in the domain of IS Audit.

Muhammad Ajmal Gondal
Auditor-General of Pakistan

[1] *Performance Evaluations of Information Systems and Information Systems Performance Evaluations refer to the same concept. This guide uses the term Information Systems Performance Evaluation.*

PROJECT TEAM

Sr. No.	SAI Name / Body	Name of Member	Designation
1	AFROSAI-e	Fredrick M. Bobo	Information Systems Audit Manager
2		Brighton Mpatisha	Assistant Director IT Audit Zambia
3	India	Dr. Sandip Roy	Director General of Audit
4		Deepak Raghu	Director Audit
5	Pakistan	Muhammad Ali Farooq Gheba (***Project Team Lead***)	Director Audit
6	Philippines	Marlon R. Marquina	Director IV – Information Technology Audit Office
7		Love P. Magtangob	OIC – Supervising Auditor Information Systems and Technology Audit Division (ISTAD)
8		Mark Anthony A. Pardilla	OIC – Supervising Auditor ISTAD
9		Rayziell S. Verunque	OIC – Supervising Auditor ISTAD
10		Blaine Jenner A. Bilalat	Division Chief - Data Analytics and Electronic Evidence Unit
11	Poland	Pawel Banaś	Advisor to the NIK President
12	United States of America	Michael Holland	Assistant Director
13		Sabine Paul	Assistant Director
14		Lauri Barnes	Senior Communication Analyst
15		Anthony Gray	Information Technology Analyst
16		Evan Kreiensieck	Information Technology Analyst
17		Ashley Mattson	Information Technology Analyst
Note: *Colleagues from SAI Russia, actively participated in the project during the survey and early development stage and later opted out of the project.*			

Abstract

The Information Technology (IT) landscape is continuously changing with new business solutions and comparatively more advanced technologies getting introduced at a fast pace. Use of IT in the public sector has become widespread. A large variety of Information Systems (IS) solutions having different quality, cost, and sustainability factors are readily available for achieving specific tasks. Hence the use of IT is becoming a key audit area for the Supreme Audit Institution (SAI) Auditor.

In the light of the above context this document builds a case to review an IS solution from a performance perspective. It highlights how this idea is viable and logical and touches upon the benefits of carrying out a dedicated Information Systems Performance Evaluations (ISPE). It also establishes links with the overarching International Organization of Supreme Audit Institutions (INTOSAI) framework for the purpose of clarity.

The document has been prepared as a practitioner guide, enabling an SAI auditor to undertake an ISPE from start to finish. It comprises 05 chapters.

The first chapter builds the conceptual foundation for an ISPE. Chapter two elaborates planning, followed by execution and reporting in chapters three and four, respectively. Case studies and important review points in the context of an ISPE have been included in the guide. In addition, a reporting template as well as an (optional) performance rating methodology have been included for the purpose of making an ISPE report more value-added.

Lastly, chapter 05 contains results of a survey, carried out during the preparation of the subject document. The survey gives an important insight into the current practices related to ISPE being carried amongst SAIs.

The guide is presented as a live document with an aim of having it revisited for changes/enhancements in five years’ time. An e-version of an ISPE is also envisaged in the update.

CHAPTER 01

Introduction to Guidance on Information Systems Performance Evaluations

Chapter 1: Introduction

In this chapter an effort has been made to build a case and a conceptual basis for undertaking information systems performance evaluations. All major aspects related to the topic have been first identified and then linked together in a logical manner. Giving due consideration to higher level INTOSAI pronouncements, a space has been created for undertaking a more specialized field-work level audit exercise focusing on information systems performance evaluations.

1.1 Information Technology landscape

IT has revolutionized the way people are communicating with each other and conducting various activities, both in the public and private sectors, during the last few decades. Globalization in its true sense has been manifested through the expansion of IT around the world. More recently we have witnessed a technological enhancement phase coined as the “Fourth Industrial Revolution” or “Industry 4.0.” The Industry 4.0, concept represents the change digitization and automation[1] have made to every aspect of underlying businesses. Fourth Industrial Revolution Technologies comprises of solutions/concepts such as, artificial intelligence (AI), mobility (including autonomous vehicles), block-chain, drones,[2] internet of things, cyber-physical systems, and cloud computing,[3] etc.

The Covid-19 pandemic further accelerated the use of IT for all types of business solutions including more use of remote operations and work-from-home solutions. Resultantly the IT industry has grown over the last few years and is expected to grow even further. The global spending of IT increased from USD 3.87 trillion in 2020 to USD 4.23 trillion in 2021.[4]

The United Nations Conference on Trade and Development’s Technology and Innovation Report 2023 lists out 17 frontier technologies, most of which are IT based, highlighting that their combined market value is expected to reach USD 9.5 trillion by 2023.[5]

1.2 Multiplicity and diversity of IS solutions

Advancement in IT has led to the generation of multifarious IS solutions. In the public sector, policies aimed at enhancing public service delivery through the use of IT have been steadily

[1] “An Overview of Industry 4.0: Definition, Components, and Government Initiatives”, Journal of Advance Research in Dynamical & Control Systems, Vol. 10, 14-Special Issue, 2018, page 1379.

[2] Global Technology Governance Report 2021: Harnessing Fourth Industrial Revolution Technologies in a COVID-19 World, World Economic Forum, pg 04

[3] https://www.twi-global.com/what-we-do/research-and-technology/technologies/industry-4-0, accessed 27 June 2022.

[4] https://www.statista.com/statistics/203935/overall-it-spending-worldwide/, accessed 28 June 2022

[5] Technology And Innovation Report 2023 - United Nations Conference On Trade And Development (UNCTAD), pg xvi

increasing, adding to the multifariousness of the IS being used. Not only is there great diversity in the range of IT solutions catering for different types of activities, there are also all numerous alternatives/substitutes available for providing the same services[6] in a different manner. For example, if an organization wants to automate its business process, there are various options for doing the same, ranging from multiple standalone IT applications to enterprise resource planning (ERP) systems. Similarly, for networking and data management, various alternatives and solutions are available. The proliferation of IT applications arising from the advancement in IT has further increased the IT solution universe.

The ever-increasing range of alternatives offer both an opportunity as well as a challenge for the selection of IS solutions. The opportunity is the ability of a large variety of choices from which to choose. The challenge is to choose the best alternative to support the underlying business objective and to help achieve business targets/goals.

The multiplicity of IT solutions and the wide range of competing alternatives pose two different sets of challenges for organizations implementing IT initiatives. One set of challenges deals with addressing the diversity/multiplicity of IS solutions available. This domain comprises of questions such as:

- What processes do we need to automate? To what extent should this automation be (i.e., will the automation be for the sake of automation)? Will it add value to our business and how will its impact be gauged? Will new avoidable risks be added resulting in more cost or not?
- What processes do we need to integrate through IS?
- How will the automated process impact our business environment, including aspects such as cybersecurity?
- What are our key deliverables and goals from subject automation / integration / enhancement?

Such questions need to be addressed by senior management of the organization enabling that organization take sound decisions with regards to IS procurements.

[6] For the purpose of clarity, IS signifies the combination of technology and digital data coming together to perform a specific task or activity. Although at times IT and IS are used interchangeably in this context, IS constitutes a more umbrella level term as compared with IT.

Once an organization has mapped the type of automation it desires, the type and extent of IT services it is looking for, both in case on new automation or transformation from a legacy to a more contemporary solution, the next step is selecting the most feasible IT alternative available. This represents the second set of challenges faced by any organization undertaking IT initiatives and comprises of addressing questions such as:

- How much expense are we willing to spend on the IS initiative?
- What alternates are available?
- Which alternates are most compatible with our business environment?
- How will the selected IS solution remain sustainable in the long term?

Operational level managers and implementation teams are normally tasked with the execution-end of an IS solution.

Hence, for all organizations, dealing with IS solutions is a major task having short term and long term impacts on the future of that business. Only by making the most feasible decisions, can an organization achieve maximum value and thereby good performance from the IS solution. Performance of the IS solution is therefore directly linked with the overall performance of that organization.

1.3 Public Sector Organizations and IS Initiatives

Public sector organizations have even higher stakes as compared with other entities when it comes to undertaking IS initiatives. Firstly, there is an inherent scarcity of financial resources/budget as multiple organizations at national and sub-national levels have competing demands and urgent needs. The second aspect is that of financial accountability. Public money needs to be spent with utmost care and due diligence ensuring that maximum value was drawn from the funds that were utilized. Lastly, another important aspect is the “quality” of service delivery being managed through IT. That is how a specific public service has added value to its services through the use of IT (e.g., vehicle registration solutions, pension disbursement solutions etc.).

Hence for government functionaries, the challenge of undertaking IS tasks is significant as the public sector auditors ultimately have to give an assurance that the IS solutions procured and implemented were adequate and beneficial.

1.4 Information Systems and the Performance Perspective

Implementing an IS does not necessarily mean that it will be successful. If an IS solution is, on the surface, delivering results, having its own set of controls and protocols, it cannot singularly be flagged as a success. IT initiatives can face failure due to various factors.

According to a report titled "Improving IT Project Outcomes" published by International Data Corporation in 2009,[7] "50% of (IT) projects required rework and 20 to 25% did not provide return on investment". In addition, research done by "Boston Consulting Group found that 70% of digital transformations fell short of their objectives. Further the 2020 Global Application Modernization Business Barometer Report found that 74% of organizations that had started a legacy system modernization project had failed to complete it."[8]

The causes for the failure of IT projects can be many. Some of these include:

- "Gap between users and automation experts
- Difficulties with the economic evaluation of information projects
- Mis-match between information systems and organizations"[9]
- "Underestimating or ignoring the impact of change
- Trying to do it too cheap"[10]
- "Unbalanced ecosystems. (Structures that become manifest in the interdependencies between entities and resources can be described as ecosystems.)"[11]

From the above illustration, it can be appreciated that there is a very specific and critical angle of *"performance"* linked with IS implemented across any entity including government organizations. For example, just moving from manual to automated process or from an obsolete system to a newer one is by no means the end goal. In fact, it is the manner in which an IS performs that ultimately determines whether that IS implementation was a success, a failure or a success to what extent.

The performance perspective puts together all such factors and variables (such as cost savings, timeliness, increased output, etc.). These factors and variables have the sum effect of

[7] Why Do Information Technology Projects Fail?, Adam Alami, Procedia Computer Science 100 (2016) 62 – 71

[8] Why IT projects still fail (cio.com), accessed 08 August 2022

[9] Information Organization and Information Systems Design – An integrated approach to information problems by Bart Prakken, © 2000 Springer Science+Business Media Dordrech, pg 06

[10] 10 reasons for IT failure | ZDNet, accessed 08 August 2022

[11] Why Do Information Technology Projects Fail?, Adam Alami, Procedia Computer Science 100 (2016) 62 – 71

ascertaining whether an IS solution can be termed an accomplishment in an objective manner or whether there are gaps and the performance of the IS solution is not satisfactory.

1.5 Audit and the emerging IT landscape

The influx of IT solutions across private and public activities has brought forward challenges and opportunities for the work of SAIs. On one hand, they represent significant capacity challenges as traditional approaches to test controls might no longer be viable. On the other hand, they present an opportunity for the SAIs to add value to their services and enhance their institutional competency by taking advantage of new auditing tools and techniques. In this context, auditing ISs has taken center stage in the work of the SAIs.

1.6 The performance evaluation concept – Simple yet challenging

The term performance as a variable noun can be defined as:

- The manner in which a mechanism performs[12]
- How well a person, machine etc. does a piece of work or an activity[13]
- Someone or something's performance is how successful they are or how well they do something[14]

Hence, there is an inherent element of "evaluation" or "assessment" when the term performance is used as a variable noun. This assessment of performance varies greatly depending upon the "context" in which it is being carried out. For example, if the context is achievement of United Nations Sustainable Development Goals (UNSDGs), then the performance of a government may be the attainment of or extent to which UNSDGs were achieved over a specific period of time. Similarly, performance of intra-city mass transit system would be totally different. Such a review may include, commuter data analysis, revenues, city traffic flow changes, or increased job offerings.

Performance therefore, envisages analyzing things from a unique perspective different from other evaluation approaches such as compliance reviews or financial assessments. The set of variables/indicators for reviewing performance may comprise quantifiable factors (e.g., cost savings) and non-quantifiable factors (e.g., ease of doing business). How to piece together and weigh different performance parameters in a specific context to present a holistic assessment is the key and most challenging part of a performance evaluation assignment.

[12] Performance Definition & Meaning - Merriam-Webster, accessed 09th August 2022
[13] PERFORMANCE | meaning in the Cambridge English Dictionary, accessed 09th August 2022
[14] Performance definition and meaning | Collins English Dictionary (collinsdictionary.com), accessed 09th August 2022

1.7 Defining IS Performance Evaluations

In order to define IS Performance Evaluations, it is imperative to have a definitional overview of Performance Auditing and Information Systems Auditing and then illustrate how the unique concept of IS Performance Evaluation emerges from these two domains.

1.7.1 Performance Auditing

ISAAI 300 defines performance auditing as[15] "an independent, objective a reliable examination of whether government undertakings, systems, operations, programmes, activities or organizations are operating in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvement."

1.7.2 Information Systems Audit

INTOSAI GUID 5100 defines information systems audit,[16] "as the examination of controls related to IT-driven information systems, in order to identify instances of deviation from criteria, which have in turn been identified based on the type of audit engagement - i.e. Financial Audit, Compliance Audit or Performance Audit."

- ISACA elaborates information systems auditing as,[17] "the formal examination and/or testing of information systems to determine whether:
- ISs are in compliance with applicable laws, regulations, contracts and/or industry guidelines.
- ISs and related processes comply with governance criteria and related and relevant policies and procedures.
- IS data and information have appropriate levels of confidentiality, integrity and availability
- IS operations are being accomplished efficiently and effectiveness targets are being met".

1.7.3 The definition

Information Systems Performance Evaluations **(ISPE)** is an audit review approach wherein the auditor assesses an implemented IS solution or programme from the point of view of its performance. This assessment includes determining whether the IS is achieving specific goals. By extension, an IS performance evaluation can include

[15] Section 03 Para 09 of ISSAI 300
[16] Para 3.1 of INTOSAI GUID 5100
[17] Para 1.0 CISA Review Manual 27th Edition

assessing the processes which contribute to the program's ability to achieve specific goals. This performance can be measured in both technical and non-technical terms. For example, the business value that an IS solution has added to the organization or its average system up-time, load management statistics, etc.

Hence, performance evaluation envisages review of an IT solution or programme along performance related parameters in order to draw a holistic picture on how and to what extent the subject IT implementation has performed and delivered intended outputs or outcomes.

Further, the scope of a performance evaluation may vary with the type of review taking place. For example, an IS performance evaluation maybe carried out for a unique IS solution pertaining to one entity or for an ERP solution spread across various public offices or further still for a broader IS programme containing multiple IS solutions spread across different public sector areas.

SAI Auditors may assess information systems performance evaluation through different approaches based on their mandate and working practice. Such as, the performance of the IS can be evaluated in terms of whether or not the targets adopted in terms of scheduled timelines, sanctioned budget and functional metrics have been achieved.

Similarly, performance can also be evaluated through classification levels. That is by concluding from a performance review the extent to which the IS solution is performing very well, or average or poorly, etc. as the case may be.

Before going into the details of ISPE two the following two clarifications are given in order to avoid any confusing or misinterpretation viz a viz the subject guidance. These are:

- ISPE is not being presented as contrary in any way to the INTOSAI pronouncements governing IS Auditing and Performance Auditing. Rather the ISPE concept is being introduced as a drill-down product and a specific audit deliverable drawing concepts from the higher-level prescribed auditing pronouncements.
- The term "evaluation" in this guidance is being used solely from an audit review perspective.

1.8 Uniqueness of Information Systems Performance Evaluations (ISPE)

From the planning stage to the reporting stage ISPE represents a slightly different analytical and thinking process than the one followed in a purely performance audit or an IS Audit. Illustratively:

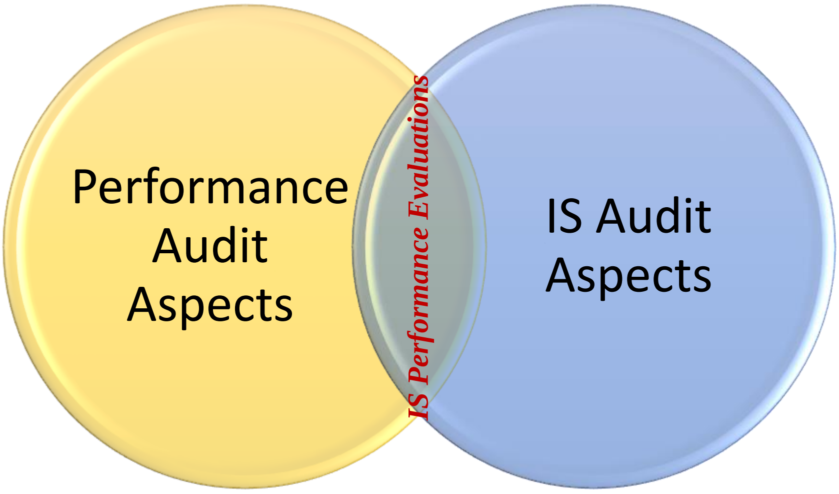


Figure - 01

The IS performance evaluation encompasses elements of both performance audits and IS audits. However, in contrast to an IS audit, not all IT audit controls reviews would necessarily be part of an ISPE. In addition, in contrast to a typical performance audit, performance weightages may have to be assigned to IT control assessments.

Elaborating this concept further, a standard performance audit exercise is an audit approach in which commonly identified performance variables such as economy, efficiency, effectiveness etc. are linked with the project or system being reviewed whether IT based or not.

1.9 Standard IS Audit and ISPE comparison

IS Audit is an umbrella term dealing with the whole universe of IT Auditing. It is a very "live" concept and as IT technologies continue to enhance/change the domain of IS auditing keeps on modifying with new subjects getting added to IT. The INTOSAI WGITA project titled, "Roadmap for development of future GUIDs in the 5100 Series" highlighted this concept. It linked together how new emerging technologies directly correlated with new auditable areas. From standard IS audit domains such as IT Governance, IT Data management, IS Security, etc., the scope of audit work has moved on to more complex and specialized IT areas such artificial intelligence (AI), Cloud computing, cyber security, crypto currency transaction analysis etc.

Hence, in an IS Audit exercise, audit checklists and review points are specific to an IS domain area being reviewed. Performance considerations are not the focal point of a typical IS audit review, rather, they may be part of a set of subsidiary questions which auditors may ask along with their core analysis.

Furthermore, the end-product of a standard IS audit exercise would include risk assessment findings or comments on the level of system maturity implemented in an organization. For example, if the specific IS audit domain under review is cyber security resilience in an organization, the IS report would primarily include a commentary on the state of internal controls and allied practices with regards to that specific IS audit domain.

On the other hand, in a performance evaluation exercise, those IT aspects and factors are identified and evaluated which can be quantified or qualified and related with the overall performance of that IS system in organization. This approach leads to questions that are not necessarily covered in a standard IS audit exercise. For example, how does a new IS system in any organization integrate with the overall IT framework across the government? Does it add value to the public sector at a holistic level? Or does an IT framework align with the strategic organizational plans or goals. Other factors that could be evaluated or quantified could include assessing how far and in what manner the specific business processes have been catered for by the IS solution in an efficient, reliable, and transparent manner. Broad-based assessment could also include assessing whether the IS has facilitated business change management in an organization (i.e., has the IS solution become part of the new organizational culture[18]) etc.

Hence ISPE presents a specific/specialized audit exercise taking concepts from both IS auditing and Performance auditing for preparing a uniquely presentable audit deliverable.

1.10 Existing INTOSAIs GUIDs on IT Audit

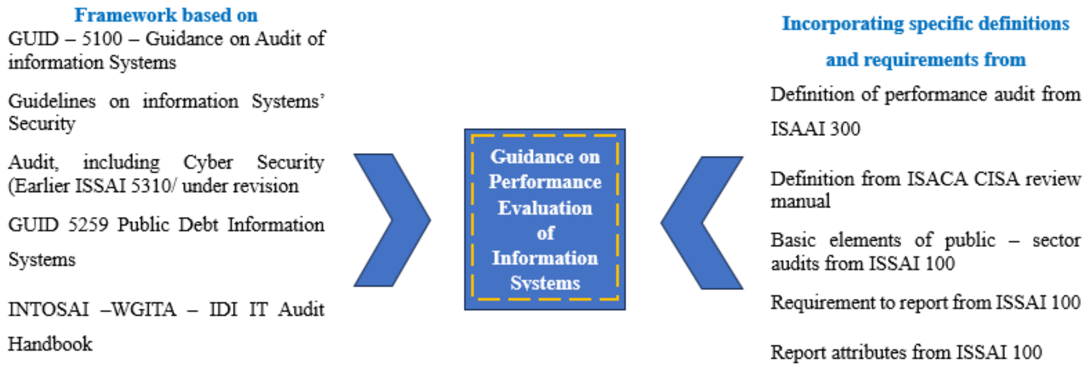
The following major documents and pronouncements are currently available at the INTOSAI platform:

- GUID – 5100 – Guidance on Audit of Information Systems
- Guidelines on Information Systems' Security Audit, including Cyber Security (Earlier ISSAI 5310) /under revision

[18] In many traditional organizations IT experts/ consults are embedded in an entity to facilitate transition to a new business process facilitated by IT. However, if the solution is over complex and dysfunctional with the working culture of that organization, employees only learn the bare minimum usage of the system and the IT experts end-up becoming silos of information only. This greatly reduces the utility of the IS implemented and due benefits are not achieved from it.

- GUID 5259 Public Debt Information Systems
- INTOSAI – WGITA – IDI IT Audit Handbook

Illustratively:


Framework based on
GUID – 5100 – Guidance on Audit of information Systems
Guidelines on information Systems' Security
Audit, including Cyber Security (Earlier ISSAI 5310/ under revision
GUID 5259 Public Debt Information Systems
INTOSAI –WGITA – IDI IT Audit Handbook
Guidance on Performance Evaluation of Information Systems
Incorporating specific definitions and requirements from
Definition of performance audit from ISAAI 300
Definition from ISACA CISA review manual
Basic elements of public – sector audits from ISSAI 100
Requirement to report from ISSAI 100
Report attributes from ISSAI 100

1.11 Need for specific guidance document/work-tool guide on information systems performance evaluations (ISPE)

As has been highlighted earlier in this chapter, large amount of expense is being incurred globally in the IT sector, and the same holds true for the public organizations. Information system solutions are more critically impacting government operations and services than even a decade earlier. At the same time, more budget is being utilized by undertaking IS initiatives by government organizations. This new digitalized and fast-changing IT audit environment mandates the need for carrying out performance evaluation reviews of IS impacted in the government. This is needed to answer basic questions such as,

How is the IS solution in an organization performing upon which significant funds were spent with even more needed for its upkeep and with key government processes now solely relying on the IS solution?

The existing INTOSAI GUIDs and IDI-WGITA handbook *(listed at 1.10 above)* at present cover IS auditing from a broad general perspective with exception being that of information security. These documents do not cover IS performance evaluation as a unique audit exercise with defined objectives, methodologies, and deliverables. Moreover, being higher level INTOSAI pronouncements, these GUIDs/Documents do-not contain the implementation details and procedural steps that can act as one-stop practical auditing tool with respect to IS Performance Evaluation for the SAI auditor.

For example, ISSAI 5310 on Information Security focuses on methods and practices to review an IT security environment. Similarly, IT Application/IT General control reviews given in the IT Audit handbook focus of the assessment of the controls in place with regards to an IT implementation. In addition, GUID 5100 is within the INTOSAI IFPP an umbrella document on IS Auditing. It outlines major IS Auditing aspects and proposes that IS Auditing can be carried out as a component of a regular Performance Audit or Compliance Audit exercise. It does not propose or provides details on stand-alone IS Audit reporting.

Hence, there is significant need and scope to develop a practitioner guide on the IS performance evaluation. To begin with, such a document would give the conceptual clarity of undertaking IS Performance Evaluation as a stand-alone audit exercise with presentable reporting deliverables. Then it would act as a one-stop tool to facilitate IS Auditor in practically carrying out IS performance evaluation.

Considering the currency of the topic and the plausible working space as no guidance documents or work tools on the dimensions and aspects being considered in this document are available, at the INTOSAI level, the subject guidance development has been undertaken.

1.12 About the guidance document/Its Objective

The subject guidance document[19] *"envisages preparation of Guidance based document to facilitate SAIs in carrying out performance evaluation of Information Systems. The document would look to propose best practices and steps that could be deployed to objectively and comprehensively evaluate the performance of Information Systems."*

1.12.1 Future prospective enhancements / development in the guidance document

Considering the steady enhancements in IT, this guidance document has been developed as a live document subject to future revisions. An initial revision is proposed after 05 years. Areas envisaged for its revised version may include:

- *Developing guidance on performance evaluation of AI Solutions. AI is impacting public & private sector processes globally at such a scale that it warrants examination as a specific sub area of ISPE.*
- *Development of further guidance to cover ongoing IT / IS Projects.*
- *Development of an e-version of the guidance, offering interoperability with standard* Audit Management Information Systems (AMIS) *solutions.*

[19] Description of Project as per approved PID

1.13 Benefits of undertaking IS performance evaluation

The subject guidance comprises audit execution methodology as well as a (sample) reporting template. It will provide the dual benefit of assisting the auditor in carrying out performance evaluations of IS and presenting their findings along a (sample) pre-defined reporting methodology to add more value to the presentation of their findings. Having a working tool to conduct IS performance evaluation will add to the reporting diversity of the SAI and enable it to approach the ever-changing IT Audit environment in an adequately results-oriented way.

Through ISPE reports, comparison on IS implementation across different entities would be facilitated and broader IT programme reviews would be possible. On the one hand, reports so prepared will act as a facilitating tool for executives for improving their IS implementation practices. On the other hand, it will strengthen parliamentary oversight over public spending through presentation of more diversified reporting facilitated through IS performance evaluation reviews.

1.14 Methodology

The methodology used for development of subject guidance document involved the following techniques:

- Leveraging information from other INTOSAI WGITA products
- Survey to gather information on Information System Performance Evaluation practices across SAIs
- Research on the subject topic looking for best practices in public and private domains around the world

1.15 Structure of the guidance document

This guidance document has been framed across five chapters, arranged in their logical sequence. The discussion flows from audit planning (chapter 02) to audit execution (chapter 03) and finally concludes at ISPE audit reporting (chapter 04). Separately, results of a survey highlighting practices in IS performance evaluation across SAIs has been added at the end in Chapter 05.

CHAPTER 02
Planning the Information Systems
Performance Evaluation

2.1 Introduction

Planning for the performance evaluation involves (1) prioritizing and selecting information systems; (2) planning the audit; and (3) designing the audit.

2.2 Prioritizing and Selecting Information Systems

The proliferation of information systems that organizations rely on to meet their mission has made selecting which systems to audit more challenging. SAIs face complex choices when deciding which systems to audit, what to audit in those systems, and how frequently audits should be conducted. A risk-based approach helps with prioritizing and selecting suitable areas to audit. Additionally, the SAI will need to incorporate obligatory audits, like those required by law or requested by a legislative authority or other oversight entities.[20]

Prioritizing and selecting information systems involves:

- identifying the audit universe, i.e., specific topics, entities (e.g., ministries, departments, or agencies), programmes, public sector areas, or critical issues
- using criteria to prioritize and select a specific system(s) / programme for evaluation, and
- selecting an audit subject.

2.2.1 Identifying a Universe of Information Systems

The audit universe includes specific topics, entities (e.g., ministries, departments, or agencies), or critical issues that are impacted by information systems, including those which the auditor general is mandated to audit. The business processes in the organization(s) predominantly relying on IT constitute an important part of this universe. The audit universe can be informed by some of the following factors:[21]

- Risk assessments
- SAI strategic plan
- Audit coverage cycles
- Requests from the legislative authorities
- Requests from the audited entities

Specific steps that the SAI can take to identify the audit universe include the following:[22]

- Scanning the public sector environment

[20] International Organization of Supreme Audit Institutions (INTOSAI) Working Group on IT Audit, *INTOSAI Development Initiative (IDI) Handbook on IT Audit for Supreme Audit Institutions*

[21] SAI responses to survey for Preparation of Guidance on Performance Evaluation of Information Systems

[22] International Organization of Supreme Audit Institutions*, Performance Audit ISSAI Implementation Handbook: 68*

- Reviewing official announcements
- Conducting a financial analysis
- Considering the views and suggestions of citizens as well as other stakeholders
- Monitoring media reports

The SAI may put in place adequate procedures and processes to validate the information gathered to ensure accurate profiling of the audit universe.

2.2.2 Prioritizing Potential Systems for Evaluation

After identifying the audit universe, the next step is identifying potential systems to evaluate. Identifying these systems may include the following steps:

- Inventorying the information systems associated with the topics, entities, and issues identified in the audit universe and categorizing them.
- Determining which of the systems impact critical functions, business processes or assets, such as money, materials, customers, decision making, and how close to real-time they operate.
- Assessing the risks that affect these systems and the severity of their impact on the business.
- Ranking the systems based on the above assessment and deciding the audit priority, resources, schedule, and frequency.

2.2.3 Selecting Specific Systems for Evaluation

Auditors should analyze specific systems and impacts they have on the key business processes associated with the identified topics, entities, and issues. The auditors may share knowledge from previous audits, and information from the entity's strategic planning process may be relevant. In this process, auditors should consider whether the performance evaluation would be sufficiently significant, auditable, and aligned with the SAI's mandate. The selection process should aim to maximise the expected impact of the audit while accounting for SAI's audit capacities (e.g., human resources and professional skills).[23] The selection process may consider the systems that have been prioritized for performance evaluation by the SAIs.

In addition, the evaluation should consider the need for a ***material topic*** and ***risks for performance problems*** (problems related to effectiveness, economy, and efficiency –the three E's), the need for an ***auditable topic*** (considering the SAI's capacities to carry out a high quality audit, but also the timeliness, other work in progress and the sensitivity) and the need for

[23] ISSAI 300- 36

potential for change (the audit need to be likely to contribute to the improvement of the functioning of government and its entities)[24].

2.2.4 Other Considerations in Prioritizing and Selecting Information Systems

When prioritizing and selecting information systems for performance evaluation, an auditor can explore other considerations, including the following:

- **The system's size and its impact on other entities**: The size of an information system could have an impact on the need for a performance evaluation. In other circumstances, the spread and impact of the information system on government operations would also affect the need for a performance evaluation. For example, an integrated financial management system used by a large percentage of government entities could be a good candidate for an information system performance evaluation associated with financial management. Similarly, IS programmes spread across various entities having broader sector-wise objectives, goals and outcomes could also be a criterion for their selection.
- **A system used in highly sensitive or critical operations**: A system (or systems) used in highly sensitive operations or that impacts critical government operations may be selected for a performance evaluation. For example, the U.S. Government Accountability Office has conducted a series of evaluations aimed at helping the Department of Defense improve the information systems that support its efforts to accurately account for and reliably report its spending and assets. Financial management weaknesses at the Department of Defense are a key impediment in the U.S. Federal Government's efforts to achieve an opinion on the federal government's accrual-based consolidated financial statements.[25]
- **Levels of control, concern, and influence as an SAI**: Prioritising and selecting an information system for performance evaluation might also depend on the levels of control, concern, and influence an SAI may have over an information system. Information systems might be selected based on the level of concern that stakeholders have expressed (sphere of concern) and how the SAI is positioned to influence potential improvements affecting the livelihood of its citizens (sphere of influence). For example, the SAI might select a system used in the administration of government subsidies (e.g.,

[24] AFROSAI-E Performance Audit Handbook

[25] GAO, *Financial Management: DOD Needs to Improve System Oversight*, GAO-23-104539 (Washington, D.C., Mar. 7, 2023); *DOD Financial Management: Air Force Needs to Improve Its System Migration Efforts*, GAO-22-103636 (Washington, D.C., Feb 28, 2022); *Financial Audit: FY 2021 and FY 2020 Consolidated Financial Statements of the U.S. Government*, GAO-22-105122 (Washington, D.C., Feb. 17, 2022); *Financial Management: DOD Needs to Implement Comprehensive Plans to Improve Its Systems Environment*, GAO-20-252 (Washington, D.C., Sept. 30, 2020).

social cash) or in a farmers' input support programme based on concerns that stakeholders have about that system.

In addition, in certain cases, a SAI may be limited in its ability to conduct aspects of a performance evaluation due to external factors such as the sensitivity of data in defense ministry information systems, if the SAI does not have access to such sensitive information.

2.3 Planning for the ISPE Audit

Planning for the audit includes determining the timing of the audit report, conducting a pre-study of the audit subject, identifying potential audit approaches, determining stakeholder involvement, and communicating with the audited entity.

2.3.1 Timing of the Audit Report

An important consideration when planning for the audit is determining when to perform the evaluation and issue the audit report. The timing of the audit work and resulting report may maximize the value of the evaluation and increase its impact on the audited entity and stakeholders. Determining when the audit report will be issued may also influence the time frames of the evaluation.

In a survey administered in preparation for this guide, most of the SAIs stated that they perform IS evaluations during post-implementation of the system/IT solution (15 of 24 respondents) or as the systems/IT solutions are being implemented (10 of 24 respondents). Others responded that they performed the evaluations approximately three years after the system/IT solution has been implemented or more than three years after the system/IT solution has been implemented (6 respondents).[26]

Auditors should use professional judgement to determine the appropriate timing of an audit report based on their understanding of identified concerns, timing of key system-related activities, and other external factors. As an example, if auditors identify issues of immediate concern, they might consider issuing a smaller-scope report before completing the evaluation and issuing a more comprehensive report at the conclusion of the evaluation. This approach may help to address the immediate issues before they become more significant problems. As another example, if an implemented system is not meeting its intended goals and will be deployed to additional sites, the audit team may issue an audit report before the system begins this expansion. Further, if legislators plan to develop a bill to include provisions related to audit

[26] SAI responses to survey for Preparation of Guidance on Performance Evaluation of Information Systems

findings, the audit team might consider timing the issuance of a report so it can inform these legislative deliberations.

The timing of the audit report also introduces the potential for risk. For example, if a report is otherwise unbiased but published at a time that could be perceived as favoring a particular political entity, it might raise concerns about why the SAI decided to publish the report at that time.

2.3.2 Pre-study of the Audit Subject (i.e., System)

Conducting a pre-study of the audit subject helps ensure that the audit is properly designed and helps establish whether conditions for a successful audit exist. The goals of conducting a pre-study of the audit subject are to inform audit planning and help ensure that the auditor acquires sufficient knowledge of the audited program or audited entity's business before the team begins detailed audit work.[27] In addition, as discussed subsequently in this guide, the audit organization should use the audit pre-study to inform initial decisions about staff resources needed to perform the audit.[28] Therefore, before starting detailed audit work, it is generally necessary to conduct research to build knowledge, consider various audit designs, and determine whether the necessary data are available.

During the pre-study of an ISPE exercise, auditors should gather information on the audit subject and the audited entities' business and determine whether the audit is expected to add value to the audited entity (e.g., enhance the audit subject's economy, efficiency and effectiveness by reinforcing internal controls, and determine the risk for fraud, waste, and abuse). Collecting preliminary information about the information system can help auditors understand any performance weaknesses of the IS.

As part of the pre-study, auditors should develop an understanding of the system architecture, the underlying data, and the sources of the system's underlying data to identify the required audit tools and techniques. In addition, the auditor should also draw out the linkages between different business operations being carried out through the IS solution(s). Based on this understanding of the IS, auditors can then determine potential approaches for the audit (the identification of audit approaches is discussed in greater detail later in this chapter).[29]

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

[28] See section 2.4.2, Audit Resources

[29] 2022 IDI Handbook

Collecting additional information enables the audit team to understand the organizational structures, organizational goals, internal controls, internal and external environmental factors, external constraints, and pre-existing criteria or criteria that the audit team needs to develop. In addition, collecting this information allows the auditor to develop a concrete understanding of the audit subject to properly assess and identify any issues.

Performance metrics can provide a useful source of information for IS evaluations. Examples of such metrics include:

- Quantitative data (e.g., return on investment or reduced operating expenses)
- Intangible benefits (e.g., improved decision making or added flexibility)
- Status of development and procurement (e.g., compliance to systems development standards for program design, database design, or testing)
- Status of use and operations (e.g., stakeholder satisfaction or compliance with application control standards)
- Risk mitigation (e.g., the number and severity of risks identified and addressed over time)
- Status of efforts to achieve program goals (e.g., metrics that assess whether the system is achieving outcome, product, or output objectives)[30]

It is also important to consider the sources of the information the audit team will use to collect information for pre-study. Information sources can include the audited entity (e.g., strategic or corporate plans, mission statements, annual reports, corporate policies and guidance), information system management and staff (e.g., system-level policies and guidance, performance reports, and interviews), and external sources (e.g., legislation, inspector general reports, and other external reports). While this information can be collected during audit execution, collecting it during the pre-study helps to inform audit planning.

Finally, as discussed in greater detail later in this guide, the pre-study is a good time to discuss information about the IS with internal and external stakeholders. This might include discussing related audit reports with internal stakeholders or discussing other reports and observations with external stakeholders.

[30] SAI responses to survey for Preparation of Guidance on Performance Evaluation of Information Systems

2.3.3 Identifying Potential Audit Approaches for ISPE

The standard for identifying potential audit approaches is that auditors should choose a result, problem, or system-oriented audit approach, or a combination of those.[31] These approaches are defined as follows:

i. **Result-oriented:** A result-oriented audit approach assesses whether an outcome or output objectives have been achieved or services are operating as designed.

ii. **Problem-oriented:** A problem-oriented audit approach typically starts with a preliminary problem. This approach places a special emphasis on examining, verifying, and analysing the cause of performance problems.

iii. **System-oriented:** A system-oriented audit approach examines the proper functioning of management systems. For this approach, performance benchmarks and principles of good IS management will be helpful criteria. It is important to identify weaknesses on performance of system and establish how weaknesses affect operations.

To select an approach, auditors should obtain an understanding of the organization, identify key system controls that might facilitate detailed audit planning, and consider potential resource and staff allocation to ensure that the audit team is composed of members that have the competence to conduct the audit. For example, auditors should consider the number of staff that might be available to support the audit and their relative levels of knowledge and experience. Auditors should also consider potential needs for subject matter expertise and their potential availability.

Evaluating the performance of an information system may focus on a combination of the three approaches. For example, the audit may seek to determine the extent to which a program is achieving its defined outcomes or contributing to larger organization-level outcomes. The audit may also focus on known performance problems and reasons for the performance problems. In addition, there may be elements of the audit focused on how the system is functioning or how it was developed and the extent to which system-related issues are contributing to performance issues or concerns. The type of approach selected influences the criteria selection. Considerations for selecting criteria are discussed in greater detail in section 2.7.

[31] IDI Performance Audit Handbook, p. 85

2.3.4 Stakeholder Involvement

When planning the audit, it is important to identify internal and external stakeholders and determine their roles and responsibilities, which may change throughout the audit.

- **Internal stakeholders:** At the time of the pre-study, the audit team may hold an initial meeting with internal stakeholders such as attorneys, methodologists, and technical experts. For example, internal stakeholders may advise the audit team on the audit approach or review and comment on draft audit reports. They might also be more involved in audit activities. For example, stakeholders might develop targeted analyses or draft audit products based on their areas of expertise (e.g., cost, schedule, or software development approaches). They might also provide staff that work as part of the audit team on a day-to-day basis.
- **External stakeholders:** Examples of external stakeholders include Parliamentary bodies, academic and business communities, research institutions, and legal experts not within the SAI. Typically, external stakeholders play different roles, such as providing advice/direction, providing input, or reviewing draft audit products, as appropriate. Without engaging internal and external stakeholders early and identifying their levels of contribution, the audit team risks the stakeholders being unavailable to contribute as anticipated. As a result, the team might miss opportunities for valuable context, input, insight, and analysis. In addition, audit timeframes might be delayed or stakeholder input might be rushed.

As the audit team begins to work with internal and external stakeholders, it is important to safeguard against threats associated with real or perceived bias, including financial or other potential conflicts of interest. Identifying potential threats to stakeholder independence is important for ensuring the integrity and objectivity of the audit. If new threats to independence arise, either real or perceived, internal and external stakeholders should disclose these to the audit team. The team should consult with its general counsel to determine if a threat to a stakeholder’s independence poses too much of a risk to that particular assignment.

2.3.5 Communication with the Audited Entity

The audit team should also plan to maintain effective communication with the audited entity. In the early audit stages, the audit team and audited entity should agree on communication protocols.[32] Different ways to communicate with the audited entity include face-to-face

[32] See, for example, GAO, *GAO's Agency Protocols (Updated January 23, 2019)*, GAO-19-55G. (Washington, D.C., Nov. 19, 2018).

meetings with officials, teleconference or videoconference meetings, letters, and emails. Auditors should plan to meet with the audited entity during key audit milestones, which may include an initiation or entrance meeting, working meetings, and meetings to communicate audit findings. While communicating with the audited entity, auditors should maintain professionalism and independence. The use of audit liaisons can facilitate communication between the audit teams and audited agencies. These liaisons can also assist with scheduling and organizing meetings, answering certain questions, and mediating between entities if conflict arises.

2.4 Designing the ISPE Audit

When designing an audit, the team needs to take steps to ensure the resulting report is unbiased and impactful. Audit design begins with identifying and assessing common areas of risk and mitigating any identified risks. In addition, staff assigned to the audit need to meet competencies expected by the SAI and have proper expertise to effectively carry out research and analysis on information systems. Establishing a time frame and milestones for completing the audit helps mitigate fraud, waste, and abuse by encouraging the audit team to complete the audit in a timely fashion. In addition, defining the audit’s scope and objectives helps to ensure a common understanding of the audit’s subject, focus, and boundaries. Auditors also need to plan for the methodology they will use, including selecting appropriate criteria and information sources.

2.4.1 Audit Risks

Identifying and addressing risks is a crucial preliminary step for conducting an audit. The audit team may need to accept some level of risk, but the team should identify controls to minimize the impact of the accepted risk. Risk should also be continuously evaluated throughout the audit life cycle so that adjustments can be made to ensure that the potential impact of risk remains low.[33]

Risks that audit teams should consider when designing the evaluations of the performance of information systems include:

- Potential for non-identification and sampling of key IT IS processes
- Potential for non-achievement of key business goals / objectives
- Potential for fraud
- Restricted and non-access to the critical system / processes

[33] GAO, *Agile Assessment Guide: Best Practices for Agile Adoption and Implementation* (GAO-20-590G), (Washington, D.C Sept. 2020).

- Risk of inadequate understanding of IS control environment
- Potential access to and sensitivity of records
- Available staffing and institutional expertise
- Available funds for travel
- Availability of appropriate audit methodologies
- Potential for complex, sensitive, or controversial issues
- Potential for unclear objectives
- Potential impact on the audit's reliability due to dependencies on external vendors or third-party services

After identifying risks, the audit team should identify approaches for mitigating them. For example, the team should document identified risks, involve appropriate stakeholders (e.g., attorneys), and document how it plans to mitigate the identified risks.

The potential impacts of overlooking key risks include difficulty in obtaining quality information; omitting relevant information or arguments; reaching incorrect or incomplete conclusions; providing limited added value for users at the end of the audit; engaging in practices that raise questions of fraud, waste, or abuse; or encountering political sensitivities.[34]

The U.S. Government Accountability Office's assessment of the U.S. Citizen and Immigration Services Transformation program provides one example of how an audit team has addressed risk early in an assessment of an IT system.[35] This audit included an in-depth assessment of the program's Agile software development practices. Because programs using Agile may approach their software development efforts in various ways, different criteria might be applicable for different programs. To limit the risk of using inappropriate criteria, the audit team took steps to understand how the audited entity was approaching Agile software development. Specifically, the audit team performed on-site observations of the agency's software development approach over a 3-week period. During these observations, the team attended development team meetings, including sprint planning and sprint review sessions, daily stand-ups, cross-team meetings, and a user story demonstration. The team also documented program planning artifacts posted on the walls of team common areas and individual team rooms. Different programs may use different approaches to Agile software development. These

[34] 2021 IDI Handbook, Pg 106

[35] GAO, *Immigration Benefits System: U.S. Citizenship and Immigration Services Can Improve Program Management*, GAO-16-467. (Washington, D.C., July 7, 2016).

different approaches may impact the appropriateness of potential criteria. By compiling its observations and noting potential issues, the team was able to obtain a better understanding of the program's Agile software development approach.

2.4.2 Audit Resources

The audit organization should use the audit pre-study to inform initial decisions about staff resources needed to perform the audit. This includes ensuring that the team has the appropriate number of available staff who have the competence, expertise, and independence needed to support the audit. As the audit progresses, the audit organization and audit team should re-evaluate decisions about staffing as the audit progresses and make adjustments as needed to ensure that staff assigned to the audit are aligned with planned work and needed resources.

- **Auditor competence**: Auditors need to exhibit a level of competence to make sure they can appropriately support the audit. SAIs need to communicate to auditors what competencies they are expected to hold themselves to so that auditors can either be evaluated or self-evaluate themselves and show they are meeting requirements set at the organizational level.[36] Auditor competence may include expectations for managing work effectively and independently, producing quality work products, and working effectively in a team environment.
- **Auditor expertise**: Auditors should also have an appropriate level of expertise for conducting an audit of an IT system. This may be demonstrated by SAI-level expectations for training or certifications in IT-related fields. In addition, if an audit team plans to focus on a specific aspect of an IT system, the team needs to ensure that staff have the requisite skills and abilities. For example, team members may need to supplement existing expertise with targeted training. This might include obtaining training and/or certifications in topics such as cost and schedule estimation, Agile software development, information security, or other relevant topics.[37]
- **Auditor independence**: The SAIs should ensure available staff are independent. Individual auditors may be the only ones able to identify certain risks, such as financial commitments, familial bonds, or political bias that may result in actual or perceived conflicts of interest. For example, auditors need to avoid having, or having the appearance of, relationships with an organization (e.g., recent employment at the

[36] Auditor Competence Guide: 10

[37] Relevant certifications might include certifications in areas such as cost and schedule estimation, Agile software development, and information security.

audited entity) that could cast doubt on their ability to perform an unbiased audit.[38] If there is a chance of a real or perceived conflict of interest, the SAI should consult appropriate entities (e.g., general counsel) to discuss the potential conflict. Individuals who may have real or perceived conflicts of interest should be reassigned to other audits.

2.4.3 Audit Timeframes

After completing a pre-study, the audit team should develop target dates for audit milestones to monitor audit progress. These milestones will also help guide the audit methodology and give auditors expectations to strive for once the audit has started. For example, key milestones may include confirming the proposed audit methodology, developing a preliminary audit message, and developing a draft report for SAI management review.

2.5 Audit Objectives, Scope and Methodology

Identifying the audit's objectives, scope, and methodology is critical to ensuring that the audit's subject, focus, and boundaries are well-understood. This is critical to identifying the resources that are required to respond to the audit and keeping the audit team focused on developing a concise audit report in a timely manner.

The objectives determine the type of engagement to be conducted and the applicable standards to be followed. In general, audit objectives for ISPE may vary widely and include assessments of program effectiveness, economy, and efficiency; internal control; compliance; and prospective analyses. Audit objectives may also pertain to the current status or condition of a program. These overall objectives are not mutually exclusive. For example, a performance evaluation with an objective of determining or evaluating program effectiveness may also involve an additional objective of evaluating the program's internal controls.[39] Further details on objectives with respect to ISPE have been highlighted earlier at Para 1.7.3, which may be referred to.

The scope defines the boundary of the audit and is directly tied to the audit objectives. The scope defines the subject matter that the auditors will assess and report on, such as a particular system or aspect of a system, the necessary documents or records, the period of time reviewed, and the locations that will be included.[40]

[38] IDI Handbook page 32

[39] GAO-21-368G.

[40] GAO, Government Auditing Standards: 2018 Revision Technical Update April 2021 (Supersedes GAO-18-568G), GAO-21-368G (Washington, D.C., Apr 14, 2021).

Initial considerations for the audit methodology include identifying appropriate criteria and selecting appropriate data and information sources. This may involve building a broad IS environment canvas and developing its review approaches in a systematic fashion subsequently. At this early stage of the assessment, teams are exploring potential audit approaches and collecting information to inform initial decisions. Considerations for selecting appropriate information sources are discussed in greater detail in section 2.11. Chapter 3 of this guide discusses specific criteria and approaches that might be applicable to specific types of evaluations in greater detail.

SAIs may revisit the initial audit objectives, scope, and methodology throughout the engagement, based on ongoing audit findings. However, auditors should be aware that changes may have significant impacts on audit plans and timeframes.

2.6 Criteria Selection

The difference between an exploratory audit and a ISPE is the use of criteria, meaning the selection of criteria is a key part of planning the audit. The criteria documents an ideal state of an organization, against which the reality of the organization can be measured. The criteria provide a basis for evaluating the evidence, developing audit findings, and reaching conclusions on the audit objectives. They also form an important element in discussions within the audit team and with SAI management and in communication with the audited entities.

Auditors should identify suitable criteria that correspond to the audit questions and objectives for the performance evaluation and may include but not be limited to the principles of economy, efficiency, and effectiveness.

The criteria can be qualitative or quantitative and should define what the audited entity will be assessed against. The criteria may be general or specific, focusing on what should be (according to laws, regulations, or objectives), what is expected (according to sound principles, scientific knowledge and best practice), or what could be (given better conditions).

Diverse sources can be used to identify criteria, including performance measurement frameworks. Auditors should disclose the sources for the criteria and ensure criteria are relevant and understandable for users. Additionally, user confidence in the findings and conclusions of a performance audit depends largely on the criteria. Thus, it is crucial to select criteria that are complete, reliable, and objective in the context of the subject matter and audit objectives.

In order for the ISPE to produce meaningful and accurate results, the criteria used must be appropriate for the audited entity. In addition, the audited agency should be made aware of the criteria. Although the criteria should be discussed with the audited entities, it is ultimately the auditor's responsibility to select / formulate suitable criteria. While defining and communicating criteria during the planning phase may enhance their reliability and general acceptance, in audits covering complex issues it is not always possible to set criteria in advance. Instead, the criteria may be defined during the audit process. [41] Risk and impact considerations viz-a-viz IT processes may also aid in development of suitable criterion.

Whereas in some audit types there are unequivocal criteria, this is not typically the case in performance evaluation. The performance evaluation objectives, questions, and approach determine the relevance and the type of suitable criteria. In a problem-oriented performance evaluation, the starting point is a known or suspected deviation from what should or could be. The main objective, however, is not just to verify the problem (the deviation from the criterion and its consequences) but to identify causes. This makes it important to decide how to examine and verify causes during the design phase. Conclusions and recommendations are primarily based on the process of analyzing and confirming causes, even though they are always rooted in normative criteria. Some examples of criteria include the following:

- Laws and regulations that are applicable the audited agency
- Goals, policies, and procedures established by the audited agency[42]
- Technically-developed standards or norms[43]
- Provisions of contracts or grant agreements that are significant within the context of the audit objectives
- Applicable internal controls[44]
- Guidance from oversight agencies[45]
- Reports published by government advisory entities, as appropriate[46]

[41] ISSAI 300 -27

[42] For example, Department of Defense, *Business Systems Requirements and Acquisition, Instruction 5000.75* (incorporating change 2 [Jan. 24, 2020]) (Washington, D.C.: Feb. 2, 2017).

[43] International Organization of Supreme Audit Institutions, *GUID 3910: Central Concepts for Performance Auditing* (2019).

[44] See, for example, GAO, Standards for Internal Control in the Federal Government, GAO-14-704G. (Washington, D.C., Sep 10, 2014).

[45] See, for example, OMB, FY22 Capital Planning Guidance. (Washington, D.C. Nov. 16, 2020).

[46] See, for example, Defense Science Board, Report of the Defense Science Board Task Force on the Design and Acquisition of Software for Defense Systems. (Washington, D.C. Feb. 14, 2018).

- Relevant best or leading practices[47]

Furthermore, under an ISPE criterion identification or formulation may include the assessment of adequacy levels for the IS under review.

2.7 Selecting Appropriate Data and Information Sources

When selecting evidence to be used for analysis, an auditor must consider the sufficiency and appropriateness of the evidence collected. In order to be sufficient, there needs to be enough evidence that a knowledgeable person would be persuaded that the findings are reasonable. The appropriateness of the evidence is determined by its relevancy, validity, and reliability. When the evidence collected is both sufficient and appropriate, the auditor has a strong starting point from which to begin an analysis and produce well-supported findings.[48]

Evidence that might be useful for assessing the performance of an information system includes the following:

- Information collected from public-facing government sources, such as dashboards and reports[49]
- Documentary evidence in the form of policy or guidance
- Observations made by auditors during site visits
- Evidence collected while performing cybersecurity tests or other analyses of an agency's systems.
- Testimonial evidence collected from knowledgeable government officials in responses to questionnaires or statements made during interviews

It is useful for auditors to request key documentation and information at the beginning of audit design to help the audit team obtain a more comprehensive understanding of the information system. Table 1 provides examples of what such documentation and information might include.

Table 1: Documentation and Information an Audit Team Might Request During Initial Audit Design

Document/Information	Description
Organization chart and contact information	Description of and contact information for system leadership and external leadership with responsibility over system activities

[47] GAO, Agile Assessment Guide: Best Practices for Agile Adoption and Implementation (GAO-20-590G), (Washington, D.C Sept. 2020).

[48] 2021 IDI Handbook, Pg. 118.

[49] One example of this is the United States government's Federal IT Dashboard, which provides information about portfolios of IT investments as well as individual investments across the federal government. See https://www.itdashboard.gov/

Systems inventory / computer network diagram / systems architecture	Description of systems and applications, their relationships, and associated business functions
System development life cycle methodology	A document that describes the approach management is using to develop the system
Decision memoranda	Documentation describing the rationale for decisions made at key system development milestones (e.g., approval for the system to proceed into development)
Concept of operations or operational concept	A document used to communicate overall quantitative and qualitative system characteristics to the user, developer, and other organizational elements
Business case or budget request	Documentation that describes the rationale for developing a system and the annual funds requested. These may be combined or developed as separate sets of documentation.
Initial and current system baseline	Initial and current versions of the system's documented and approved cost, schedule, and performance expectations.
Entity Performance Parameters	KPIs established by the entity for review of its business operations and / or information systems.
Project plan	A document that describes planned activities and associated time frames
Recent status review reports	Recent internal briefings on how the system is progressing towards cost, schedule, and performance expectations
Risk management plan	A plan that describes how management intends to identify, track, and mitigate system risks
Risk register	A document that describes the status of identified system risks
Capability implementation plan	A document or set of documents used to prepare for and manage the delivery of the system's capability and to support statutory and regulatory requirements
Test strategy	A strategy that defines how capabilities will be tested and evaluated to satisfy criteria and demonstrate operational effectiveness
Results of computer security tests or audits	Recent results of tests or audits describing identified vulnerabilities or weaknesses

Source: WGITA

Note: Different organizations may use different names when referring to these documents and all organizations might not require systems to develop these documents. In addition, elements of some documentation identified above may be combined into different documents. For example, the business case may include information about the organization and key contacts.

If auditors know they will likely focus on specific aspects of the system during this early stage, they may also request additional documentation associated with that specific topic. For example, when the U.S. Government Accountability Office assessed the reliability of cost estimates for the Federal Emergency Management Agency's Grants Management Modernization program, the audit team collected documentation supporting the program's life cycle cost estimate.[11] This documentation included the cost estimating model, a report on the program's cost estimating baseline document and life cycle cost estimate, and briefings provided to Department of Homeland Security and Federal Emergency Management Agency management regarding the cost estimate. The team also interviewed program officials responsible for developing and reviewing the cost estimate to understand their methodology, data, and approach for developing the estimate.

After designing an audit with these factors in mind, an audit team is ready to begin its detailed audit work.

CHAPTER 03

Audit Execution and Best Practices

3.1 Introduction

This Chapter will cover guidance on:

- As elaborated in Chapter-01 & 02, various approaches and allied aspects can be adopted for undertaking an ISPE. In this chapter as a way of illustration, an ISPE is elaborated along the dimensions of time, cost, and functionality.
- Best practices from case studies on audit engagements where such performance evaluation has previously been carried out.

3.2 Project Management Analysis for implementation of the Information System

This section will cover guidance on conducting ISPE on the time dimension in context of IS project implementation. The objective is to assess whether the information system being evaluated has been implemented within the scheduled timelines and whether the audited entity has adopted adequate and effective internal controls to mitigate the risk of delays in implementation of the IS.

3.2.1 Steps in conducting Project Management Analysis

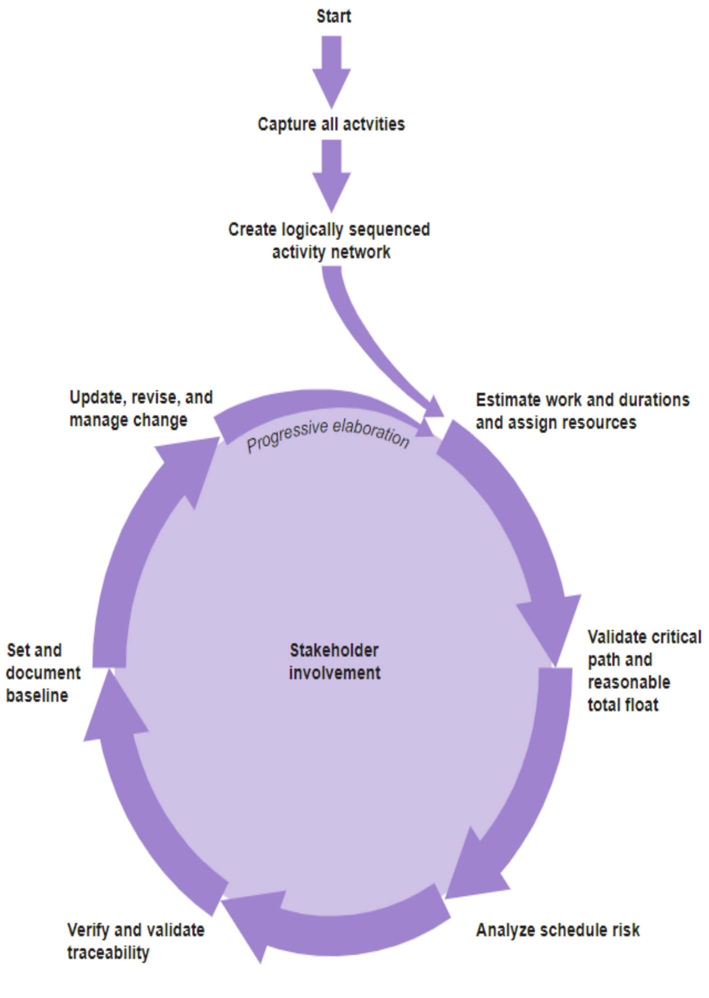
Analysis of the project management function is critical for information system performance evaluation projects which have remained at the implementation stage for extended periods of time and have exceeded their scheduled timelines for completion. This analysis could also be relevant for those IS projects which have been successfully completed but with significant time overruns, in order to evaluate the performance by determining the specific reasons for the delays. Project Management Analysis may be conducted by Auditors by verification as to whether the audited entity has taken the following steps:[50]

1. Comprehensive enumeration of individual tasks in the IS project
2. Estimation of time required for each individual task
3. Assignment of each task to a specific individual project team member
4. Identification of sequential dependencies among the tasks
5. Identification of the critical path for the IS project
6. Alignment of the overall scheduled timelines with the timelines determined for the critical path for the IS project

[50] Adapted from US GAO Schedule Assessment Guide- https://gaoinnovations.gov/schedule-guide/

7. Conduct of periodic reviews and revision of scheduled timelines to reflect true and fair view, based on the remainder of tasks on the critical path to be completed.

The broad framework for the steps above may be represented as follows-


Start
Capture all actvities
Create logically sequenced activity network
Estimate work and durations and assign resources
Validate critical path and reasonable total float
Analyze schedule risk
Verify and validate traceability
Set and document baseline
Update, revise, and manage change
Progressive elaboration
Stakeholder involvement

Source: Adapted from Keith D. Hornbacher. | GAO-16-89G

3.2.1.1 Comprehensive enumeration of individual tasks in the IS Project

Objective:

To determine whether the audited entity has clearly defined the exact and complete scope of the IS project. The individual tasks which are each required to be completed to achieve project completion have to be listed out, at an appropriate level of granularity.

The definition of level of granularity for tasks is the prerogative of the audited entity. The risk in this process is that instead of individually defined tasks, only broad milestones/ project phases have been defined.

Establishing a Work Breakdown Structure (WBS) is the key control for ensuring appropriate level of granularity. A WBS deconstructs the overall project work into successively greater levels of detail until the work is subdivided to a level suitable for management control. By breaking work down into smaller elements, management can more easily plan and schedule the program's activities and assign responsibility for the work. It is also essential for establishing a reliable schedule baseline.

The definition of granularity for each task at the base level should be based on the following considerations:

- The duration of each activity should be as short as possible to facilitate the objective measurement of accomplished effort.
- The scope of work/ effort involved in each task should be the full-time work assigned to the primary project team member who will be assigned that task.

Risk which should have been mitigated by the audited entity:

Incomplete listing of project tasks or insufficient level of granularity may result in the risk of unforeseen delays due to time required for the tasks which have been erroneously excluded or not clearly defined in terms of scope of work, from the list. Further it may also result in system not being developed as per envisaged scope and extent.

3.2.1.2 Estimation of time required for each individual task

Objective:

To determine whether the time required for completion of each task has been estimated on a reasonable basis, with due justification on record for tasks which have been allotted significant time durations.

Risk which should have been mitigated by the audited entity:

Inaccurate estimation of time required for completion of tasks may result in longer duration of time being necessary to complete tasks which had been allotted shorter time durations.

3.2.1.3 Assignment of each task to a specific individual project team

Objective:

To examine whether assignment of each task to individual project team members has been carried out, in order to enable clarity on responsibility for each task.

Risk which should have been mitigated by the audited entity:

Lack of clarity on task ownership may result in avoidable delays in assignment to suitable human resources and commencement of tasks.

3.2.1.4 Identification of sequential dependencies among the tasks

Objective:

To verify whether sequential dependencies[51] among each of the IS project tasks have been identified (e.g., in some cases, User Acceptance Testing for a module may only commence after completion of the Product Integration Testing for that module).

Risk which should have been mitigated by the audited entity:

Lack of identification of sequential dependencies may result in unconnected and stand-alone tasks whose completion is not factored into the overall timelines for completion of the project.

3.2.1.5 Identification of the critical path for the IS project

Objective:

To verify whether the critical path for completion of the project has been established, with clear identification of the tasks which are part of the critical path, as well as determination of the maximum slacks available for tasks which are not part of the critical path.

Risk which should have been mitigated by the audited entity:

Lack of identification of the critical path for the project results in the significant and material risk that the timelines for completion of the project as a whole may be inaccurate.

[51] Adapted from UN National Audit Office, Delivery Environment Complexity Analytic, p. 33- https://www.nao.org.uk/wp-content/uploads/2013/10/10251-001-DECA-Guidance_web-final.pdf

3.2.1.6 Alignment of overall scheduled timelines with the timelines determined for the critical path for the IS project

Objective:

To verify whether the overall scheduled timelines for project implementation have been estimated based on the overall duration of the time allotted for the tasks which are part of the critical path.

Risk which should have been mitigated by the audited entity:

Lack of alignment of the overall project timelines with the timelines for completion of tasks on the critical path results in a material risk of inaccurate estimation of the scheduled timelines.

3.2.1.7 Conduct of periodic reviews and revision of scheduled timelines reflect true and fair view, based on the remainder of the tasks on the critical path to be completed

Objective:

To verify whether the periodicity of review of progress and reporting thereon to the governance entities has been clearly established, and that revised scheduled timelines have been accurately estimated at those periodic intervals, based on actual progress achieved in implementation of the project.

Risk which should have been mitigated by the audited entity:

Lack of periodic reviews and revisions to the scheduled timelines for project completion results in the material risk that there is a severe mismatch between the original scheduled timelines for completion and the timelines which can be realistically achieved, thus not reflecting a true and fair view of the progress made.

3.2.2 Adoption of appropriate technology for IS Project Management

In IS Project implementation, the use of appropriate Project Management technology by the audited entity is crucial for consistently monitoring the project tasks and generating progress reports for review by senior management at regular intervals.

Auditors should examine the adequacy of the Project Management tool/ software application used by the audited entity, on the basis of factors such as project scope, budget, scheduled duration, complexity of functions, and number of personnel involved.

Absence of utilization of appropriate project management technology tools and associated management information system reports, ranging from very basic and generic office productivity suite software applications to advanced Enterprise Resource Planning systems, may indicate significant risks to achieving the scheduled timelines.

3.2.3 Formal identification and mitigation of risks

Auditors may examine whether the audited entity has maintained an updated risk register/inventory wherein all potential risks arising during IS project implementation have been identified, measured (in terms of both probability of occurrence as well as impact on timelines and cost), and prioritized.

Once all potential risks have been identified, Auditors may examine whether appropriate risk mitigation actions have been identified and assigned to project team members, for each identified risk.

3.2.4 Resolution of time constraints

Auditors may examine whether the audited entity has, at periodic intervals, reviewed individual tasks which have exceeded the timelines for their completion and taken necessary steps to resolve the underlying constraints/ reasons for such overruns. In cases where the resolution could not be achieved as intended, Auditors may examine whether the underlying constraints/reasons are formally documented in the risk register/inventory and if an assignment of appropriate priority and reporting to governance entities was ensured.

3.2.5 Periodic review of progress achieved

Auditors may examine whether in cases of delays in completion of tasks which are not part of the critical path, the governance entities have reviewed the risk of the maximum slacks being exceeded and initiated mitigation actions to achieve the overall project timelines. In cases of delays in completion of tasks which are part of the critical path, auditors may examine whether the governance entities have reviewed the impact on the overall project timelines and accordingly revised the scheduled timelines to reflect a true and fair view of timelines for completion.

In summary, systematic Project Management Analysis enables Auditors to conduct IS performance evaluations on the time dimension. It is essential that this analysis is carried out with due diligence, in order to derive assurance that the audited entity has adopted adequate and effective internal controls to mitigate the risk of time overruns during IS project implementation.

3.3 Cost-Benefits Analysis for the Information System

This section will cover guidance on conducting ISPE on the cost dimension in context of IS project implementation. The objective is to assess whether the information system(s) / programme(s) being evaluated has been implemented within the budgeted costs, as well as to assess whether the benefits accrued from the use of the information system outweigh the life-cycle costs across the design, development, testing, deployment, operations and maintenance phases of the information system.

On the cost dimension, the standard processes which may be examined by Auditors include the following:

3.3.1 Steps in conducting Cost Benefits Analysis

This analysis is critical for the evaluation of information systems which have been implemented by the audited entities with the expectations of containment of life-cycle costs at previously estimated limits and accrual of life-cycle benefits which exceed such costs. The net-positive impact from the information system would usually be the main factors highlighted in the project proposal for implementation of the information system, and also be the main justification for investment of budgetary resources at the time of the project approval decision.

It may also be pertinent to highlight here that the benefits in the public sector may not always be quantifiable in financial terms. Social benefits and other initiatives based on political mandates would have to be considered irrespective of financial viability. In such cases, the benefits from delivery of IT services would need to be taken into account and quantified to offset any shortcomings in the financial net present value of an IS project / programme.

Traditional Cost Benefits Analysis may be conducted with the following steps:

i. Definition of the useful life of the information system

ii. Comprehensive estimation of Total Cost of Ownership[52]

[52] Adapted from US GAO Cost Estimating and Assessment Guide- https://gaoinnovations.gov/cost-guide/

iii. Comprehensive estimation of Benefits Realization[53]

3.3.1.1 Definition of the useful life of the information system

Objective:

To ensure that there is clarity on the estimated useful life of the information system, since the costs and benefits would also have to in turn be estimated over that period of time. The useful life of the information system is typically considered to be 15 years for ERP systems and lower for other domain-specific information systems.

Factors such as pace of technology obsolescence in the business domain of the audited entity, extent of acceptable dependence on the software provider, nature of software (proprietary or open-source), interfaces with other software applications in the eco-system of the audited entity, as well as inter-operability with its broader IT environment and concerns over data security should be considered, in deciding upon the definition of the useful life of the information system.

Risk which should have been mitigated by the audited entity:

Inaccurate estimation of the useful life of the information system may result in premature obsolescence, excessive dependence on the software provider, forced upgrades/replacement to maintain compatibility with other software applications in the eco-system of the audited entity / broader IT environment, and unforeseen replacement requirements, all of which could significantly increase life-cycle costs and far outweigh any potential benefits to the audited entity, from the information system.

3.3.1.2 Comprehensive estimation of the Total Cost of Ownership

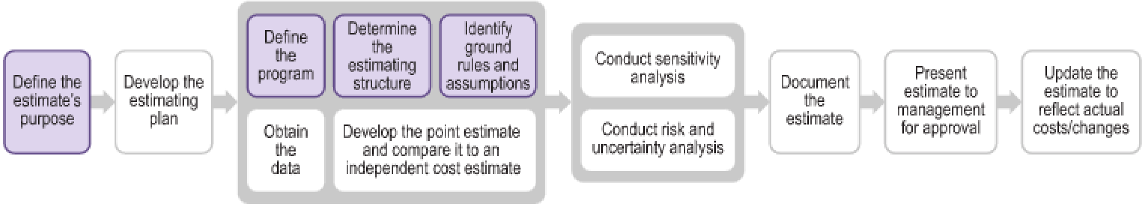
Objective:

To examine whether the audited entity has undertaken the following steps as part of its cost estimation function, prior to commencement of the IS project implementation:

i. Total Cost of Ownership (TCO), i.e., a comprehensive assessment of information technology (IT) or other costs across enterprise boundaries

[53] Adapted from United Nations Board of Auditors- Ninth annual progress report on the implementation of the United Nations enterprise resource planning system, p. 37- https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/184/36/PDF/N2018436.pdf

over time has been estimated, including hardware and software acquisition, management and support, communications, end-user expenses and the opportunity cost of downtime, training and other productivity losses. Auditors should assess the reliability of a cost estimate by evaluating the extent to which the audited entity has followed the steps below in preparation of cost estimates:


Define the estimate's purpose
Develop the estimating plan
Define the program
Determine the estimating structure
Identify ground rules and assumptions
Obtain the data
Develop the point estimate and compare it to an independent cost estimate
Conduct sensitivity analysis
Conduct risk and uncertainty analysis
Document the estimate
Present estimate to management for approval
Update the estimate to reflect actual costs/changes

Source: GAO. | GAO-20-195G

ii. The TCO has been estimated with inclusion of four broad categories of costs direct, indirect, training and maintenance.[54]

i. Direct costs constitute the expenses towards remuneration of project team members' pay and allowances, payments to the software implementing partner/ system integrator, and procurement of hardware and software.

ii. Indirect costs constitute the expenses towards change management, transition and temporary productivity losses arising from business process reengineering due to the IS and would need to be assessed by considering a uniform standard cost across all business process owners and considering an appropriate baseline for continuous improvements.

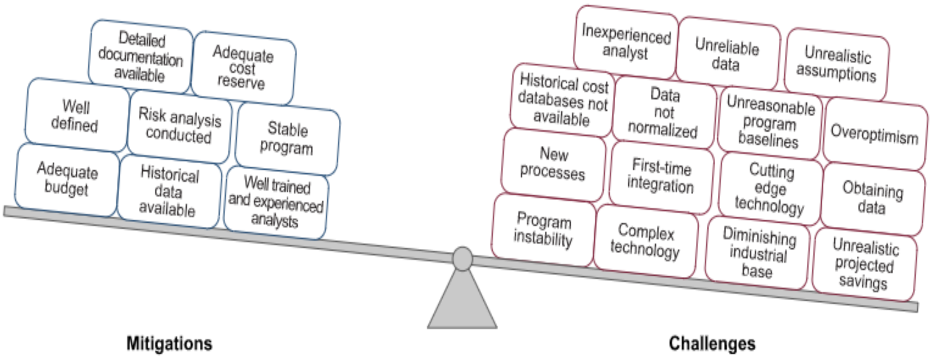
iii. Training costs would constitute the estimates for training existing personnel (in-person, virtual or self-learning modes) as well as new recruits during the useful life of the IS.

[54] Adapted from United Nations Board of Auditors- Ninth annual progress report on the implementation of the United Nations enterprise resource planning system, p. 37- https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/184/36/PDF/N2018436.pdf

iv. Maintenance costs would constitute expenses towards periodic replacement of hardware and software during the useful life, payments to the maintenance and operations partner, as well as expenses towards the system integrator implementing any significant changes that will be required to be IS based on foreseeable events that are expected to occur during the useful life.

Risk which should have been mitigated by the audited entity:

Incomplete enumeration of costs results in the material risk that the information system will not achieve its originally intended net-positive impact for the audited entity. Specifically, estimation of direct costs and training costs may be accurate over the useful life of the information system, but there is a significant risk that indirect costs and maintenance costs are under-estimated over the life-cycle of the information system, especially for periods beyond five years into the future. Absence of appropriate sensitivity analysis to assess the underlying assumptions that have been made, may result in material risks which may impact the TCO estimate.



Source: GAO. | GAO-20-195G

3.3.1.3 Comprehensive estimation of Benefits Realization

Objective:

To examine whether the audited entity has prepared a Benefits Realization plan, using a well-defined methodology to measure qualitative and quantitative benefits, which may be tangible or intangible, from the baseline adopted, along with the assumptions and processes underlying the benefits measurement process. These benefits may also include avoided costs, such as penalties or fines that will not be incurred in the future due to application controls adopted and time saved by personnel due to efficiency gains through process re-engineering.

Risk which should have been mitigated by the audited entity:

Excessively optimistic assumptions, over-estimation of process efficiencies that can be achieved, lack of a well-defined methodology to identify and measure qualitative benefits, unrealistic quantification of qualitative benefits, and lack of clarity in the Benefits Realization plan are some of the risks that may arise over the useful life of the information system, especially for periods beyond five years into the future. The intangible benefits such as enhanced goodwill, improved service delivery, etc. may be left out and not quantified.

3.3.2 Periodic review of progress of expenditure and benefits realized during IS project implementation

Auditors may examine whether periodicity of review of progress of expenditure on the IS and benefits realized from the IS and reporting thereon to the governance entities has been clearly established.

Absence of periodic review may indicate significant risks to ensuring that actual costs are contained within the budgeted estimates and to ensuring that there is sufficient accountability to realize the benefits that were to accrue to the audited entity from the implementation of the IS.

3.3.3 Resolution of cost constraints

Auditors may examine whether the audited entity has periodically reviewed the TCO estimate during IS project implementation and obtained necessary approvals from the governance entities with due justification, in case of material changes in the estimated costs. This would be crucial to ensure that the TCO estimate consistently provides a true and fair view, with adequate documentation to explain the reasons for revisions made.

3.3.4 Review of baseline for measurement of benefits to be realized

Auditors may examine whether the baseline / benchmark against which the benefits were proposed to be measured had been accurately defined and was supported by corroborative evidence. This is essential, in order to derive assurance that the baseline had not been understated. Auditors may examine the methodology adopted by the audited entity to measure qualitative and quantitative benefits (both tangible and non-tangible) from the baseline to derive assurance that the assumptions and processes underlying the benefits measurement process were reasonable and realistic, over the useful life of the IS.

3.3.5 Comparison of Costs and Benefits

Auditors may compare the estimates for TCO and the estimates for benefits realization, and identify the main reasons for:

- Determining that the IS offers net positive benefits to the audited entity compared to the TCO

  OR
- Determining that the IS does not offer net positive benefits to the audited entity compared to the TCO, due to either
  - Actual benefits that are being accrued falling short of the estimated benefits, due to either unrealistic assumptions or inaccurate measurement of benefits
  - TCO exceeding the actual benefits that are being accrued, due to incomplete and/ or inaccurate estimates of all categories of costs.

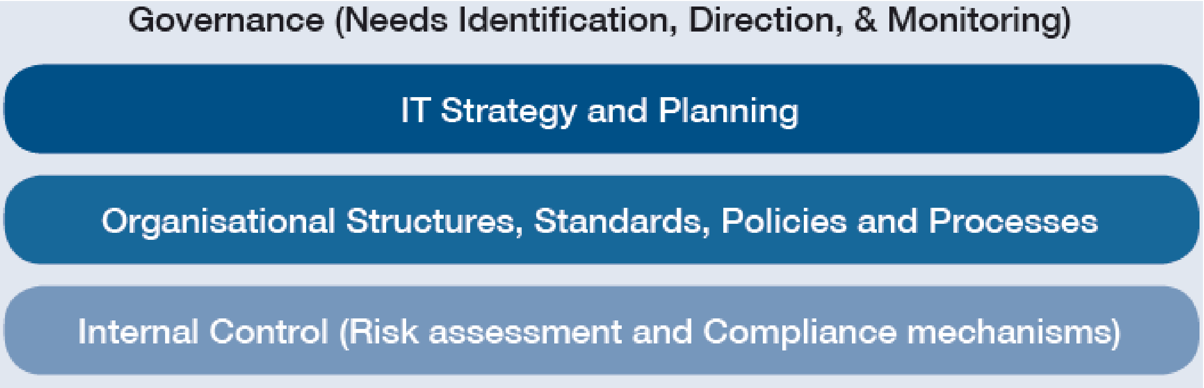
In summary, systematic Cost-Benefits Analysis enables Auditors to evaluate IS project implementation on the cost dimension. It is essential that this analysis is carried out with due diligence, in order to derive assurance that the audited entity has adopted adequate and effective internal controls to mitigate the risk of cost overruns during IS project implementation, and that the benefits realized from the information system outweigh the costs, over its complete lifecycle.

3.4 Evaluation of functionality of the information system

This Section will cover guidance on conducting ISPE with respect to functionality dimension. The objective is to assess whether the information system being evaluated has been functioning as intended by the audited entity. This may entail determining whether the IS is achieving its business objectives as well as its technical objectives. In addition, while some aspects of functionality discussed below are associated with IS controls addressed in greater detail in the IT Audit Handbook, they are also included here because of their potential impact on the overall performance of an individual IS. The evaluation of the functionality of the information system may be carried out on the following aspects:[55]

3.4.1 IS Governance

This section will cover guidance on conducting performance evaluation focused on the extent to which the IS conforms to key elements of IS governance. The objective is to assess whether the IS is aligned to and contributing to the overall strategic goals and objectives of the organization and the extent to which it conforms to key policies and processes and organizational internal controls. In this section, the system can be either an individual system or a portfolio of information systems. In addition, the organization can be defined as the entity specifically responsible for the information system or a higher-level entity such as a department or government as a whole. The same concept is introduced below.[56]


Governance (Needs Identification, Direction, & Monitoring)
IT Strategy and Planning
Organisational Structures, Standards, Policies and Processes
Internal Control (Risk assessment and Compliance mechanisms)

Source: Adapted from IDI INTOSAI Handbook on IT Audit

3.4.1.1 Steps in conducting an IS Governance Analysis

Analysis of the information systems' governance is important for determining the extent to which an information system is contributing to the overall organization's goals and objectives and conforms to other key elements of IS governance.[57] This analysis is important for ensuring that investments are effectively contributing to larger organizational goals and may involve individual information systems or portfolios of information systems. Steps that may be involved in an IS governance analysis include:

[55] IDI-INTOSAI Handbook on IT Audit- https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-english-version.pdf

[56] Adapted from COBIT 5 Framework and ISO 38500

[57] GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity* (Supersedes AIMD-10.1.23), GAO-04-394G (Washington, D.C., Mar. 1, 2004).

1. Evaluating the extent to which an IS is periodically assessed based on its alignment to broader missions, goals, and strategies and ability to deliver intended benefits.
2. Assess the IS on the basis of cost, schedule, performance, and risk.
3. Evaluate the IS relative to defined policies, standards, processes and mechanisms for monitoring compliance.
4. Assess the extent to which an IS's performance expectations are reevaluated on a periodic basis.

3.4.1.1.1. Evaluating IS selection based on alignment to organizational missions, goals, and strategies and ability to deliver benefits

Objective:

To determine the extent to which an IS is periodically evaluated based on its alignment to broader missions, goals, and strategies and ability to deliver intended benefits.

An organization should periodically reassess an IS's continued strategic alignment to organizational mission, goals, strategies, and priorities, as well as its ability to deliver on its performance expectations and deliver intended benefits. In some cases, this may result in an IS being identified as a candidate for retirement. Such periodic evaluations may also consider the extent to which an IS's underlying technology is consistent with emerging technologies and potential successor ISs.

Risk which should have been mitigated by the audited entity:

If an organization has not established a process and criteria for reassessing ISs, an IS may continue to operate well beyond the time that it is delivering intended benefits or meeting the need of the organization. Also, if an organization has not identified its broader mission, goals, and strategies in a strategic plan or IT strategic plan, it risks not having the information needed to conduct such an assessment.

3.4.1.1.2. Assessing the IS on the basis of cost, schedule, performance, and risk

Objective:

To periodically assess the IS on the basis of cost, schedule, performance, and risk

An organization should periodically evaluate an IS on the basis of its ability to achieve its cost, schedule, and performance outcomes and its identified risks.[58]

[58] IDI-INTOSAI Handbook on IT Audit- https://www.intosaicommunity.net/wgita/wp-content/uploads/2018/04/it-audit-handbook-english-version.pdf

• Cost may include life cycle costs broken apart into initial costs, ongoing development costs, and indirect costs.

• Schedule may include the life cycle schedule and the schedule of benefits.

• Benefit may include tangible benefits and intangible benefits estimated using a variety of techniques (e.g., cost/benefit analyses using net present value, return on investment calculations).

• Risk may include investment, organizational, funding, and technical risks.

Note that this step involves periodic reassessment of the investment relative to these defined cost and schedule expectations. Other elements of this guide address more detailed cost and schedule assessments of an IS.

Risk which should have been mitigated by the audited entity:

If a program has not developed reliable cost and schedule estimates or has not developed reliable assessments the extent to which it is achieving its benefits, decisions resulting from a periodic assessment will not be based on reliable information. In addition, if an IS does not actively take appropriate steps to monitor and manage its risks, an assessment or program risk will not necessarily be based on a comprehensive risk assessment. Without periodic assessments of cost, schedule, performance, and risk, entities risk not having the information needed to proactively identify performance problems and potential corrective actions. For example, entities may not have sufficient information available to make well-informed decisions about whether to continue funding an IS.

3.4.1.1.3. Evaluate the IS relative to defined policies, standards, processes and mechanisms for monitoring compliance

Objective:

An organization should periodically assess the IS relative to defined policies, standards, processes. This may include compliance with policies, standards, and processes defined by the organization, defined in statute, and by established best or leading practices. The extent to which an auditor selects specific policies, standards, and processes for evaluation depends on numerous factors described elsewhere in this guide.

Risk which should have been mitigated by the audited entity:

If an organization does not have processes in place (i.e., internal controls) for evaluating and documenting IS compliance with policies, standards, and processes, the IS risks not complying with the associated requirements.

3.4.1.1.4. Periodically assessing the IS’s performance expectations

Objective:

To determine the extent to which the IS’s performance expectations are periodically assessed.

An organization should assess the performance expectations for an IS on a periodic, or annual, basis (e.g., performance expectations for a particular investment are to meet or exceed the performance goals by the end of the first year). An IS’s expectations should take into account its past performance, in addition to serving as the basis for future reviews of the IS and the extent to which it is achieving its expectations in the context of an organization’s larger portfolio, or portfolios, of ISs.

Risk which should have been mitigated by the audited entity:

If an organization does not have a process to ensure that IS performance expectations are periodically assessed, an IS may continue to operate with performance expectations that are no longer relevant or reasonable.

3.4.1.1.5. Determining the extent to which an IS continues to meet organizational needs

Objective:

To determine the extent to which an IS undergoes periodic assessments of its continued strategic alignment and ability to deliver intended benefits.

An organization should periodically assess an IS’s continued strategic alignment to organizational mission, goals, and strategies as well as its ability to deliver on its performance expectations and deliver intended benefits. In some cases, this may result in an IS being identified as a candidate for retirement based on its continuing business case and the mission benefits it is delivering. Such periodic evaluations may also consider the extent to which an IS’s underlying technology is consistent with emerging technologies and potential successor ISs.

Risk which should have been mitigated by the audited entity:

If an organization has not established a process for periodically evaluating ISs, an IS may continue to operate well beyond the time that it is delivering intended benefits or meeting the need of the organization.

3.4.2 Capacity Management

Moving-on from IS governance, an important parameter linked with the performance dimension of an IS is Capacity management, both in terms of human resources (HR) and technology. Capacity management is the function which is responsible for ensuring that the capacity of the information system and the users in the audited entity is sufficient to meet current and future performance requirements.

The audited entity should maintain documentation on current and future performance requirements to be met by the information system, with well-defined KPIs.

Auditors may examine whether:

i. The entity performs a periodic capacity gap analysis for its organization, and when was the last exercise conducted.

ii. The management has established benchmarks based on rational internal working or applicable industry standards regarding the utilization of an IS. (This indicator would help assess whether the optimum utilization of IS is being undertaken).

iii. The HR and software have appropriate compatibility and performance efficiency and whether the HR has the skills to utilize the IS solution available to an adequate level.

iv. The existing HR and system capacity are adequately spread across the organization, to avoid having silos of excellence instead of an improved standard of service delivery/operations.

v. Baseline KPIs for current requirements are being achieved by the information system

vi. There are plans to upgrade the capacity of the information system (processing power, memory, storage, network availability etc.) to enable achievement of the KPIs for identified future requirements

vii. Risk assessment framework has been adopted, to identify key risks to achieving the future capacity, specify contingency plans in case capacity increase is not achieved and mitigation measures for each risk

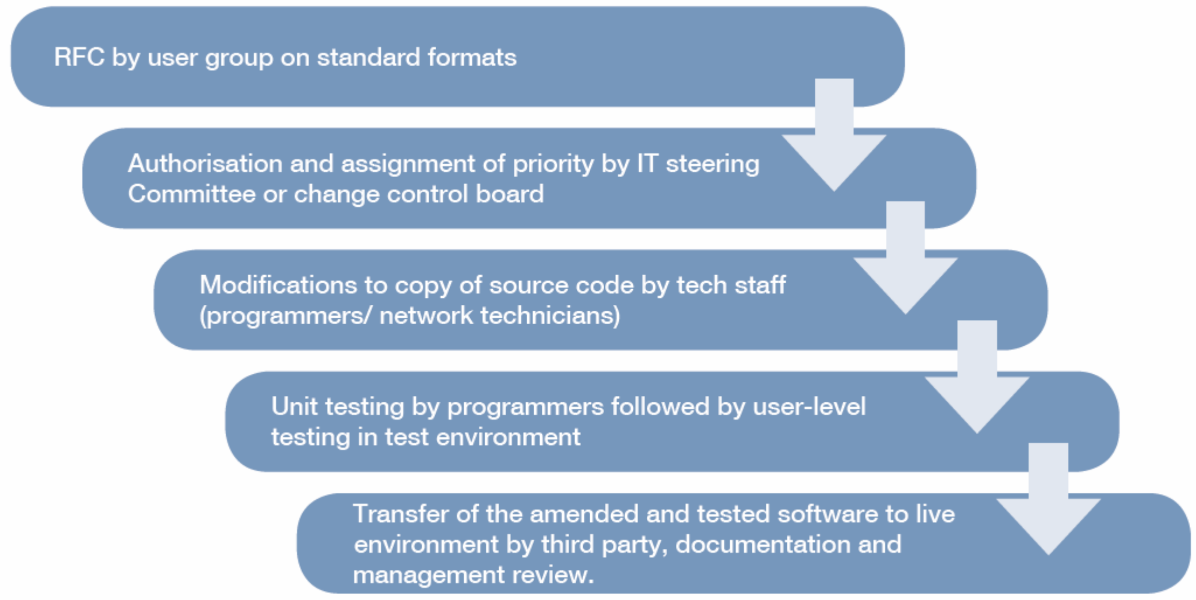
viii. There are plans to maintain and upgrade the capacity of end users to effectively use the information system for current and future business requirements, with appropriate list of options for in-person training, remote / virtual training and self-learning sessions.

3.4.3 Change Management

The manner in which changes to the IS implementation are carried out greatly affects its performance in the short term and more significantly in the medium / long term. Poor change management practices lead to unmanaged IT solutions which become problematic over time and lose their efficiency.

Typically change management involves assessing whether changes to the information system are authorized, tested, documented and controlled. Unauthorized or accidental changes to the production environment of the information system can have severe adverse impacts in terms of performance of the information system and in terms of financial consequences for the audited entity. A well-defined change management process mitigates against such risks. The change management process should also have provisions for emergency changes, but with controls such as approval from the competent authority and documentation specifying the justification for the same.

Auditors may examine whether the following key elements of change management have been adopted by the audited entity:



RFC by user group on standard formats

Authorisation and assignment of priority by IT steering Committee or change control board

Modifications to copy of source code by tech staff (programmers/ network technicians)

Unit testing by programmers followed by user-level testing in test environment

Transfer of the amended and tested software to live environment by third party, documentation and management review.

Source: IDI INSTOSAI Handbook on IT Audit / Note: RFC – Request for Change

3.4.4 Incident Management

In order to assess the reliability and efficiency of an IS solution with regards to its day-to-day operations, a useful indicator is to review the number of incidents that on average occur in the subject IS solution and the manner in which these are identified, analyzed, escalated (if required) and resolved. In this context, having a sound knowledge on incident management review techniques as illustrated below would assist the auditor in the ISPE exercise. Incident Management is the function which is used to respond to unexpected errors in the functionality of the information system, which could include incidents such as unauthorized user access or intrusion, network failure, incorrect functionality of the software or inability to use. Such incidents, unless resolved immediately, could have severe adverse impacts in terms of performance of the information system and in terms of financial consequences for the audited entity. A well-defined incident management process mitigates against such risks.

Auditors may examine whether

i. Incidents or errors noticed by users of the information system are recorded, analyzed, and resolved in a timely manner by the audited entity.

ii. Incidents which impact data security have been accorded high priority and have been resolved in a timely manner by the audited entity.

iii. Root causes have been identified for major or recurring incidents and suitable mitigation measures, including communications with end users, have been adopted until the underlying problems have been resolved. Incidents may emanate from issues or bugs from a documented change which had not been adequately tested or from unauthorized changes to the production environment.

iv. Mechanisms have been put in place for the detection of and documentation of conditions that could lead to the identification of an incident.

v. There are documented procedures for detecting and recording abnormal conditions in a systematic manner.

3.4.5 Service Level Management

Service Level Management is the function which deals with the specifications of the parameters for service levels that the information system has to fulfil, in order to meet the business objectives of the audited entity.

The parameters for service levels typically specify the Key Performance Indicators (KPI) for the functionality delivered by the information system for the audited entity.

The KPIs are agreed to by the business process owners of the audited entity on the one hand, and the owners of the information system on the other hand. These are in turn reflected, where necessary, in a formal Service Level Agreement, which is signed by the audited entity and external software service providers.

Auditors may examine whether:

i. The information system is able to fulfil internal service level parameters to the satisfaction of business process owners and if not, appropriate measures are being taken to achieve those parameters.

ii. The information system is functioning as per the documented agreements.

iii. The SLA contains quantifiable and tangible parameters to be monitored and reviewed and are such parameters consistent the goals and targets designed for the subject IS solution or as per current industry best practice.

iv. The information system is functioning as per the documented agreements, and are such documents consistent with the organization's policy and applicable laws and procedure.

v. Mechanisms are in place for identifying gaps in performance, addressing gaps identified, and following up on the implementation of corrective action taken as a result of evaluating of the performance of the information system.

vi. There are sufficient provisions in the SLA with external software service providers to safeguard the financial and reputational interests of the audited entity, in case of failure to meet KPIs.

Furthermore, it may also be necessary for an entity to have internal SLAs in cases where different departments / sub-offices are linked together to perform a specific business process. Like for an external SLA, internal SLAs should also be well defined and soundly implemented in order to ensure adequate level of performance from the IS Solution.

3.4.6 Data Security

A most evident manifestation of an IS implementation is the presence of digital information at the heart of all business activities and processes. Hence its central role necessitates the auditor to ***Identify, Analyze, Build, and Evaluate (IABE)*** a performance evaluation matrix centered around data security.

Security is the function which is responsible for ensuring confidentiality, integrity, and availability of data used by the information system, in a manner applicable with the relevant laws of the land and/or international best practices.

At a broad level, a performance evaluation matrix based on IABE would have the following contours:

- Existence of organization wide data management policy/procedures/SOPs, their approval level, dissemination and adaptation.
- The legal framework linked with the data management policy/procedures/SOPs, and its adequacy, such as having a clearly established trail of data evidence.
- Rational used for framing of such a Data Security framework and its currency.
- Is the expense being incurred on the data management and its data security aspects consist with its value and threats? Organizational data would have varied classification levels requiring a corresponding treatment of risk.
- Conducting substantive test scenarios to examine whether the data kept by the organization is a robust and consistent manner.

Furthermore, to assist an auditor to explore the domain of data security, the topic in general is briefly touched upon below.

Data Security includes those measures necessary to detect, document, and counter such threats, and protect the IS infrastructure from unauthorized users. Deficiencies in maintenance of confidentiality, integrity, and availability of data can have severe adverse impacts in terms of performance of the information system and in terms of financial consequences for the audited entity. A well-defined data security function mitigates against such risks.

Auditors may examine whether the following elements of data security[59] are in place, during the information systems performance evaluation:

i. **Distinct organization unit**

A distinct organizational unit is entrusted with the responsibility for implementing the data security policy for the information system. This organization unit should acquire appropriate tools, monitor the status of compliance with the processes required for data security, organize necessary training for the personnel, and function as first responder to data security incidents for the information system.

ii. **Clear and formal documentation**

Clear and formal documentation for receiving input data, computation or processing of data, and dissemination of output data has been prepared and is being followed, for the information system under review. The status of compliance with the formally documented processes for input, processing, and output of data would probably be the most significant predictor of data security levels for the information system.

iii. **Management of Human Resources**

Employees handling personal data in an organization need to receive appropriate awareness training and regular updates in an effort to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organization's security policy. The management of risks to security should encompass all phases of employment association with the organization and in accordance with the critical processes identified according to the nature of the organization:

- Pre-Employment: Defining roles and responsibilities of the job, defining appropriate privileges to access data for the role and conducting appropriate screening of the candidate for the job, in line with formal processes.
- During Employment: Providing periodic reminders to employees with access to sensitive information on their responsibilities and

[59] Adapted from ISO 27000 series *Information Security Management System*

providing periodic security awareness training on latest security risks and mitigation measures.

- Termination or Change of Employment: To prevent unauthorized access to sensitive information, access should be revoked immediately upon termination/ separation of an employee with access to such information. This also includes the return of any devices or assets of the organization that was held by the employee in fiduciary capacity.

iv. Physical security

Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing the building or facility where the information system is physically stored on computer servers/ end user systems.

Auditors may examine whether the physical security for the information system under review includes the following elements, depending on the criticality of the information system:

- Warning signs, armed security guards, and perimeter control
- Strong building material and the use of locks and safes
- Use of access controlled doors within the building to selectively permit access to users based on pass cards/ keys
- Safeguards to minimize the risk from physical hazards such as fire/ flooding.
- Triggering of appropriate alerts and incident responses (e.g., by security guards and police).

3.4.7 Asset Management

Asset Management is the function which is responsible for economic, efficient and effective maintenance of hardware and software assets across their lifecycles. Deficiencies in Asset Management may have an adverse impact on the performance of the information system, in the form of diversion of IS resources for other purposes, increased costs due to absence of monitoring of warranty periods for hardware and license terms for software applications.

Auditors may examine whether the following elements are in place for Asset Management, for the information system under review:

i. Clearly defined policy for end use of hardware and software assets of the organization by employees, especially at locations outside the premises of the organization and external to the internal network. This policy should cover areas of responsibility and responsive processes for incidents such as damage to and theft of hardware devices and data or functionality loss due to virus/ worm attack from the Internet.

ii. Updated and complete inventory/ database of all hardware devices and software application licenses (including those whose Intellectual Property Rights vest with the organization itself) that are in active use across the organization. The inventory/ database should include details such as Asset Identification Number, Physical Location, Assigned User, Use Commencement Date, Warranty Period, Useful Life, Asset Replacement Value, Asset Criticality etc.

iii. Review of asset inventory/ database has been carried out at periodic intervals to remove those assets which are no longer required by the organization.

iv. Priority of hardware and software assets has been clearly assigned, based on monetary value or criticality to operations, to ensure that planning for replacement is initiated on time, to mitigate financial or reputational risks.

v. Replacement of hardware and software assets has been carried out on time, to mitigate the risks of incompatible assets due to obsolescence/ vulnerabilities that may be exploited by new threats such as viruses.

vi. Processes have been clearly defined and are being complied with for disposal/ re-use of assets- authorization required for disposal or re-use of hardware assets and ensuring that data is erased prior to disposal or re-use of hardware assets.

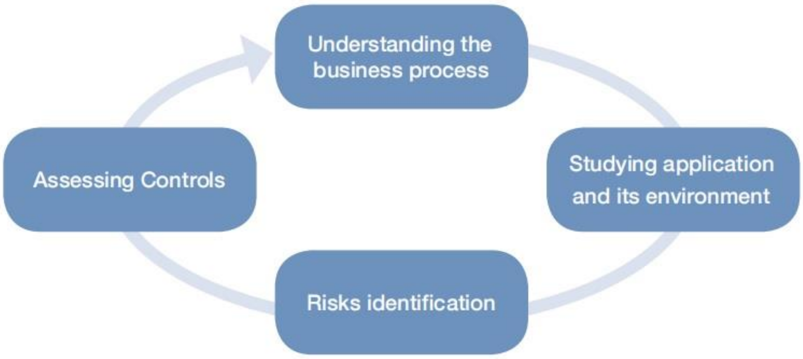
3.4.8 IS Operations

An ISPE exercise would involve review of the overall IS operations taking place in the organization. These operations would invariably be linked with business processes relevant to the auditee organization having defined outputs and outcomes. The IS auditor would have to develop a sound understanding of these IS operations and identify such check points within these operations which have a bearing on the overall performance of the IS in terms of delivering an optimum level of IT services in a most economic and value based manner.

In order to carry out such an assessment, various application controls which identify the manner in which a typical IS system functions would have to be analyzed. In this context, given below are details regarding application control review of an IS which would facilitate the auditor in drawing up the relevant review / analysis queries.

Application controls serve to replicate the function of business rules which govern the processes of the audited entity which are implemented through the information system under review.

The process by which Auditors may review the application controls may be summarized as follows:

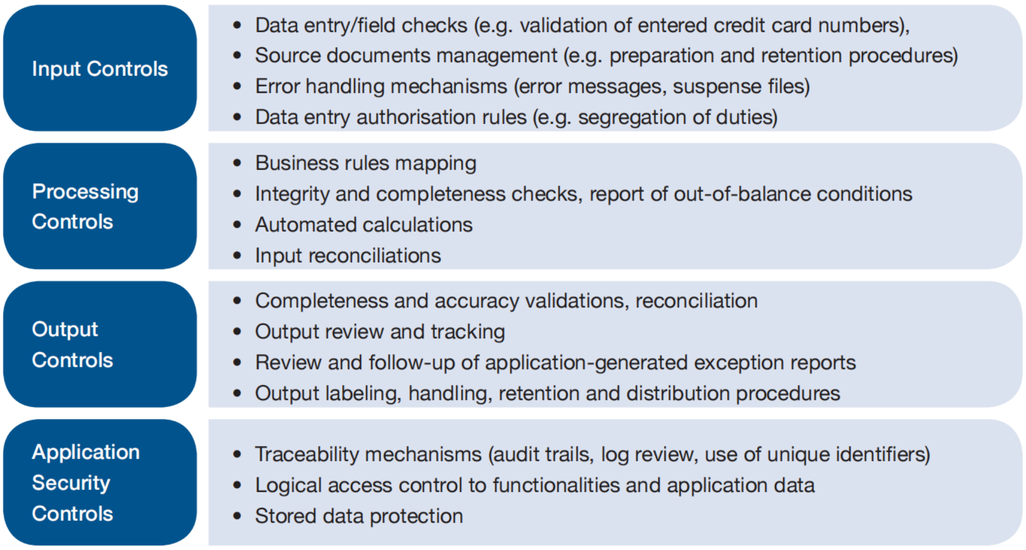

Understanding the business process
Studying application and its environment
Risks identification
Assessing Controls

Source: IDI INSTOSAI Handbook on IT Audit

Application controls may also include manual procedures that operate in proximity to the information system under review. For example, the photograph of a warehouse at a particular location may have to be authenticated off-line by personnel, before being uploaded into the system with associated geographic meta data tags. The extent of such manual controls and the combination of manual and automated controls for the information system may have been a result of cost and design considerations. Auditors should therefore carefully review and identify manual procedures and controls that serve to function as supplementary or complementary controls to the application controls themselves.

The review of application controls may commence with their classification into Input Controls (data origination and data entry); Transaction Processing Controls (reflecting business rules and logic) and Output Controls (distribution of results). Cutting across this classification is Security Controls (logging, communications, storage).

While it is not feasible to provide detailed guidance and checklists for the various types of information systems whose performance may be evaluated, Auditors must be aware of application control concepts that are common to all information systems. Auditors should then identify specific audit checks and tests for the information system under review. The common control elements are as below:



Input Controls	• Data entry/field checks (e.g. validation of entered credit card numbers), • Source documents management (e.g. preparation and retention procedures) • Error handling mechanisms (error messages, suspense files) • Data entry authorisation rules (e.g. segregation of duties)
Processing Controls	• Business rules mapping • Integrity and completeness checks, report of out-of-balance conditions • Automated calculations • Input reconciliations
Output Controls	• Completeness and accuracy validations, reconciliation • Output review and tracking • Review and follow-up of application-generated exception reports • Output labeling, handling, retention and distribution procedures
Application Security Controls	• Traceability mechanisms (audit trails, log review, use of unique identifiers) • Logical access control to functionalities and application data • Stored data protection

Source: IDI INSTOSAI Handbook on IT Audit

Consequences of application control failures can range from simple user dissatisfaction to material financial losses to even loss of lives, depending on the criticality of the functions of the information system. It is therefore critical that application controls are thoroughly reviewed by Auditors.

3.4.9 Business Continuity and Disaster Recovery

Sustainability and reliability of an information system are critical towards its overall performance. An IS Auditor would have to link together all such important factors which affect the reliability and sustainability of an IS and then move towards an overall assessment on whether the subject IS implementation is adequate or not. In this regard, business continuity and disaster recovery are two important areas to review.

The IS auditor would initially analyze the presence and implementation of a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in the subject organization. Next they would assess the adequacy of BCP / DRP in light of the current IT risks & challenges prevalent and whether the current implementation is adequate to meet these risks & challenges.

A typical business continuity and disaster recovery review would involve the following details:

Business Continuity Planning refers to the set of plans and processes which are responsible for ensuring that the audited entity and the information system under review are able to continue to function in the immediate aftermath of adverse events (on account of natural phenomena such as earthquakes, cyclones, tsunamis etc. or on account of human acts such as arson, sabotage, terrorism, warfare etc.) that prove disastrous and disrupt their normal functioning.

Disaster Recovery Planning refers to the set of plans and processes which are responsible for the eventual recovery of IT infrastructure and data, after the adverse circumstances that caused the disruption are no longer in play and it is considered safe for normal functioning to resume.

Auditors may examine whether

i. A specific organizational unit with clearly defined roles has been entrusted with the responsibility for BCP and DRP for the audited entity as a whole and specifically for the information system under review.

ii. Business Impact Assessment (BIA) has been carried out, with

- Assessment of criticality and sensitivity of the information system's assets, and assignment of priority on the basis of such assessment for critical assets
- Identification of risks to critical technology assets, including hardware, databases, storage devices, and network resources of the information system under review, and the associated mitigation measures.

iii. Clear documentation for the BCP and DRP processes has been updated and maintained, such as:

- Creating and maintaining mirror sites/ redundant nodes at different physical locations for data files, computer programs and critical documents, at periodic intervals. These mirror sites/ redundant nodes should be sufficiently updated so as to serve as the new operational site, in case the original operational site is damaged beyond recovery due to any disaster.

- Establishing recovery of data files, computer programs and critical documents from the mirror sites/ redundant nodes to the original operational site.
- Managing outsourced services, since they represent a distinct risk area where the BCP and DRP are not fully under the control of the audited entity. The continuity of the function through the outsourced service provider presents a risk through potential loss of the business knowledge, process ownership, inability to change the service provider in case of deficient performance and takeover of the service provider by other entities.

iv. Preventive controls have been adopted to as part of mitigation measures, including environment controls to minimize impact of physical threats to hardware (such as fire-suppression systems or back-up power supplies) and security controls to minimize impact of malicious attacks intended to take advantage of increased vulnerability during the adverse circumstances.

v. Personnel entrusted with specific roles under the BCP and DRP processes have received adequate training to ensure agility and readiness at short notice.

vi. Simulation exercises have been carried out to test the effectiveness of the BCP and DRP processes.

3.5 Case Studies

The objective of this section is to offer guidance on best practices from case studies on audit engagements, where such information systems performance evaluations have previously been carried out, by various SAIs.

This Section is organized as per best practices adopted by Auditors during examination of selected aspects of functionality of the information system under review.

3.5.1 IS Governance

3.5.1.1 Assessment of Interoperability between Electronic Healthcare Systems, Government Accountability Office, USA

Auditors examined the Departments of Defense (DOD) and Veterans Affairs (VA)' plans to achieve interoperability between their electronic healthcare systems.[60] These systems represent two of the nation's largest health care systems, serving approximately 16 million veterans and active duty service members and their beneficiaries, at a cost of more than $100 billion a year. Auditors found that the departments had initiated short and long term plans to improve performance by increasing interoperability between their electronic healthcare record systems and by developing plans to modernize these systems. Despite actions taken, DOD and VA did not demonstrate that all data in their systems complied with national standards and were computable in real time by the deadline established by the National Defense Authorization Act. Additionally, the plans these agencies had developed lacked outcome-oriented metrics and goals for defining and measuring interoperability progress. GAO made six recommendations to DOD and VA to facilitate oversight activities, all of which the agencies concurred with and have since implemented.

3.5.1.2 Review of IT Business Systems' Operational Performance Metrics, Government Accountability Office, USA

Auditors examined the performance of the portfolio of major IT business programs at the Department of Defense by analyzing operational performance data for the department's top 25 programs against guidance from the Office of Management and Budget.[61] This guidance requires programs to report at least 5 operational performance metrics consistent with the following four categories: customer satisfaction, strategic and business results, financial performance, and innovation. Auditors found that, as of December 2021, each of the 25 DOD programs had identified, at a minimum, the required number of operational performance metrics in each of the required categories. However, auditors found that 19 of 25 of these programs did not fully report their performance

[60] GAO, *Electronic Health Records: Outcome-Oriented Metrics and Goals Needed to Gauge DOD's and VA's Progress in Achieving Interoperability*, GAO-15-530, Washington, D.C., Aug. 13, 2015

[61] GAO, *Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning*, GAO-22-105330, Washington, D.C., Jun. 14, 2022

relative to these metrics, to include 11 programs not reporting any data. The report included a recommendation for the Chief Information Officer to ensure that major IT business programs report operational performance measures, as appropriate, as part of the department's submission to the federal IT Dashboard. DOD concurred with the recommendation and described actions it was taking and planned to take in order to address it.

3.5.1.3 Land Registry software application, Government of Haryana, India[62]

Auditors examined the process by which the contract for development of the software application for recording and maintaining land titles and property sales transactions was awarded to a software services provider, and noticed that Functional Requirements Specification document had not been prepared and finalized prior to award of the contract. The outcome was that the audited entity was not in a position to clearly define the scope of work and monitor progress in development of the software application, as additional requirements were added during the course of software development. Also, Auditors noticed that the audited entity had not constituted a committee for testing the software application. The outcome was that the audited entity was not in a position to ascertain whether the software application developed actually functioned as expected by its users.

3.5.1.4 Integrated Financial Management System, Government of Karnataka, India[63]

Auditors examined the process by which the contract for development of the software application for managing the life-cycle of public finances from budget to accounts was awarded to a software services provider, and noticed that detailed scope of work and timelines for completion of the software development had not been clearly defined. The outcome was that the audited entity was not in a position to take mitigation measures when there were repeated delays during the development of the software application. Also, Auditors noticed that Key Performance Indicators had not been defined in the Service Level Agreement. The outcome was that the audited entity was not in a

[62] https://cag.gov.in/uploads/download_audit_report/2019/8%20CHAPTER_IV-060509af8007592.84799775.pdf

[63] https://cag.gov.in/uploads/download_audit_report/2021/k2_compressed_eng-0632c082937de12.10612683.pdf

position to enforce minimum performance standards during the use of the information system.

3.5.1.5 Emergency Response System, Government of Madhya Pradesh, India[64]

Auditors examined the process by which the contract for development of the software application for managing emergency responses (police, fire, medical services) to calls made (Dial 100) by citizens was awarded to a software services provider, and noticed that the tender process had been initiated prior to identification of functional requirements and Detailed Project Report (DPR). In fact, the DPR had been prepared subsequent to price discovery from the tender process, to define scope of work deemed to be commensurate with the duration and size of the contract. Auditors also noticed that core responsibility of the audited entity in monitoring the progress of work and payments to the software developer had been entrusted to a Project Management Consultant. As a result, the audited entity was not in a position to effectively intervene and initiate mitigation measures when necessary.

3.5.2 Application Controls

3.5.2.1 Review of Information Security Controls of the Security and Exchange Commission's Systems for Financial Reporting, Government Accountability Office, USA

GAO assessed the Securities and Exchange Commission's (SEC) internal control structure and procedures for financial reporting.[65] This was done by examining the SEC's information security policies and procedures, testing controls, and interviewing key officials on whether controls were in place, adequately designed, and operating effectively. GAO found deficiencies in the SEC computing environment, such as internal firewalls allowing internal users without legitimate business to access a key financial system, as well as additional shortcomings. To address these deficiencies, GAO recommended that the Chairman of the SEC take the following 2 actions:

[64] https://cag.gov.in/uploads/download_audit_report/2021/Report%20No.%206%20of%202021_DIAL%20100_English-0622d69963164c1.79584021.pdf

[65] GAO, *Information Security: SEC Improved Control of Financial Systems but Needs to Take Additional Actions*, GAO-17-469 , Washington, D.C., July 27, 2017

- Maintain up-to-date network diagrams and asset inventories in the system security plans for the General Support System, which provides (1) business application services to internal and external customers and (2) security services necessary to support these applications, and a key financial system to accurately and completely reflect the current operating environment.
- Perform continuous monitoring using automated configuration and vulnerability scanning on the operating systems, databases, and network devices.

In addition to these two recommendations, GAO made 13 detailed recommendations in a limited official use only report. Those recommendations addressed access control, configuration management, and separation of duties.

3.5.2.2 Assessment of Internal Controls Over Financial Reporting Supporting the Internal Revenue Service’s Fiscal Years 2022 and 2021 Financial Statement Audits, Government Accountability Office, USA

GAO audits the financial statements of the Internal Revenue Service (IRS) annually. As part of these audits, GAO assesses IRS's key financial reporting controls, including information system controls. In this report, GAO identified new deficiencies in internal control over financial reporting identified during its audit of IRS's fiscal years 2022 and 2021 financial statements.[66] GAO also reported the results of GAO's fiscal year 2022 follow-up on the status of IRS's corrective actions to address recommendations contained in GAO's prior years' reports related to internal control over financial reporting that were open as of September 30, 2021. GAO made three recommendations to address the new control deficiencies in tax refunds and safeguarding assets. In a separately issued limited official use only report, GAO made 16 new recommendations to address control deficiencies in information systems related to access controls and configuration management.

[66] GAO, *Management Report: Improvements Needed in IRS's Financial Reporting and Information System Controls*, GAO-23-106401, Washington, D.C. May 25, 2023

3.5.2.3 Assessment of the Bureau of the Fiscal Service's Information System Controls over Financial Reporting, Government Accountability Office, USA

GAO performed a review of information system controls over key Bureau of Fiscal Service financial systems for fiscal years 2017 and 2018.[67] This was done by reviewing the information system control policies and procedures, observing controls in operation, conduct tests of controls, and holding discussions with officials on the design implementation and operation of controls. Using these methods, auditors looked for reasonable assurance that

a) Transactions that occurred were input into the system, accepted for processing, processed once, and properly included as output.

b) Transactions were properly recorded in the proper period.

c) Recorded transactions actually occurred and the output contained only proper data.

d) Application data and reports were protected against unauthorized access.

e) Application data and reports were readily available to users when needed.

GAO made nine new recommendations to address control deficiencies in the Fiscal Service's financial systems.

3.5.2.4 Land Registry software application, Government of Haryana, India[68]

Auditors examined the process by which business rules had been mapped into the software application in the form of controls and noticed that a key business rule which was applicable to sale of land plots whose areas were below a defined threshold, had not been mapped as an application control. The outcome was that the information system did not differentiate between sales transactions involving land plots having areas less than or greater than the defined threshold.

[67] GAO, *Management Report: Improvements Needed in the Bureau of the Fiscal Service's Information System Controls*, GAO-19-302R, Washington, D.C., Mar. 26, 2019

[68] https://cag.gov.in/uploads/download_audit_report/2019/8%20CHAPTER_IV-060509af8007592.84799775.pdf

As a result, there was a shortfall in levy of Stamp Duty on sale of such land plots whose areas were below the defined threshold that is, a direct loss of Government tax revenue.

3.5.2.5 Integrated Financial Management System, Government of Karnataka, India[69]

Auditors examined the process by which business rules had been mapped into the software application in the form of controls and noticed that key application controls had not been implemented, which had resulted in

- Non-compliance with the Indian Government Accounting Standard for Accounting of Grants received by State Government from Government of India
- Payment of salaries to employees even after their retirement
- Double payments to service providers
- Release of funds in excess of authorized budget allotment

3.5.2.6 Vehicles and Drivers' Registration System, Government of Gujarat, India[70]

The information system is used to record and maintain data on registered vehicles and licensed drivers in the State of Gujarat, India.

Auditors examined the process by which business rules had been mapped into the software application in the form of controls, and noticed that key application controls had not been implemented:

- For data entry of details of new vehicles, the newly developed software application was being used. For data entry of details of existing old vehicles, a legacy software application was being used which did not have input restriction or validation of data entered into data fields such as date of registration, date of purchase, tax paid date and tax receipt number. In the absence of application controls, there was invalid and unauthenticated data pertaining to new vehicles entered into the vehicles'

[69] https://cag.gov.in/uploads/download_audit_report/2021/k2_compressed_eng-0632c082937de12.10612683.pdf

[70] https://cag.gov.in/uploads/download_audit_report/2020/Chapter_7_Other_Tax_And_Non_Tax_Receipts_of_Re port_no_3_of_2020_Economic_and_Revenue_Sector_Government_of_Gujarat-05f8088337b2474.53313872.pdf

database using the legacy software application, resulting in evasion of Motor Vehicles Tax for new vehicles.

- For data entry of details of Driving Licenses (DLs) issued prior to the year 2010, a legacy software application was being used which did not have input restriction or validation of data entered in the fields such as DL Number and DL issue date. In the absence of application controls, there was invalid and unauthenticated data pertaining to Driving Licenses entered into the drivers' database using the legacy software application, resulting in illegal entries of drivers whose Driving Licenses had been cancelled/ not issued at all.

3.5.3 Business Continuity and Disaster Recovery

3.5.3.1 Integrated Financial Management System, Government of Karnataka, India[71]

Auditors examined the Business Continuity and Disaster Recovery Planning functions for this information system and noticed that

- Disaster Recovery Drills, i.e., simulation exercise to test the BCP and DRP had not been conducted annually, prior to the audit engagement
- When the Disaster Recovery Drill was actually conducted in the presence of the Auditors, for duration by which the database of the information system, which contained budget to accounts data, could be made available to users after the mock disaster struck was 188 minutes, against the Recovery Point Objective[72] of 0 minutes.
- The Drill Analysis Report indicated that the Digital Signatures functionality had failed as part of the Business Continuity function. This was a major failure for the financial management system, in which each bill of expenditure had to be digitally signed by the authorized officer.
- The DR off-site (i.e., the redundant node used for back-up of critical data, documents and the application) was located less than 01

[71] https://cag.gov.in/uploads/download_audit_report/2021/k2_compressed_eng-0632c082937de12.10612683.pdf

[72] The duration for which non-availability of data is tolerable

kilometer from the original operational data site, and hence did not adequately mitigate risks arising from natural disasters which might have adversely impacted the original data site.

3.5.4 Cost and Schedule Estimates

3.5.4.1 Review of Department of Defense Program's Cost and Schedule Estimates, Government Accountability Office, USA

Auditors examined the extent to which Department of Defense's (DOD) MHS GENESIS's cost estimate and program schedule were consistent with best practices.[73] GAO reviewed documentation supporting the program's October 2020 cost estimate against best practices. MHS GENESIS's contract award totaled $5.5 billion, and DOD planned to implement the program in 24 waves or phases. The first wave was completed in October 2017 with the last wave expected to be deployed by December 2023 and additional activities planned through 2025. GAO found that DOD had not fully met the characteristics associated with best practices for developing MHS GENESIS cost and schedule estimates. GAO recommended that DOD develop reliable cost and schedule estimates for the program that are consistent with best practices.

3.5.4.2 Review of Department of Veterans Affairs' Cost and Schedule Estimates, Government Accountability Office, USA

Auditors reviewed the progress of the Department of Veterans Affairs (VA) Financial Management Business Transformation (FMBT) program, which had begun implementing the Integrated Financial Acquisition Management System with the first deployment of certain capabilities at the National Cemetery Administration.[74] GAO examined the status of the FMBT program and the extent to which VA had followed certain IT management best practices. GAO found that VA had not fully met best practices for developing and managing cost and schedule estimates. GAO made two recommendations to VA to help ensure the FMBT program's cost and schedule estimates are consistent with best practices.

[73] GAO, *Electronic Health Records: Additional DOD Actions Could Improve Cost and Schedule Estimating for New System*, GAO-22-104521, Washington, D.C., Jun. 8, 2022

[74] GAO, *Veterans Affairs: Ongoing Financial Management System Modernization Program Would Benefit from Improved Cost and Schedule Estimating*, GAO-21-227, Washington, D.C., Apr. 20, 2021

3.5.4.3 Review of Housing and Urban Department's Cost Estimates, Government Accountability Office, USA

Auditors examined the Department of Housing and Urban Development (HUD) cost estimates developed for four selected IT investments, and found that the estimates were unreliable, and lacked sound basis for informing the department's investment and budgetary decisions.[75] GAO's Cost Estimating and Assessment Guide (Cost Guide) defines best practices that are associated with four characteristics of a reliable estimate – comprehensive, well documented, accurate, and credible. However, none of the cost estimates for the selected investments exhibited all of these characteristics. GAO recommended that HUD finalize and implement guidance that incorporates best practices called for in the Cost Guide.

[75] GAO, *Information Technology: HUD Needs to Address Significant Weaknesses in Its Cost Estimating Practices*, GAO-17-281, Washington, D.C., Feb. 7. 2017

CHAPTER 04

IS Performance Evaluation Reporting

Chapter 04 Introduction

Paragraph 51 of ISSAI 100[76] requires the auditors to prepare a report based on the conclusions reached. The report should be easy to understand, free from vagueness or ambiguity, and complete. It should be objective and fair, only including information supported by sufficient and appropriate audit evidence and ensuring that findings are put into perspective and context.

The performance audits provide a report on the efficiency and economy of the acquisition and use of information systems and whether the objectives were achieved. Reports may vary considerably in scope and nature, for example, assessing whether resources have been applied soundly, commenting on the impact of policies and programs, and recommending changes designed to result in improvements.[77]

As our subject guidance document addresses a further specialized area of Information Systems Performance Evaluations (ISPE), the reporting considerations would encourage inclusion of concepts form performance reporting templates and information systems reporting template as per international best practices.

This chapter discusses the minimum contents of the ISPE report, a reporting template, and an optional performance assessment rating methodology for SAI's guidance.

4.1 Contents of the Performance Evaluation Report

Paragraph 39 of ISSAI 300 states that auditors should strive to provide audit reports which are comprehensive, convincing, timely, reader-friendly, and balanced. To be comprehensive, a report should include all the information needed to address the audit objective and questions while being sufficiently detailed to provide an understanding of the subject matter and the findings and conclusions. To be convincing, it should be logically structured having a clear relationship between the objectives, criteria, findings, conclusions, and recommendations.

It is pertinent to highlight here that the reporting template and general practices used by different SAIs may vary greatly. Therefore, this chapter does not look to restrict the SAIs to follow a typical reporting template or impose a standard reporting format. Rather the purpose of this chapter is to provide an example of how a stand-alone ISPE report could look and be generated.

[76] International Standards of Supreme Audit Institutions (ISSAIs) 100 – Fundamentals Principles of Public-Sector Auditing, developed by the INTOSAI

[77] International Standards of Supreme Audit Institutions (ISSAI) 300- Fundamental Principles of Performance Auditing

The audit objectives are usually defined so as to derive assurance against very specific aspects of the performance evaluation, which were included in the scope of the audit engagement. The reporting would therefore be against those audit objectives, in the form of a pass/ fail criteria and highlighting key risks that ought to be addressed by the audited entity.

The Performance Evaluation Report may comprise of Volume I - the Executive Summary and Volume II - the Detailed Report. The Executive Summary is a concise document that includes a high-level description of the report's primary message, key objectives of the performance evaluation, and a summary of evaluation results. It is designed for top Management or executives. A comprehensive discussion of IS performance evaluation is contained in Volume II and intended for the operational level responsible for implementing the recommendations. A reporting template in the Annexes can serve as a guide in crafting the report.

4.2 Adding A Performance Assessment Rating Methodology

In order to make the ISPE report more insightful and value-driven a concept of having a performance assessment rating methodology is being introduced here. This methodology is being presented as an example with an aim to make the SAI explore new ways in which to augment their findings with additional analysis. The rating methodology is not a mandatory part of the proposed reporting template, rather the SAI may or may not follow it as per their practice mandate.

SAIs are encouraged to use the proposed technique which could be revised and refined further in the next version of this subject guidance based on their feedback.

4.2.1 Classifying Audit findings

Once the ***ISPE*** (Information Systems Performance Evaluation) field audit activity has been completed and individual audit findings communicated to the management (and responses received as the case may be) the important stage of the preparing the ISPE report draft begins. This is a crucial stage as the individual audit findings need to be linked together to present a holistic outcome of the subject audit exercise at this point. If care is not taken on compiling the results of ISPE, the desired final outcome of the subject exercise is likely not to be achieved.

In this context different approaches can be used towards representing the audit findings. One such methodology[78] suitable to be applied to a ISPE exercise is elaborated below:

[78] Performance assessment ranking methodology prepared by Muhammad Ali Farooq Gheba Director Audit SAI Pakistan, Zia-ul-Islam Executive Officer GIS, SNGPL, Ali Rajab Raza GIS Specialist

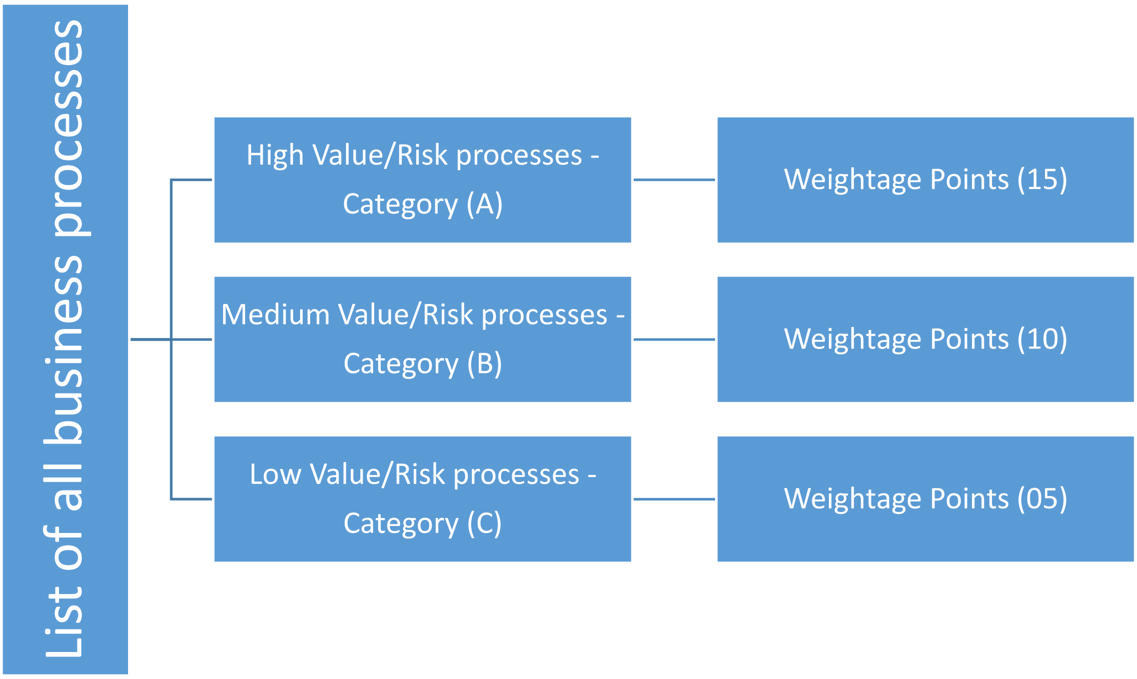
4.2.2 Categorizing Business Processes

During the planning stage the scope and extent of the ISPE would have to be clearly defined and limitations stated. Due to time and resource constraints in most cases it may not be practical to carry out an assessment of all business areas in an organization.

Hence based on this defined audit scope for the subject audit the auditor would list out all of the entity's business processes and then classify these processes into categories.

A *business process* represents any uniquely identifiable operational activity being performed by the organization using information technology in a complete or a partial manner.[79] A business process corresponds to the underlying objectives of the organization being achieved using these processes.

Once a list of all business processes has been populated the auditor would assess which of the business processes carry high audit review value and which carry lesser review value. Invariably all key business operations having high business impact would get translated to high risk audit area. In this manner the businesses in an audit organization would get classified into different categories. Illustratively:


List of all business processes
High Value/Risk processes - Category (A)
Weightage Points (15)
Medium Value/Risk processes - Category (B)
Weightage Points (10)
Low Value/Risk processes - Category (C)
Weightage Points (05)

[79] Basic planning steps have been stated here as the rating methodology is being introduced in this guidance as an example and an additional concept.

Care needs to be taken to not to make too many categories in order to avoid compilation complexities. The end result of the categorization process would be that the auditor would have classified all the business processes relevant to audit scope into the above three categories.

In order to classify any business process into a relevant risk category the auditor may need to review the system classification undertaken by the auditee organization. Systems and their allied processes that are classified as critical would automatically fall in category A or high risk and those that are classified as non-sensitive could end up in category C. However, such an entity-based system classification list should not be taken as the end word by the auditor, it is imperative that the classification exercise is undertaken by the auditor based on their understanding of the working of the organization and the auditing perspective.

4.2.3 Assigning weights to the audit findings:[80]

Once the findings have been established the next step is assigning a rating score in a systematic way so that a holistic picture can be drawn.

Nature of Finding	Impact	Rating/Score
Material	Very high impact. The shortcoming identified is such that it can/has materially impact/impacted the business process from delivering its desired outcomes completely. An indicator of system failure for the subject business process. This would also require a holistic approach to assessment. For example, an IS solution was deployed and is functionally performing well, but the business process has changed and the system is not compatible with the new needs of the entity.	04
Major	High impact. The shortcoming identified is such that it can/has significantly impact/impacted the business process from delivering its desired outcomes adequately and in economic/effective/efficient manner. That is, the system is delivering outcomes but in a significantly unsatisfactory manner.	03
Moderate	Medium impact. The shortcoming identified is such that it can/has medium impact/impacted the business process from delivering its desired outcomes in an economic/effective/efficient manner. Additionally due value from the IT/IS application not being achieved due to subject highlighted finding.	02
Low	Low impact. The shortcoming identified is such that it doesn’t impact the business process in any significant manner, however it is a constraint due to which maximum value is not being attained from the business process.	01

[80] A basic assumption used in this ranking technique is the presence of audit findings. The subject technique would not be applicable in audits which result in zero audit findings

It is important to add here that the audit findings score is a reflection of the state/quality of implementation of an IS being reviewed but it cannot be singularly treated as a reflection of the quality of audit carried out.

This methodology assumes that the auditor based on the code of ethics mandated by the SAI conducted the assignment diligently, irrespective of outcomes. However, these additional attributes (audit finding rankings, business area classification) could become valuable analytical data for the SAI in the medium and long term.

4.2.4 Calculating the performance score of the auditee organization

The two aspects of business area categorization and individual audit finding classification elaborated above would be linked together to draw an overall performance score of the auditee organization. The aim of this scoring model is not to obfuscate the underling IS performance issues identified during the subject audit exercise, rather the objective of this scoring methodology is to add a new reporting dimension to the subject audit report making it more valuable to the reader and providing additional attributes for future analysis.

The score calculation process is illustrated below:
Number of Audit findings=X
Range of score for each audit finding = 1 to 4
Range of score for each business category = 05 or 10 or 15
Minimum Audit score implying best performance= X * (01 * 05)
Maximum Audit score implying worst performance = X * (04 * 15)
Resultantly IS performance evaluation score of any organization would lie between X * (01 * 05) to X * (04 * 15)

Min Score
Good Performance
Poor Performance
Max Score

Furthermore:

Overall weight of a single finding = (Audit finding score * Business category)

Resultantly overall score of all findings would be added to get to the performance score of the auditee organization. This accumulative score would lie between the two extremes illustrated above.

As audit finding weightage and performance rating are inversely proportional the lesser the final audit score would indicate a more satisfactory level of IS performance in the auditee organization and vice versa.

The score of individual audit findings would be added together to get to the overall IS performance evaluation score or "Total Gained Score" for the auditee organization with respect to the subject audit.

The tabulation matrix for this would be as illustrated below

Business Process Category	**Nature of Audit Findings**				**Total Gained Score**
	Material Findings Weighted Score	**Major Findings Weighted Score**	**Moderate Findings Weighted Score**	**Low Findings Weighted Score**	
High Value/Risk processes - Category (A = 15)	N*(4 x A)	N*(3 x A)	N*(2 x A)	N*(1 x A)	
Medium Value/Risk processes - Category (B =10)	N*(4 x B)	N*(3 x B)	N*(2 x B)	N*(1 x B)	
Low Value/Risk processes - Category (C =5)	N*(4 x C)	N*(3 x C)	N*(2 x C)	N*(1 x C)	
Total Gained Score					
Total No. of Findings					
***N = N equals to the number of findings of each category**					

Example:

To illustrate how a typical scoring process and subsequent performance levels would be calculated let us assume an example scenario.

ISPE was carried out for an organization named Xel. 45 Audit findings of different nature each related to different business categories have been made and the findings classified as be method explain earlier. The **Total Gained Score** for the audit exercise can be calculated as follows *(number of findings and their individual weights have been assumed for purpose of calculation)*:

Business Process Category	Nature of Audit Findings				Total Gained Score
	Material Findings Weighted Score	Major Findings Weighted Score	Moderate Findings Weighted Score	Low Findings Weighted Score	
High Value/Risk processes - Category (A = 15)	2(4x15) =120	4 (3x15)=180	10(2x15)=300	5(1x15)= 75	675
Medium Value/Risk processes - Category (B =10)	1 (4x10) = 40	3(3x10) =90	6(2x10) = 120	2(1x10)= 20	270
Low Value/Risk processes - Category (C =5)	0 (4x5) = 0	2(3x5)=30	4(2x5) =40	6(1x5) =30	100
Total Gained Score	160	300	460	125	**1045**
Total No. of Findings	3	9	20	13	**45**

Maximum possible value of overall findings = No. of Findings (Max. audit finding weight x Max. Process Category weight)
Maximum possible value of findings = 45 (4*15) = ***2700***
Minimum possible value of overall findings = No. of Findings (Min. audit finding weight x Min. Process Category weight)
Minimum possible value of finding = 45 (1*5) = ***225***
The Total Gained Score / overall IS performance evaluation score of the audit exercise = **1045**

4.2.5 Calculation of performance level:

Once we have calculated the performance score the next step is to assess what type or level of performance does this score reflect? In order to do so we need to translate the score into its corresponding performance level category. The calculation process is as follows

Step 01: **Calculating the range:** In order to calculate the performance level we need to first calculate the range of values along which we can place our Total Gained Score.

Continuing with our above example, our overall finding score limits were:

Min
225

Max
2700

We convert our finding score limits into a range starting from zero. For this we subtract maximum value from the minimum value as:

Max – Min = 2700-225 =2475. Hence our audit findings have a range of 0 to 2475.

Step 02: **Adjusting Gained Total Score with respect to range:** As the range is from zero our gained total score needs to be adjusted so that it can be measured from zero.

Total Gained Score – Minimum finding limit = ***Effective Score*** for Performance Value Calculation

= 1045-225 = **820**

Step 03: **Calculating the performance percentage:** Now that we have a score that can be traced on our range we can calculate the performance percentage as follows:

Performance level = (Effective Score/Maximum Range Value) x 100

Performance level = (820/2475) x 100 = 33.13% (Good Performance Level -3)

4.2.6 Performance Levels

The performance scores can be assigned different levels as illustrated below:

Level	**Performance Levels**	**Accumulative Audit Findings Score**
4	Exceptional Performance	25% or less
3	Good Performance	26% to 40%
2	Satisfactory Performance	41% to 55%
1	Un-Satisfactory Performance	56% to 70%
0	Highly Un-satisfactory/Adverse Performance	71% or more

The above-illustrated performance rating methodology can also be used to carry out other types of result analysis as performance of individual processes reviewed during the audit or nature of audit finding wise analysis of IS reviewed.

4.2.7 Presenting the performance ranking results:

It is important to clarify here that the working elaborated from 4.2.2 to 4.2.6 is the background work that the SAI Auditor would have to do in order to calculate the performance level. The auditor may apply data abstraction and present only those figures and results that they may deem necessary. The rest of the calculations would become part of the working file/permanent file of the auditee formation maintained by the audit office.

Similarly, it may not be prudent to compare performance results of different ISPEs' of different entities together in a *general fashion*. Only like things are comparable, hence cross-entity comparison of results would only be possible if these entities have similar business processes and use similar systems.

However cross-entity scan and allied performance rating would be possible if it was carried out as a specific singular ISPE exercise for an entire government sector, or broader organizational domains.

4.3 Dissemination of the Report

After a series of reviews and the approval of the Head of the Supreme Audit Institution (SAI), the performance evaluation report shall be transmitted to the Management. The report may be published and made available to the public. However, occasionally, it may be necessary to restrict or omit confidential information from the report. The decision to exclude certain information from the audit report shall be made in accordance with the policies of the SAIs.

4.4 Follow-Up Audit

A follow-up activity is a process through which auditors determine the adequacy, effectiveness, and timeliness of actions taken by Management on reported observations and recommendations.[81] A follow-up process should be established to help provide reasonable assurance that each performance evaluation conducted by auditors offers optimal benefit for the auditee by requiring that agreed-on outcomes arising from evaluations are implemented in accordance with Management undertakings or that executive Management recognizes and acknowledges the risk of delaying or not implementing proposed outcomes or recommendations. The conduct of the follow-up is aligned with the succeeding standards of the IT Audit Framework (ITAF).[82]

- Standard 1402.1 - IT audit and assurance practitioners shall monitor and periodically report to those charged with governance and oversight of the audit function (e.g., the board of directors or the audit committee) Management's progress on findings and recommendations. The reporting should include a conclusion on whether Management

[81] ITAF, 4th edition: A Professional Practices Framework for IT Audit designed & created by the ISACA

[82] Ibid.

has planned and taken appropriate, timely action to address reported audit findings and recommendations.

- Standard 1402.2 - Progress on the overall status of the implementation of audit findings should be regularly reported to the audit committee if one is in place.

- Standard 1402.3 - Where it is determined that the risk related to a finding has been accepted and is greater than the enterprise's risk appetite, this risk acceptance should be discussed with senior Management. The acceptance of the risk (particularly failure to resolve the risk) should be brought to the attention of the audit committee (if one is in place) or the board of directors.

Decisions on the timing of follow-up activities should consider the significance of the reported findings and the effect on the auditee's strategy and objectives if corrective actions are not taken. The timing of follow-up activities in relation to the original reporting is a matter of professional judgment dependent on a number of considerations, such as the nature or magnitude of associated risk and costs to the enterprise.

As follow-up activities are a vital component of an audit or evaluation process, they should be scheduled along with other steps necessary to perform each evaluation. The schedule may be determined based on the degree of difficulty, the risk and exposure involved, the performance evaluation results, and the time needed to implement remedial steps, among other considerations. Follow-up activities may be broken down into three areas:

- Casual – This is the most basic form of follow-up and may be satisfied by a review of the agency's procedures or an informal telephone conversation. Memo correspondence may also be used. It is usually applicable to the less critical findings.

- Limited – typically involves more process owner/client interaction. It may include verifying procedures or transactions, which in most cases is not accomplished through memos or telephone conversations with the agency.

- Detailed – more time-consuming and can include substantial agency involvement. Verifying procedures and audit trails, as well as substantiating computer records, are examples. The more critical review findings usually require detailed follow-up. Enumerated below are general procedures for conducting a detailed follow-up:

- Analyze the auditee's response and verify if it is aligned with the previously agreed upon strategy.
- Assess action taken against the recommendation.
- Seek evidence to verify the implementation of the action and seek clarification if necessary.
- In case the response of the process owner/client differs from the recommendation, assess if the response effectively mitigates the risk and is more efficient than the recommendation.
- In case the response of the Management is different from the recommendation and is assessed to be ineffective or inefficient, reiterate recommendations and evaluate Management's response to SAI's reiteration.
- In case management decides not to act on issues raised or elected to accept the risks, prepare a Management Acceptance of Risk.
- Prepare to communicate the results of the follow-up procedures.

Aside from the proper timing, the team's capabilities and expertise responsible for follow-up and verification are also crucial in ensuring that actions taken in response to identified observations or recommendations are not only implemented but also effectively address the underlying issues. The team shall have a deep understanding of the issues, allowing them to assess whether the actions are not just superficial fixes but comprehensive solutions that truly resolve the root causes. Technical proficiency is also needed to validate the technical aspects of the controls implemented in the information systems, ensuring they are in accordance with industry standards and best practices. Having technical know-how enables the team to offer alternative solutions if the issues are not adequately addressed. Further, competent teams can expedite the follow-up verification process, preventing delays and contributing to more efficient operations and faster issue resolution. The lack of the necessary competency in conducting follow-up activities can increase the risk of recurring observations and missed opportunities for improvement.

The decision regarding the composition of the follow-up audit team is at the discretion of the SAI, and it may be influenced by the aforementioned competency requirements, available resources, desired level of objectivity, and other relevant factors. The options include having the same team that conducted the initial audit also perform the follow-up activities, establishing a separate team solely dedicated to conducting follow-up, or adopting a hybrid approach where members from the initial audit team collaborate with individuals from a dedicated follow-up team. Having the same team that conducted the initial audit and follow-up has the following advantages: (a) possessing familiarity and deep understanding of the identified issues, which can expedite the follow-up process; (b) having a coherent strategy from the audit phase through follow-up, ensuring alignment in understanding and addressing the identified observations; and (c) enabling seamless communication as they have already established relationships with stakeholders and have a clear understanding of the auditee's organization dynamics. On the other hand, having a dedicated follow-up team can also provide the following advantages: (a) offering a fresh perspective as they may view the issues from a different angle and offer diverse insights; (b) reducing potential biases; and (c) having a specialized team trained explicitly in the verification and follow-up activities can enhance the thoroughness and effectiveness of the follow-up process. Lastly, the hybrid approach can combine the advantages of familiarity with the issues and fresh perspectives that can be offered by a dedicated follow-up team. Regardless of the decision made by the SAI, it is crucial to emphasize again that the team responsible for the follow-up activities possesses the requisite competency, objectivity, and resources to thoroughly evaluate whether the actions taken have adequately addressed the identified concerns.

To facilitate monitoring of the implementation of the recommendations, the audit team shall request the audited entity to submit an Agency Action Plan and Status of Implementation (AAPSI) at least within six months from their receipt of the performance evaluation report. The team shall issue a follow-up letter to the concerned auditee if they do not submit the accomplished AAPSI within the timeline. The template "Annex-AAPSI" can be used as a guide in the preparation of this documentation.

Upon receipt of the accomplished AAPSI, the concerned Audit Team shall:

- Evaluate the Management's response detailing the actions taken. Wherever possible, evidence of actions taken should be obtained.
- Evaluate whether unimplemented recommendations are still relevant or have a greater significance. The Team Leader/ Supervisor shall decide whether implementing a particular recommendation is no longer appropriate. It could occur when compensating controls are implemented or if there are changes in the application systems, organizational objectives, key performance indicators, and

contracts, among others. Similarly, a change in the IT environment may increase the significance of the effect of a previous observation and the need for its resolution.

- In case of doubts about the information provided or the effectiveness of the actions taken, a follow-up engagement shall be scheduled to verify the implementation of critical measures.
- Utilize and update the Action Plan Monitoring tool (APMT). The "Annex- APMT" can be used to document the results of the follow-up engagement.

According to Guidelines 2402.11.1 and 2402.11.3 of the ITAF, a report on the status of agreed-on corrective actions arising from audit engagement reports, including agreed-on recommendations not implemented, should be presented to the appropriate level of Management and those charged with governance. When all the agreed-on corrective actions have been implemented, a report detailing all the implemented or completed actions can be forwarded to the Management.

In accordance with this, the Audit Team shall communicate to the Management the result of the evaluation of the accomplished AAPSI or follow-up engagement. The Team Leader/ Team Supervisor is responsible for verifying the accuracy and comprehensiveness of the APMT before its submission and presentation to the Agency Management.

ANNEXES

Volume I – Executive Summary Template

Header of the SAI

PERFORMANCE EVALUATION REPORT

< NAME OF THE INFORMATION SYSTEM/S EVALUATED>

of the

< NAME OF THE AUDITED ENTITY>

VOLUME I of II

AUDIT PERIOD

<DAY- MONTH- YEAR>

VOLUME I

EXECUTIVE SUMMARY

VOLUME I

EXECUTIVE SUMMARY

A. INTRODUCTION (STYLE: HEADING 1)

The introduction provides an overview of the Auditee's mandate, background, brief description, and purpose of the system/s subject for evaluation and how it relates to the overall Management of the Auditee and its mandate. *(Style: Normal)*

B. AUDIT OBJECTIVES, SCOPE, APPROACH, AND METHODOLOGY

This section should provide a discussion on the primary purpose of the conduct of performance evaluation. *(Style: Normal)*

<*1st paragraph: Audit Objectives*. The audit objectives should be specific and carefully determined before the commencement of field audit activity>

Example:

The primary objectives of the performance evaluation were to:

a. Review the performance of Information Systems against intended objectives.
b. Assess whether the IT project was managed with regard to economy, efficiency, and effectiveness.
c. Review compliance with applicable rules, regulations, and procedures

<*2nd paragraph: Audit Scope* The scope statement defines the audit subject or area, the period under review when the evaluation was performed, and the scope limitations.>

<*3rd paragraph: Audit Approach and Methodology*: The audit approach and methodology include a description of the criteria or disclosure of the source of benchmarks, the tools and techniques used in gathering evidence, and the statement that the performance evaluation has been conducted under applicable IS audit standards.>

C. SUMMARY OF AUDIT OBSERVATIONS AND RECOMMENDATIONS

<Introductory sentence>

Example: The observations and recommendations issued to the Management are discussed in detail in Part III, Volume II of this report, and summarized as follows>:

The order in which audit observations are presented may be based on the audit observations risk/effect ranking from highest to lowest.

<AUDIT AREA 1 (PROJECT MANAGEMENT)> (STYLE USED: HEADING 3)

1. **<Topic Sentence> (***The topic sentence consists of the overall impression of the audit area and includes the statement of fact or condition that led to the observations. It may consist of one or two sentences providing a statement of condition, criteria, cause and effect.***)** *<Insert reference page in Volume II: Page __ of Part III Volume II)* **(Style used: Topic Sentence)**

<1st paragraph: Provide a top-level discussion/summary of the noted conditions. Avoid using technical terminology and keep in mind that the intended reader is the top Management.>

<2nd paragraph: Briefly discuss the risk implications or effects>

<3rd paragraph: Provide a summary of the recommendation (may be itemized such as a, b, c... but in paragraph form)

<AUDIT AREA 2>

2. **<Topic Sentence>.** *(Page __ of Part III Volume II)*

<Discussions>

<AUDIT AREA 3>

3. **<Topic Sentence>**. *(Page __ of Part III Volume II)*

<Discussions>

D. MANAGEMENT'S COMMENTS

It provides the highlights of the comments of the Management and the rejoinder of the audit team, if applicable.

E. CONCLUSION

< Introductory paragraph: The performance evaluation results provide the Team with an adequate basis to form an opinion on the overall performance of the (Insert the name of the Information Systems evaluated).>

<2nd paragraph: Briefly discuss the performance evaluation's overall conclusion considering the objectives set.>

<3rd paragraph: Provide the results of the performance rating assessment>

Example:

For the evaluation, a performance rating methodology was used with a rating scale comprising of 05 levels starting from exceptional performance to adverse performance. (Please refer to page___, Volume II, Part III for the rating definition and detailed scores per evaluated area)

F. ACKNOWLEDGEMENT

A statement of appreciation to the Auditee for their cooperation and support during an IS performance evaluation.

<*Example:* We wish to express our appreciation to the officials and personnel of <name of Agency> for the support and cooperation extended to the audit team during the audit.>

G. FOLLOW-UP

A statement of submission of Auditee's Action Plan and Status of Implementation

<*Example:* Follow-up procedure will be conducted on the agreed-on outcomes arising from this report, including agreed-on recommendations not implemented, to determine the adequacy, effectiveness, and timeliness of actions taken by (name of audited Agency). Thus, we request that the action plan and status of implementation taken thereon using the attached Agency Action Plan and Status of Implementation (AAPSI) template be submitted within six (6) months from receipt thereof.>

For the <name of SAI>:

By

<Name and Signature>
Team Leader

<Name and Signature>
Team Supervisor

Volume II – Detailed Report Template

Header of the SAI

PERFORMANCE EVALUATION REPORT

< NAME OF THE INFORMATION SYSTEM/S EVALUATED>

of the

< NAME OF THE AUDITED ENTITY>

VOLUME II of **II**

AUDIT PERIOD

<DAY- MONTH- YEAR>

VOLUME II

DETAILED REPORT

VOLUME II

PART I – OVERVIEW OF THE AGENCY AND THE SYSTEMS

PART II – DETAILED OBJECTIVES, SCOPE, APPROACH AND METHODOLOGY

PART III – DETAILED OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT'S COMMENTS

PART IV - ANNEXES

LIST OF TABLES

LIST OF FIGURES

VOLUME II

PART I

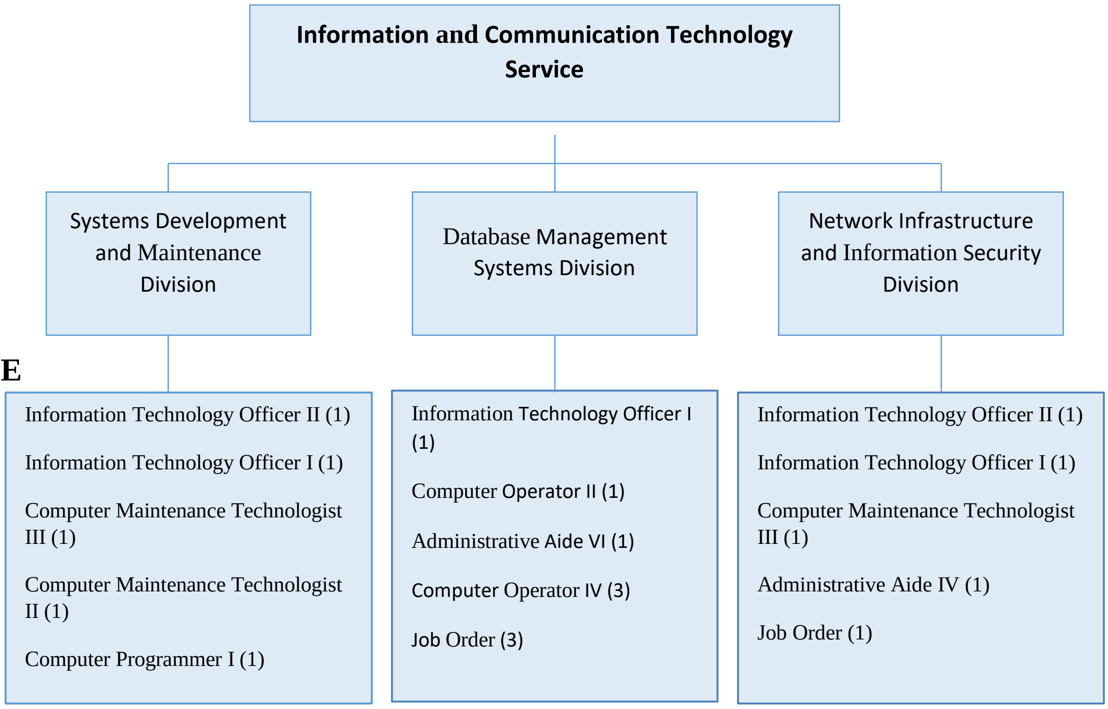
OVERVIEW OF THE AGENCY AND THE SYSTEMS

THE <NAME OF AGENCY> (STYLE: HEADING 1)

This section contains the Agency's background, vision, mission, mandate, operation, organizational structure, current leadership, employee number, IT organizational structure and functions, and other relevant information about the IS project.

(Style used: Normal)

Figure 1 Sample Figure


Information and Communication Technology Service
Systems Development and Maintenance Division
Database Management Systems Division
Network Infrastructure and Information Security Division
Information Technology Officer II (1)
Information Technology Officer I (1)
Computer Maintenance Technologist III (1)
Computer Maintenance Technologist II (1)
Computer Programmer I (1)
Information Technology Officer I (1)
Computer Operator II (1)
Administrative Aide VI (1)
Computer Operator IV (3)
Job Order (3)
Information Technology Officer II (1)
Information Technology Officer I (1)
Computer Maintenance Technologist III (1)
Administrative Aide IV (1)
Job Order (1)

THE <NAME OF THE SYSTEM>(STYLE: HEADING 1)

< Describes the system(s) under review and discussion on how it intends to support the Agency's mandate and goals> *(Style: Normal)*

Modules, Menus, and Functions

<Describes the modules and major features of the system subject for evaluation> *(Style: Normal)*

Process Flow

<Describes the process flow surrounding the system subject for evaluation> *(Style: Normal)*

VOLUME II

PART II

AUDIT OBJECTIVES, SCOPE, APPROACH, AND METHODOLOGY

AUDIT OBJECTIVES (STYLE: HEADING 1)

This section provides discussions of both general and specific objectives *(Style: Normal)*

General Objectives:

Example:

The major objectives of the performance evaluation of the Information Systems were to:

a. Review Information System's performance against intended objectives;
b. Assess whether Information Systems were managed with due regard to economy, efficiency, and effectiveness; and
c. Review compliance with applicable rules, regulations, and procedures.

Specific objectives:

Examples:

<Audit area: Project Management>

(Insert Specific Objectives)

Example: The objectives of the evaluation of the project management aspect of the IS are to assess whether the information system being evaluated has been implemented within the scheduled timelines and whether the audited entity has adopted adequate and effective internal controls to mitigate the risk of delays in the implementation of the IS. It also aims to determine whether the audited entity has clearly defined the exact and complete scope of the IS project and whether the information system being evaluated has been implemented within the budgeted costs, as well as to assess whether the benefits accrued from the use of the information system outweigh the life-cycle cost across the design, development, testing, deployment, operations, and maintenance phases of the information system.

<Audit area: Service Level Management>

(Insert Specific Objectives)

Example: The objectives of the evaluation of the service level management aspect of the IS are to assess whether the IS is able to fulfill internal service level parameters to the satisfaction of business process owners and if not, whether appropriate measures are being taken to achieve those parameters. It also aims to determine if the mechanisms are sufficient for identifying gaps in performance, addressing those gaps, and following up on the implementation of corrective action taken as a result of evaluating the performance of the IS.

AUDIT SCOPE

< This section should also indicate any areas that were excluded from the audit scope and limitations of audit coverage. On scope of audit, mention the period covered, geographical areas included or any other information that defines the scope of auditor's work.> *(Style: Normal)*

AUDIT APPROACH AND METHODOLOGY

<The section should state the methodology used, such as file review, field survey, auditee interviews, focused group discussion, market research, etc. The criteria used in the evaluation should also be included in this section.> *(Style: Normal)*

VOLUME II

PART III

DETAILED OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT'S COMMENTS

The presentation of the noted findings in the IS performance evaluation shall have the following attributes and be discussed in detail:

a. **Condition:** The factual evidence found in the course of the examination (the current state). It is a statement of the problem or deficiency. The findings may include control weaknesses, operational issues, or non-compliance with Management or legal requirements leading to not meeting the performance standards set.

b. **Criteria:** Standards and benchmarks used for comparison against the auditor's findings based on the evidence. The source of the criteria could be a Contract, Key Performance Indicators (KPIs), Operational Level Agreement (OLA), Service level agreements (SLAs), Project Plan, policies, and standards defined by the Auditee that is under review. Suppose an auditee has not defined its standards; criteria can be sourced from laws and regulations, bodies of experts such as ISACA and ISO, or can have been developed specifically for the IS performance evaluation engagement.

c. **Cause:** The reason for the difference between expected and actual conditions.

d. **Effect:** The risk or exposure the Agency or others encounter because the condition is inconsistent with the criteria. It explains the adverse impact on the performance of the systems. By articulating impact and risk, the element of effect is essential in helping to persuade auditee management to take corrective action.

Example format:

<Audit area #1 Example: PROJECT MANAGEMENT> ***(style: Heading 1)***

1. <Topic Sentence> ***(style: Heading 3)***

1.1. <Discussion> *(style: Body)*

a) **<Finding Number 1>** ***(style: Heading 2)***

1.2. <Discussion of Findings> *(style: Body)*

b) <Finding Number 2>

1.3. <Discussion of Findings and Risks>

Recommendations:

A recommendation should address the causes of weaknesses, be practical and add value, be well-founded and flow logically from the findings and conclusions, and be neither too general nor too detailed.

- The present tense is used in stating the actions to be taken by Management
- Start always w/ a verb (Conduct/Implement…)
- Doable, precise, and aligned with the Audit Observations
- Address real causes of deficiencies and must stand alone so that if uplifted, it is fully understood

Example format:

1.4. We recommended that Management:

a. <Recommendation 1>; ***(Style used: bullets)***

b. <Recommendation 2>;

Management's Comments:

Management response shall be summarized and phrased accordingly to answer the observations or recommendations directly.Whenever the auditor and auditee disagree on a particular recommendation or finding, both positions and the reasons for the difference must be included in the report.

Example format:

1.5. The Management commented the following: *(Style: Body)*

a. <Comment 1> *(Style used: bullets)*

b. <Comment 2>

Auditor's Rejoinder

If necessary and will depend on the Management Comments

Audit area 2 *(style used: Heading 1)*

2. <Topic Sentence> *(style used: Topic Sentence)*

2.1. <Discussion> *(style used: Body)*

a) <Finding Number 1> *(style used: Heading 2)*

2.2. <Discussion> *(style used: Body)*

Recommendations:

2.3. **We recommended that Management:**

a. <Recommendation 1>;

b. <Recommendation 1>

Management's Comments:

2.4. The Management commented the following:

a. <Comment 1>

b. <Comment 2>

Auditor's Rejoinder:

2.5. _______

AUDIT CONCLUSION

- Discuss the performance rating assessment methodology used. Auditors should ensure that the discussion in this section follows a clear and logical path that supports the conclusions reached, particularly the overall performance rating. It should be easy for readers to comprehend how the rating was determined.
- Result of the Assessment/Performance Rating if adopted by the SAI
- Table and Graph

ACKNOWLEDGEMENT

We wish to express our appreciation to the officials and personnel of <name of Agency> for the support and cooperation extended to the audit team during the audit.

FOLLOW-UP AUDIT ANNEXURES

Annex – I (AAPSI)

<AGENCY NAME>

AGENCY ACTION PLAN AND STATUS OF IMPLEMENTATION (AAPSI)

Information Systems Performance Evaluation Observations and Recommendations

Audit Period: _________________

As of _______________________

Audit Observations	Audit Recommendations	Management Action Plan				Status of implementation	Reason for Non-Implementation	Action Taken/ Action to be Taken
		Action Plan	Person/ Department Responsible	Target Implementation Plan				
				From	To			

____

<Name and Signature>
Position of Auditee's Officer
Date: _________

Note: Status of Implementation

a. Fully Implemented
b. Partially Implemented
c. Not Implemented

Annex - I (AAPSI)

How to Accomplish the AAPSI:

The Auditee's Management is responsible for acting upon the observations and recommendations provided by the SAIs during the ISPE. The AAPSI is a tool to signify its action plans on the observations and recommendations provided by the auditors. This serves as the basis for monitoring the agency's action plans. Management should submit the AAPSI within six months from receipt of the final ISPE Report.

1. AUDIT OBSERVATIONS AND RECOMMENDATIONS – indicate the topic sentence and recommendations as stated in the ISPE report.

2. AGENCY ACTION PLAN – indicates the Auditee's response to the recommendations provided by the auditors during the audit. The agency shall fill this, detailing the appropriate resolution on the audit observations.

3. PERSON/DEPARTMENT RESPONSIBLE – the agency shall specifically identify the person or department responsible for implementing the action plan provided. If it is not possible to identify the person, the position or rank shall suffice.

4. TARGET IMPLEMENTATION DATE – the action plan provided by the agency shall be time-bound.

5. IMPLEMENTATION STATUS – the following are the selections for the status of the implementation of the action plans:

   - FULL – action plans have been fully implemented
   - PARTIAL – action plans are implemented in some areas
   - NOT-IMPLEMENTED – Management did not implement the action plan within the target completion date

6. REASON FOR DELAY/ NON-IMPLEMENTATION – indicates the reasons why the action plan was delayed or not implemented

7. ACTION TAKEN/ ACTION TO BE TAKEN – indicate Management's corrective actions to compensate for the delay or non-implementation of the action plans.

Example accomplished AAPSI:

AGENCY A
AGENCY ACTION PLAN AND STATUS OF IMPLEMENTATION (AAPSI)

Information Systems Performance Evaluation Observations and Recommendations

Audit Period: April 4 to December 31, 2022

As of June 30, 2023

Audit Observations	Audit Recommendations	Management Action Plan				Status of implementation	Reason for Non-Implementation	Action Taken/ Action to be Taken
		Action Plan	Person/ Department Responsible	Target Implementation Plan				
				From	To			
The non-conformance with good practices in system development, acquisition, and IT project management and the inefficient monitoring process resulted in fragmented IT solutions, significant missing system requirements, and partially non-attainment of project objectives, which led to the wastage of government resources and violations of rules and regulations.	We recommended that Management develop and implement a framework and policy for developing, acquiring, implementing, and maintaining IT systems and related technology.	Noted and accepted. The IT System Development Methodology and Framework will be formulated and presented to the IT Steering Committee for review. After that, the head of the agency will review and approve it for implementation.	Planning Division	July 2023	Dec 2023	Not Implemented	Budget constraints Lack of personnel	To request additional funding To hire consultant
Inadequate IT Continuity and Disaster Recovery Plan (DRP) increases the risk of being unable to	We recommended updating and revising the IT DRP in accordance with	We will revise and update the IT DR Plan	IT Department	July 2023	Dec 2023	Partially Implemented	The authorized officials are facing time constraints in	Drafted the revised IT DRP

Audit Observations	Audit Recommendations	Management Action Plan				Status of implementation	Reason for Non-Implementation	Action Taken/ Action to be Taken
		Action Plan	Person/ Department Responsible	Target Implementation Plan				
				From	To			
provide quality public services during disruptive incidents or emergencies.	the requirements of applicable rules, regulations, and standards. Have the plans approved by authorized officials and ensure to disseminate them to all concerned personnel.						reviewing the revised IT DRP.	Subject to approval of authorized official
Absence of a remote recovery site or backup information processing facility.	We recommended that Management immediately implement a backup processing facility or remote recovery site for all essential components of computer operations in accordance with the provisions of the applicable rules, regulations, and standards.	The remote DR site is included in the CY 2024 Plans and Program	IT and Budget Departments	CY2024		Not Implemented	Subject to the approval of the funds	We already requested for the budget

Annex- II (APMT)

ACTION PLAN MONITORING TOOL (APMT)

Information Systems Performance Evaluation Observations and Recommendations
On <Name of Auditee>
Audit Period: ___________________
As of __________________________

Audit Observations	Audit Recommendations	Auditee's Action Plan				Result of Auditor's Follow-up Activity				
		Action Plan	Person/ Department Responsible	Target Implementation Plan		Date of Follow-up	Implementation Status	Actual Implementation Date	Reason for Delay/ Non-Implementation	Remarks
				From	To					

Prepared by:

<Name>
Audit Team Leader

Approved by:

<Name>
Audit Team Supervisor

Annex - II (APMT)

How to Accomplish the APMT:

The following elements are to be lifted from the AAPSI provided by the Auditee Management:

- Audit Observation
- Audit Recommendation
- Management Action Plan/ Comment
- Person/Department Responsible
- Target Date of Implementation
- Status of Implementation
- Reason for Non-Implementation
- Action Taken/ Action to be Taken

The columns provided under the APMT portion are developed to guide the Auditor in the conduct of monitoring procedures.

1. DATE OF FOLLOW-UP – Indicate the date when the follow-up is made

2. IMPLEMENTATION STATUS – The Auditor shall answer this column during the execution of the monitoring procedures. The following are the selections for the status of the implementation of the action plans:

   a. FULL – action plans have been fully implemented in all scopes mentioned
   b. PARTIAL – action plans are partially implemented in some areas or are currently being done
   c. NON-IMPLEMENTATION – Management did not implement the action plan within the target completion date

3. ACTUAL IMPLEMENTATION DATE – Part of the Auditor's examination determines the actual implementation date of the action plan set by an agency. Comparison of the actual against the target date for the implementation of action plans is significant, particularly on interrelated audit observations and action plans.

4. REASON FOR DELAY/ NON-IMPLEMENTATION – Auditors shall uncover the reasons for the delay or non-implementation of action plans. If the circumstances permit, auditors shall inquire concerned agency officers and personnel about the causes of the delay or non-implementation.

5. REMARKS – This column is for the Auditor's comments or actions to be taken as a result of the monitoring procedures conducted. This column can also be a basis for the next year's audit project.

CHAPTER 05

Survey on IS Performance Evaluations

Chapter 05

In order prepare the guidance document and have a sound understanding of ISPE practices in vogue across SAI as survey was carried out in 2021. The contents of the survey its results and analysis on these results is detailed in this section.

Purpose of Survey document

Accordingly, the subject project *"[83]envisages preparation of Guidance based document to facilitate SAIs' in carrying out performance evaluation of Information Systems. The document would look to propose best practices and steps that could be deployed to objectively and comprehensively evaluate the performance of Information Systems. It would be a live document subject to future revisions".*

In this context, the subject survey document is being submitted to solicit valuable comments and submissions on the proposed guidance document from member SAIs'. The aim is to gather comprehensive data on existing practices/standards/guidelines being used in the performance evaluations of IT systems by different SAIs, the challenges that are faced in executing such assignments, and the key aspects/ parameters that should be part of the proposed guidance, enabling a quality product to be prepared.

Note	• For Yes/No attributes please select only one choice • For multiple check-box attributes please select as many you feel relevant to your reply • Please attach extra detail against any survey question as felt necessary for your reply by adding a separate page and giving it reference to the relevant question.

Section 5.1 SAI Polices & Procedures Pertaining to IS Performance Evaluation

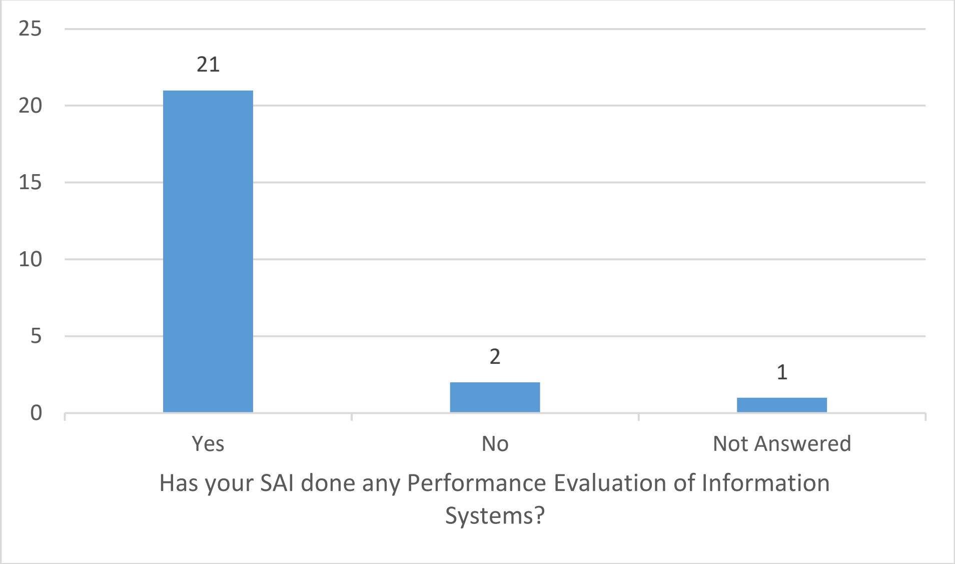
The survey received <u>24 responses</u>, of which the following information was gathered from.

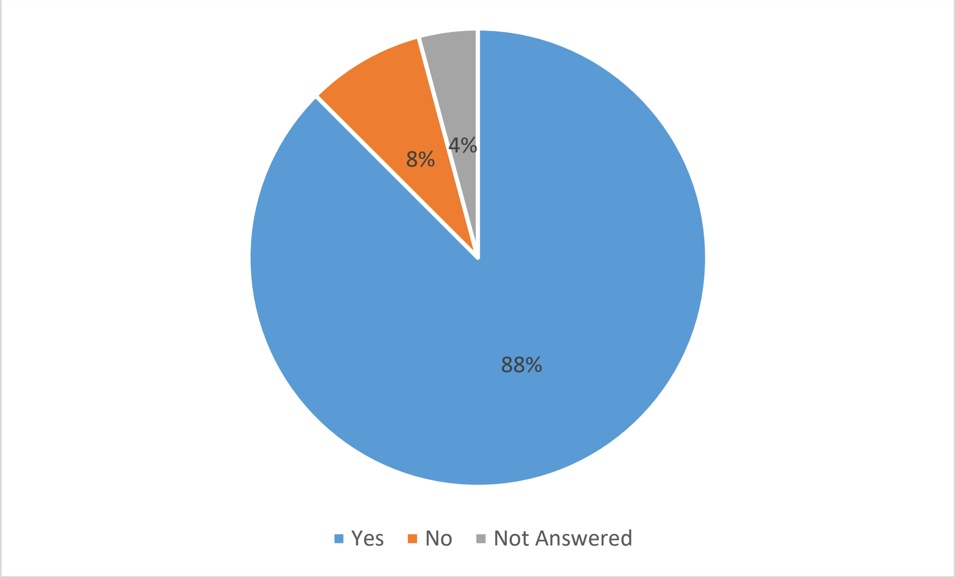
5.1.1 Has your SAI done any Performance Evaluation of Information Systems?

□ Yes
□ No

(Note: In-case of no-prior experience in IS performance evaluations please have a look at Section 5 of this survey specifically, besides any contribution you feel like making.)

[83] Description of Project as per approved PID

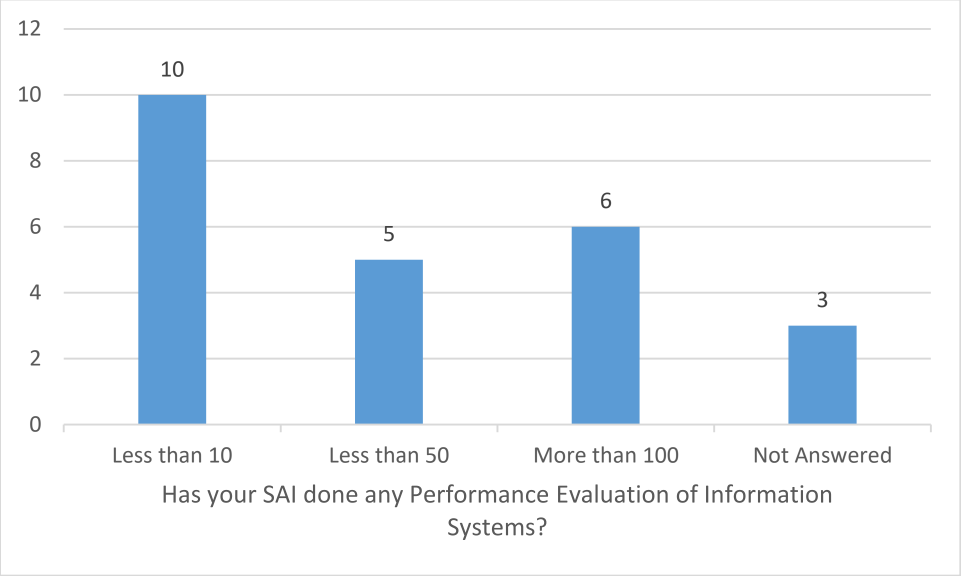


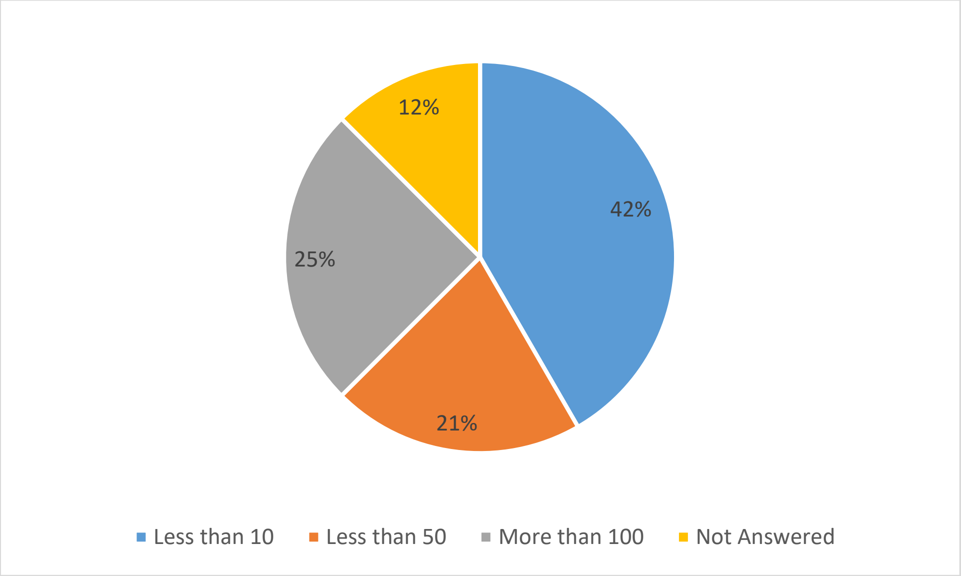


Additional Remarks:

5.1.2 How many Performance Evaluations of Information Systems have been done by your SAI during last five years?*(in case of yes against Q.2)*

□ Less than 10
□ Less than 50
□ More than 100





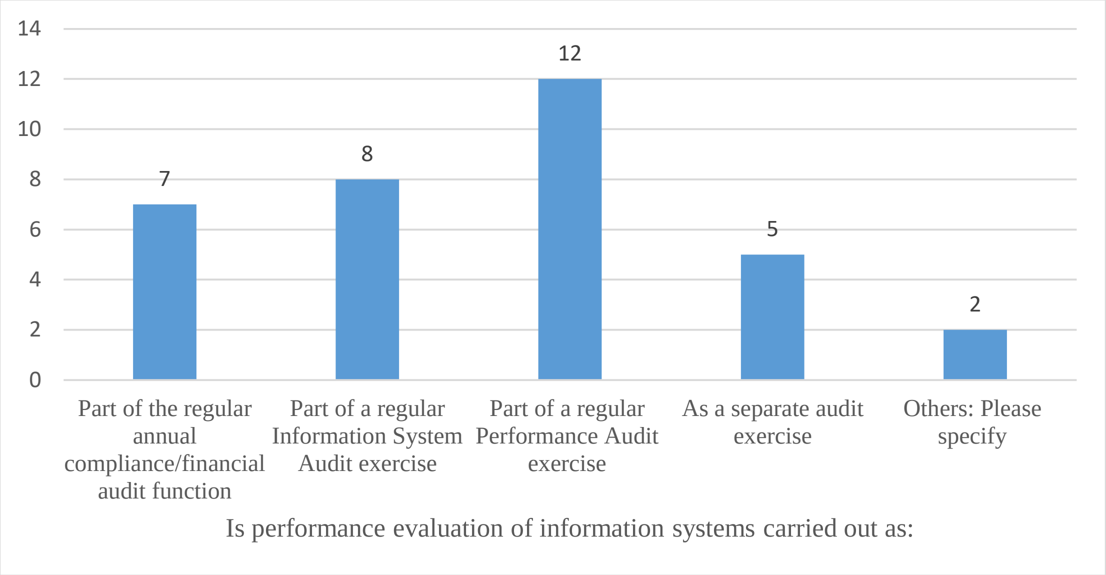
Additional Remarks:

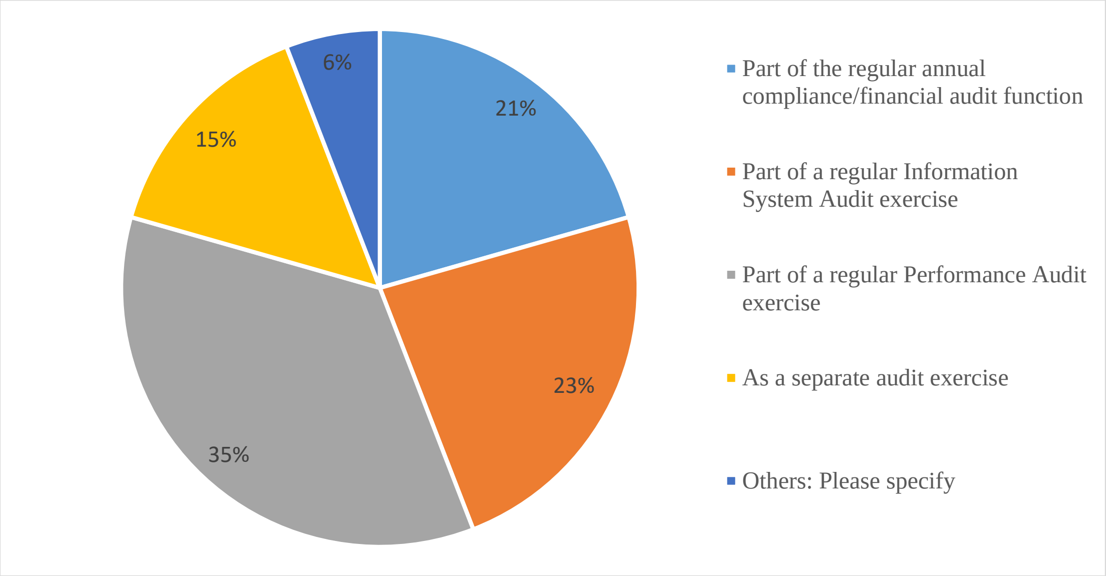
____

5.1.3 Is performance evaluation of information systems carried out as:

(Kindly select one option)

□ Part of the regular annual compliance/financial audit function
□ Part of a regular Information System Audit exercise
□ Part of a regular Performance Audit exercise
□As a separate audit exercise
□ Others: Please specify ____)

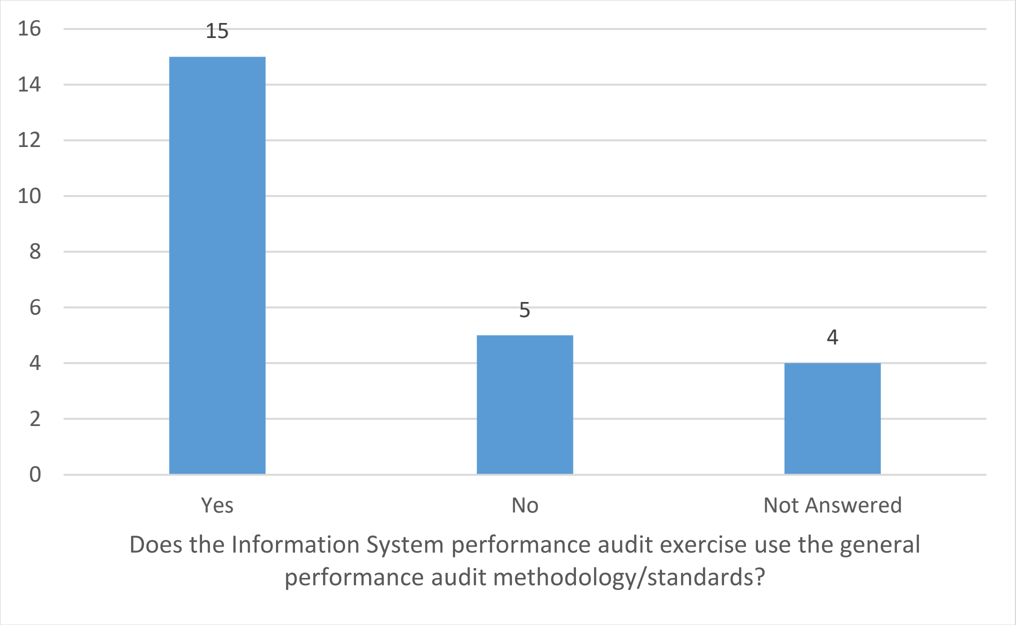


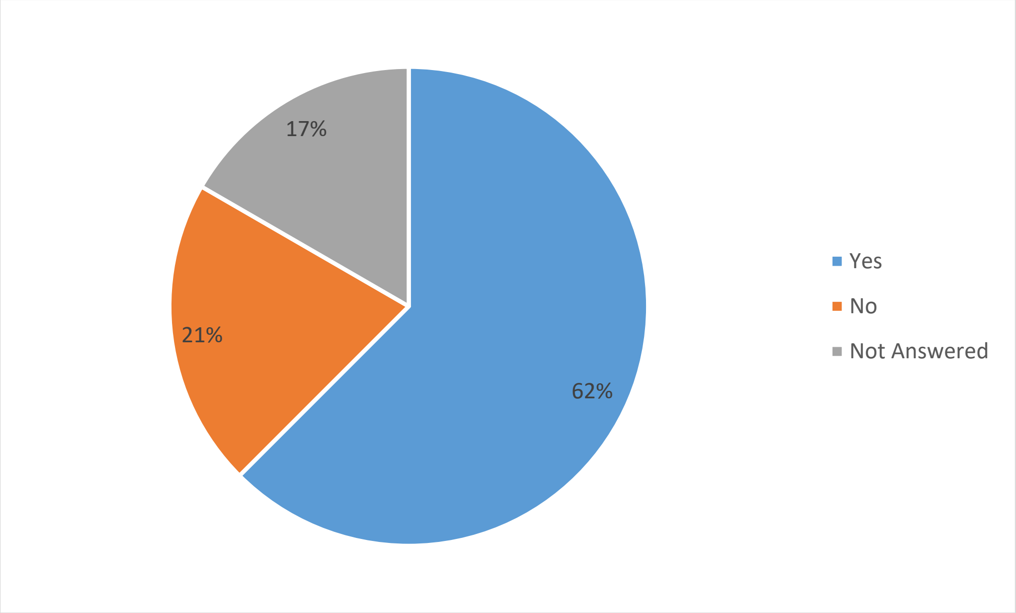


Additional Remarks:

5.1.4 Does the Information System performance audit exercise use the general performance audit methodology/standards?

□ Yes
□ No

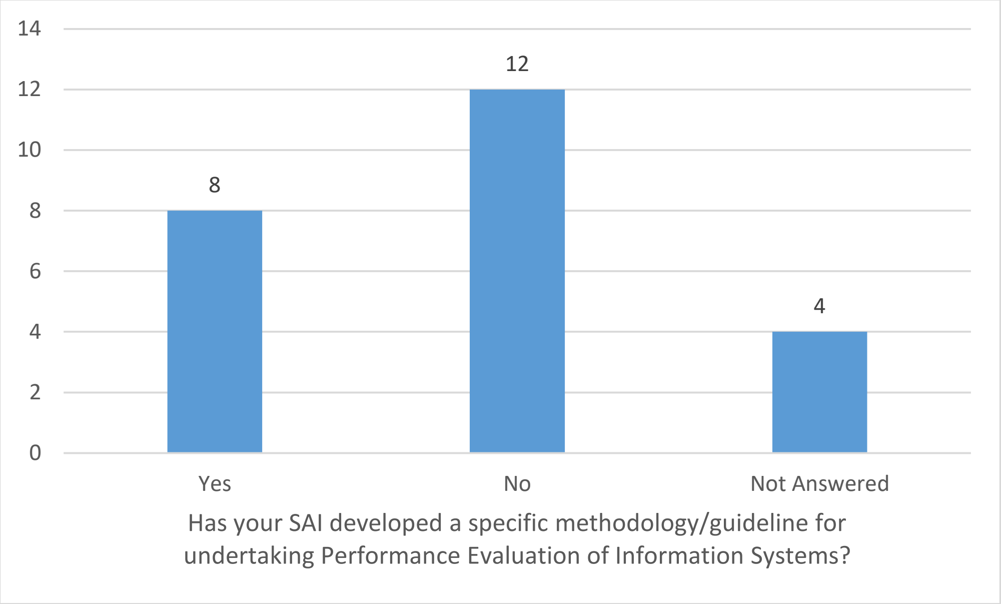


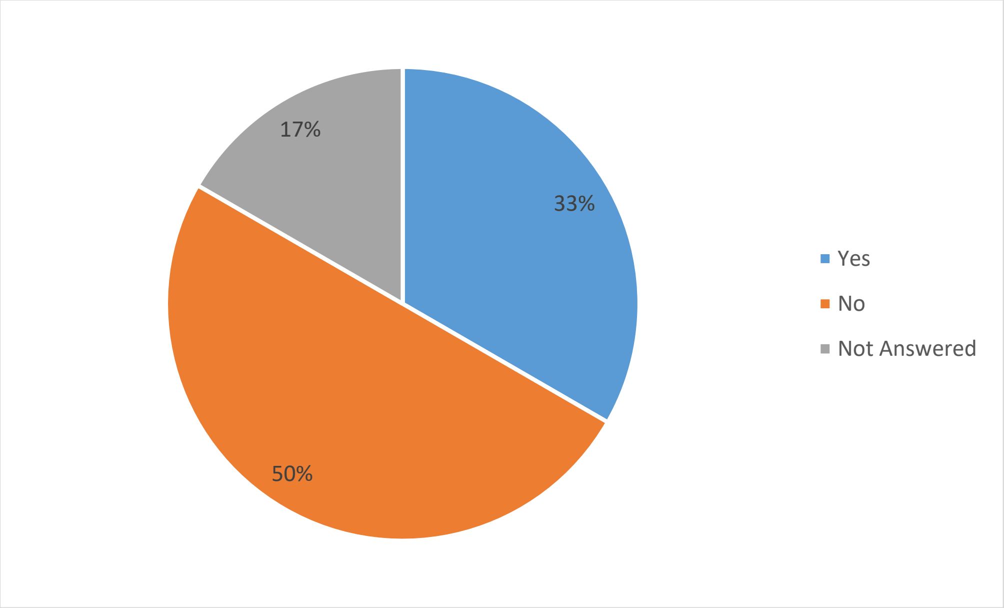


Additional Remarks:

5.1.5 Has your SAI developed a specific methodology/guideline for undertaking Performance Evaluation of Information Systems?

□ Yes
□ No





Additional Remarks:

1.5.(A) If yes then kindly share softcopy of the subject guideline/methodology for review and reference in current WGITA project

5.1.6 Does your SAI use international/regional standards/guidelines or any specified best practices for performance evaluation of an information system. (e.g. ISO, COBIT, ITIL)

☐ Yes
☐ No

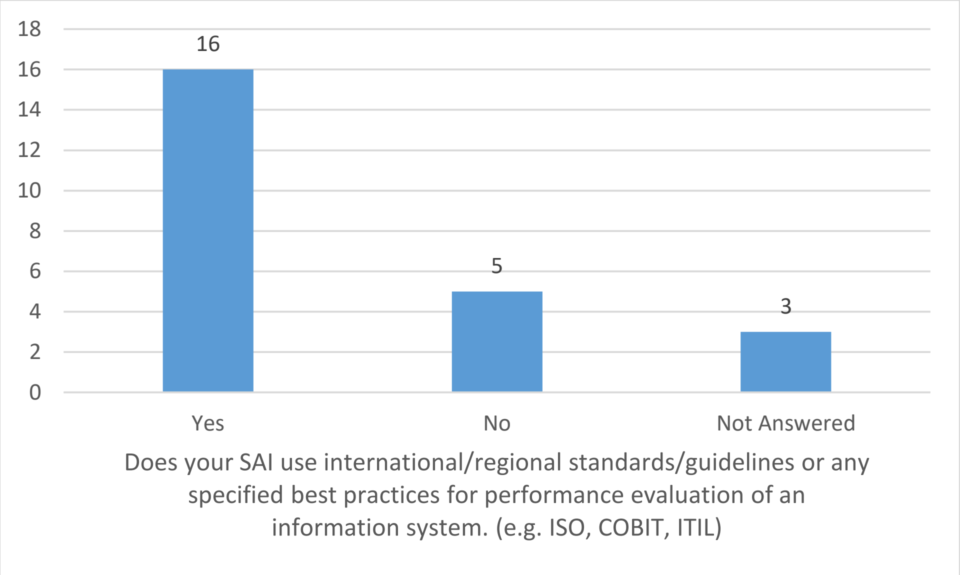
If yes then kindly list any four such standards/guidelines or best practices used

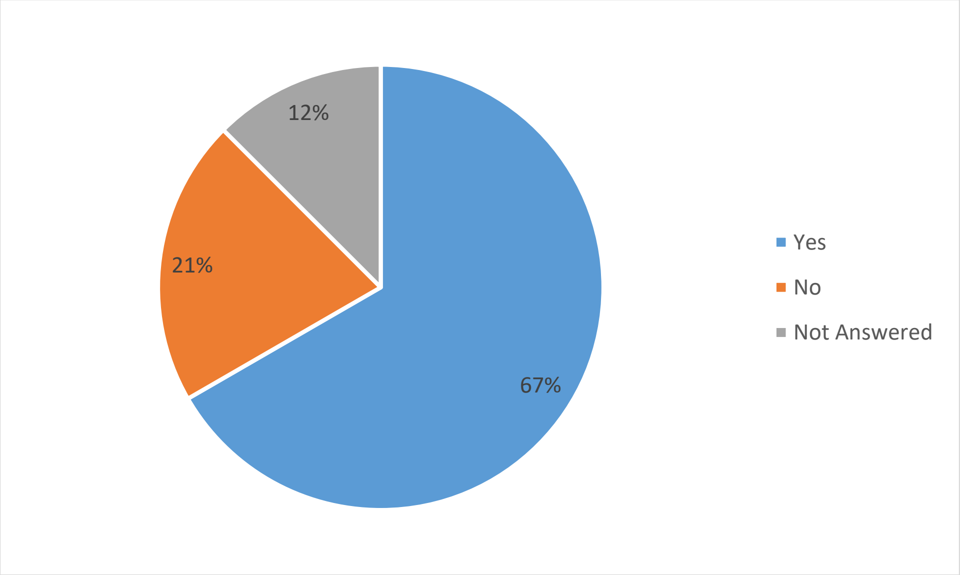
____

____

____

____



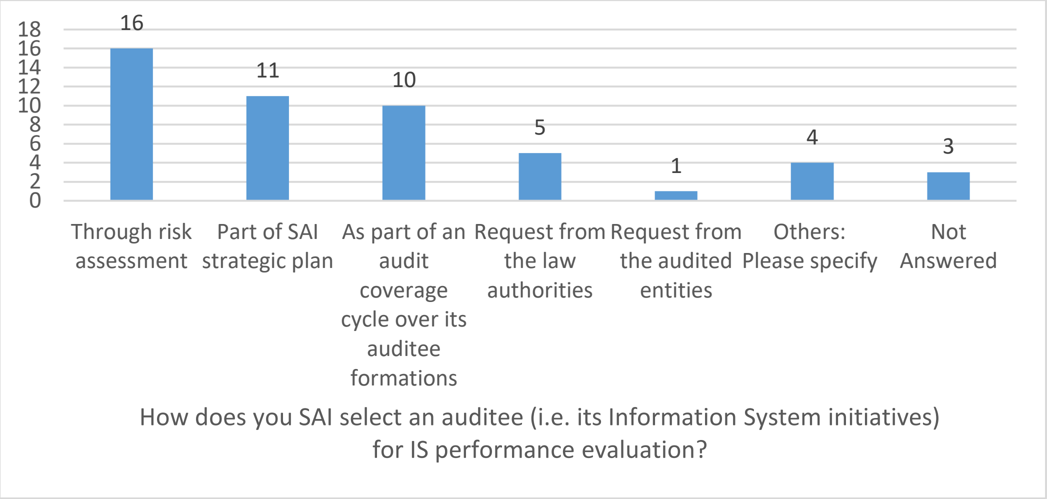


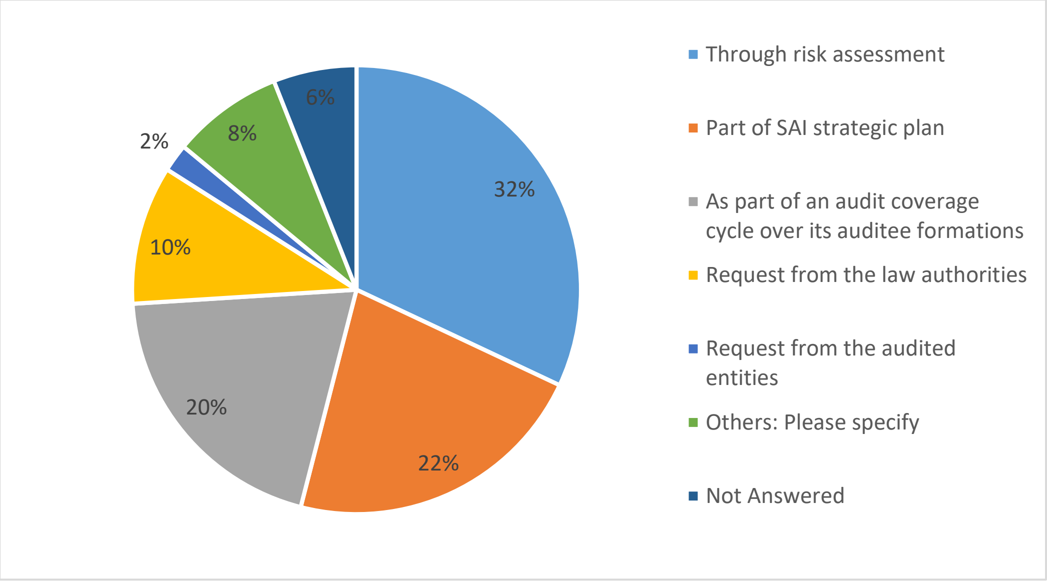
Section 5.2 Planning For the IS Performance Evaluation Exercise

5.2.1 How does you SAI select an auditee (i.e., its Information System initiatives) for IS performance evaluation?

□ Through risk assessment
□ Part of SAI strategic plan
□ As part of an audit coverage cycle over its auditee formations
□ Request from the law authorities

□ Request from the audited entities
□ Others: Please specify ____)





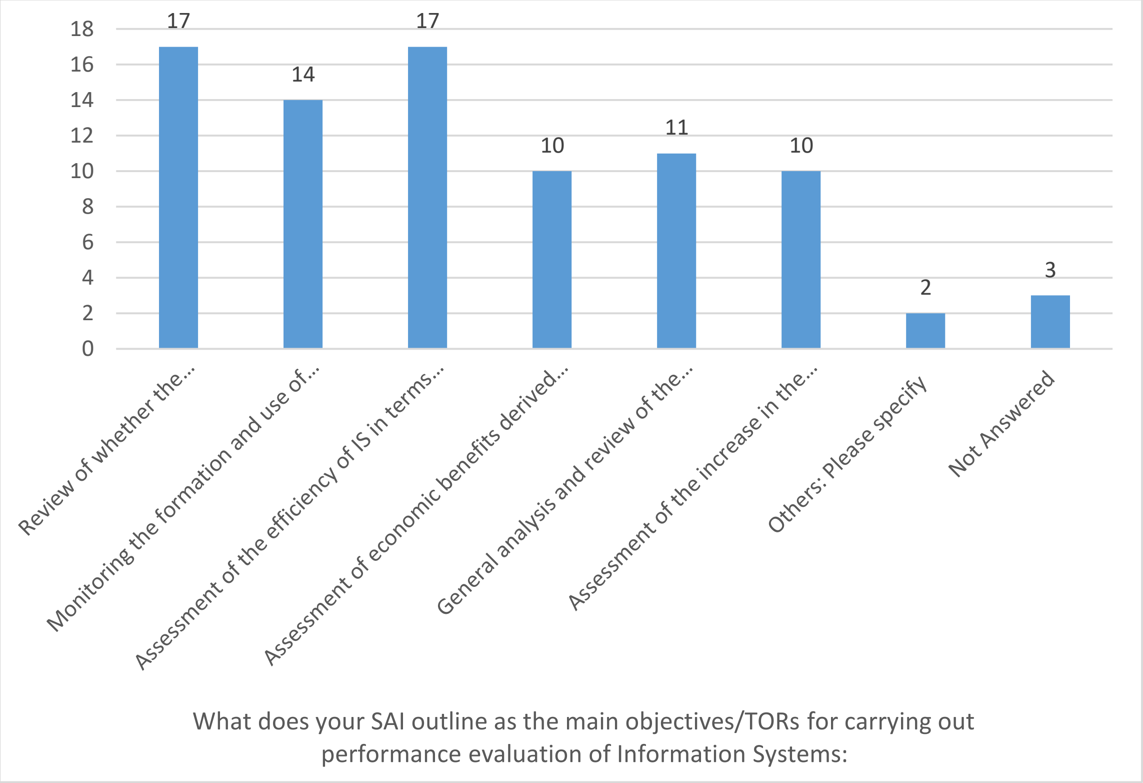
Additional Remarks:

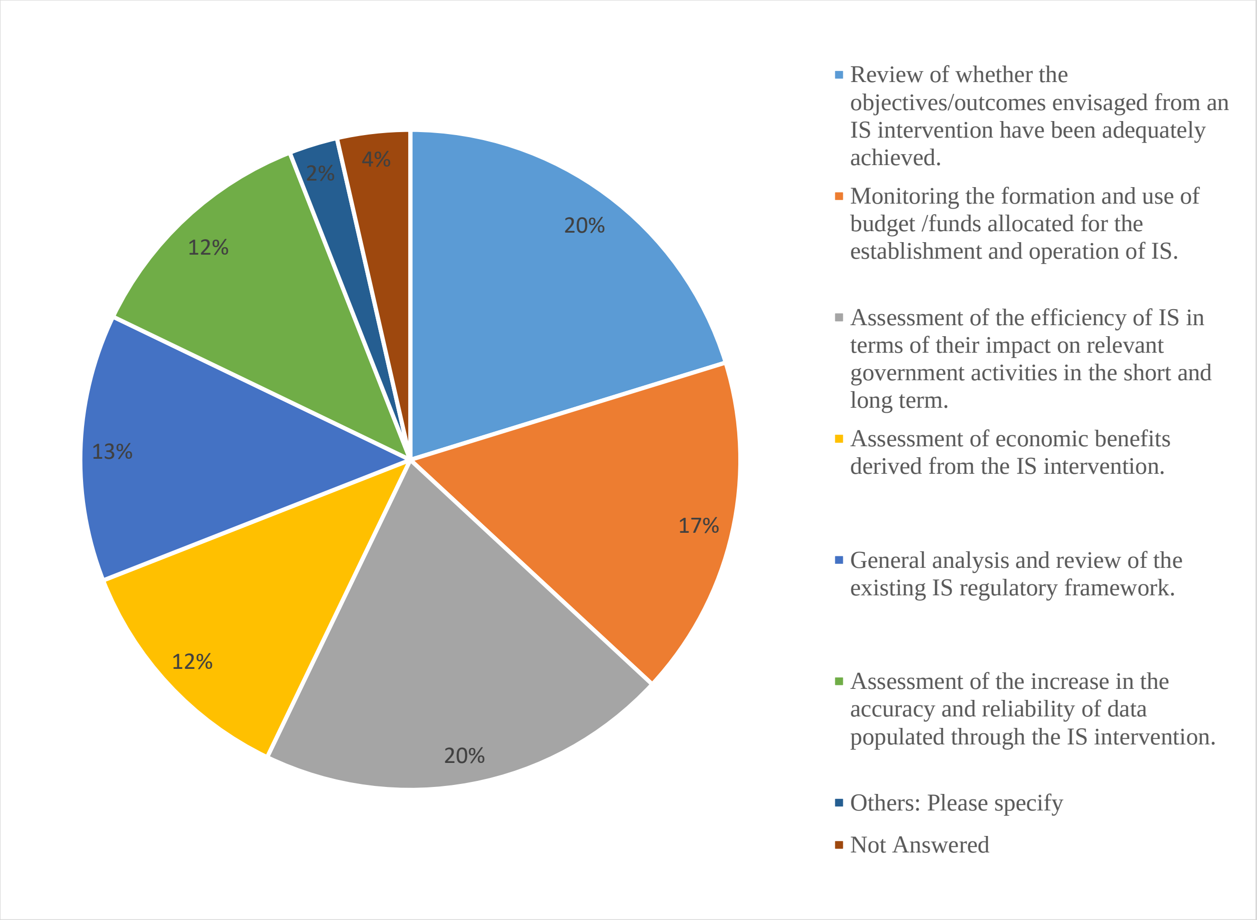
5.2.2 What does your SAI outline as the main objectives/TORs for carrying out performance evaluation of Information Systems:

□Review of whether the objectives/outcomes envisaged from an IS intervention have been adequately achieved.
□ Monitoring the formation and use of budget /funds allocated for the establishment and operation of IS.
□Assessment of the efficiency of IS in terms of their impact on relevant government activities in the short and long term.
□Assessment of economic benefits derived from the IS intervention.
□General analysis and review of the existing IS regulatory framework.

□Assessment of the increase in the accuracy and reliability of data populated through the IS intervention.

□ Others: Please specify ____)



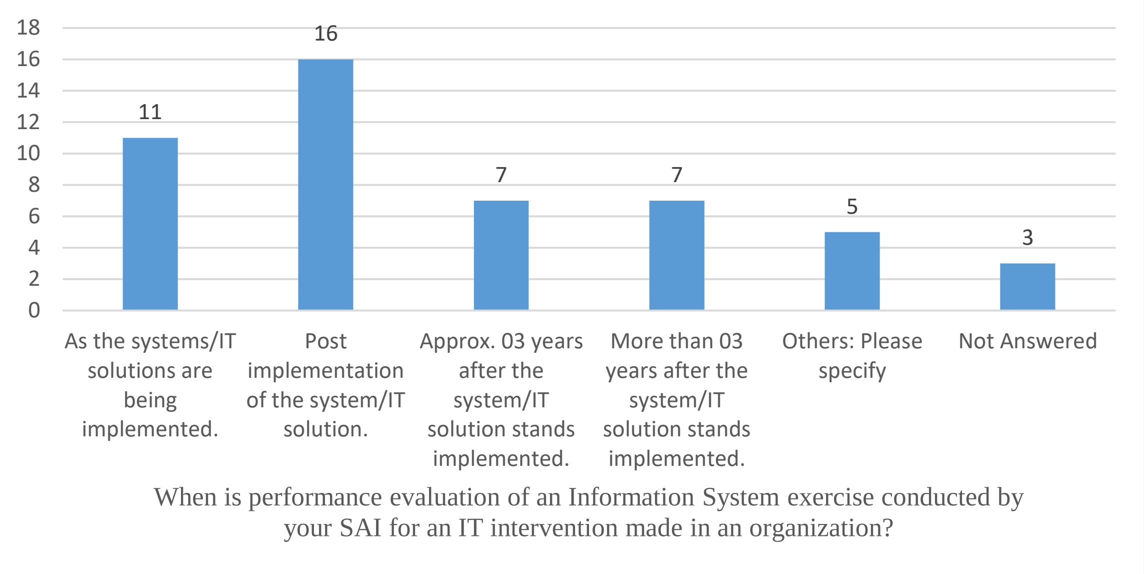


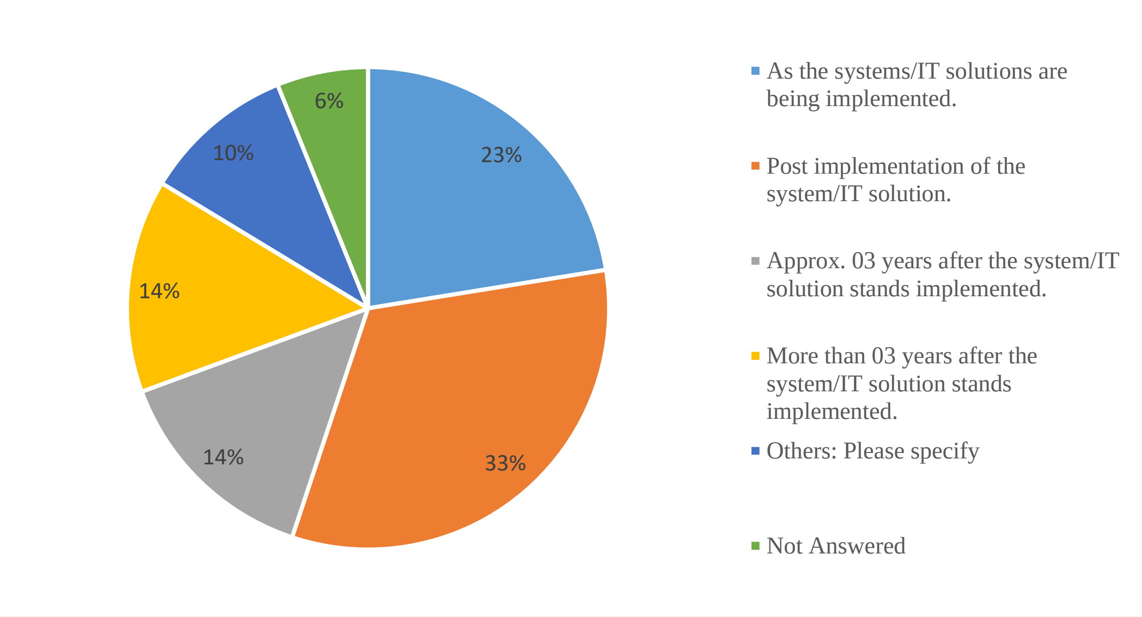
Additional Remarks:

____

5.2.3 When is performance evaluation of an Information System exercise conducted by your SAI for an IT intervention made in an organization?

□As the systems/IT solutions are being implemented.
□ Post implementation of the system/IT solution.
□Approx. 03 years after the system/IT solution stands implemented.
□More than 03 years after the system/IT solution stands implemented.
□ Others: Please specify ____)





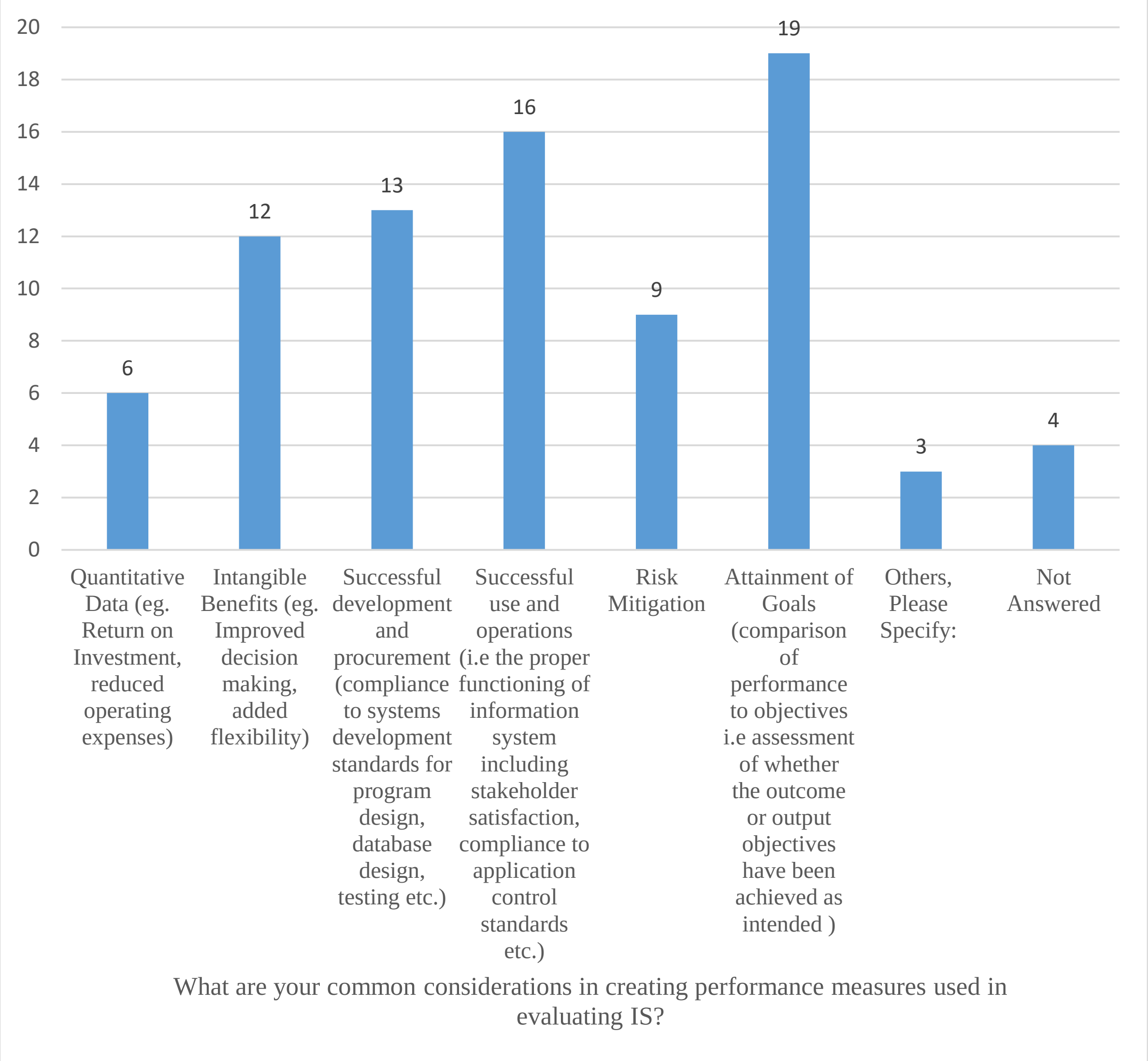
Additional Remarks:

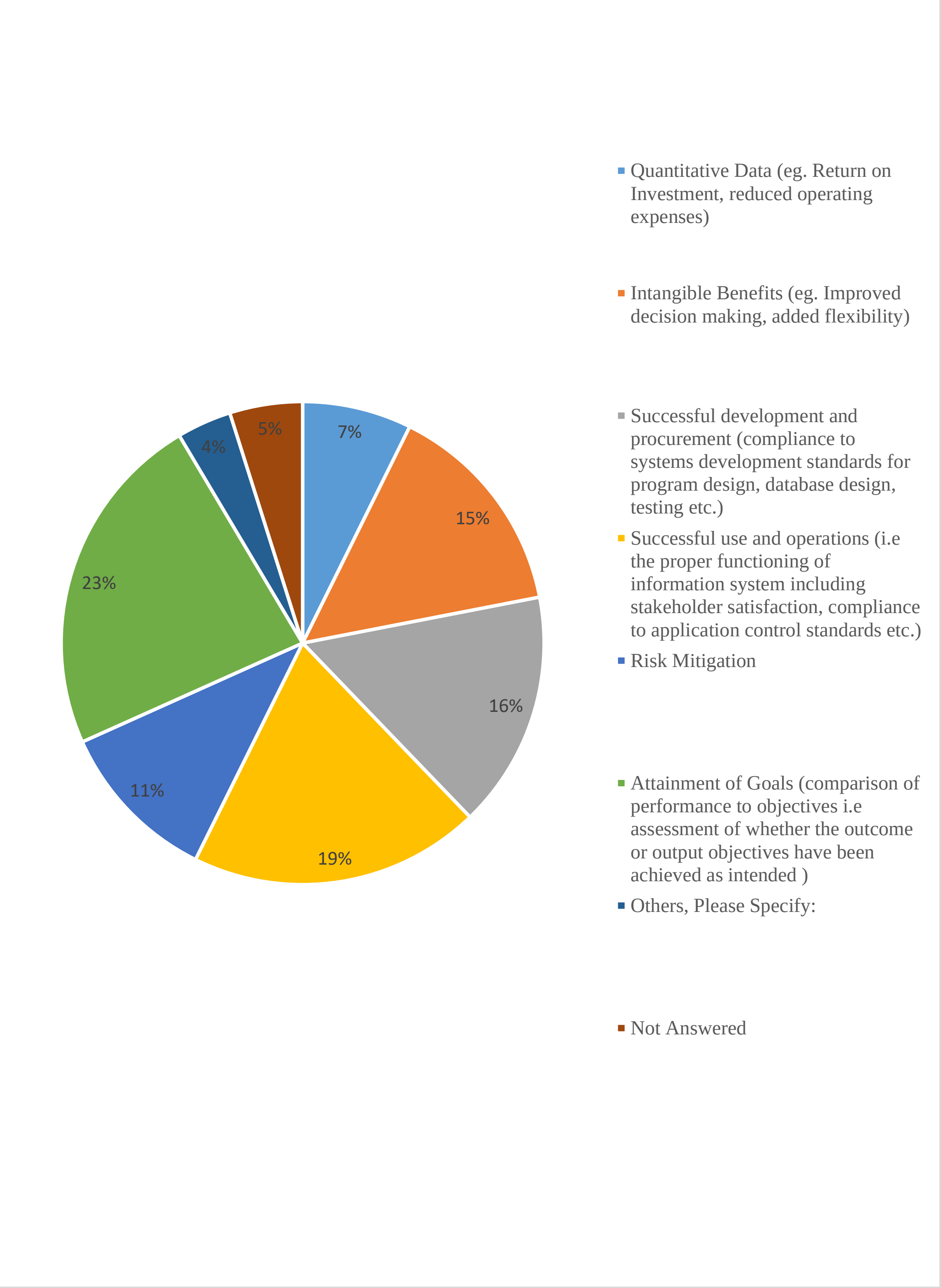
5.2.4 What are your common considerations in creating performance measures used in evaluating IS?

□Quantitative Data (eg. Return on Investment, reduced operating expenses)
□ Intangible Benefits (eg. Improved decision making, added flexibility)
□Successful development and procurement (compliance to systems development standards for program design, database design, testing etc.)
□Successful use and operations (i.e the proper functioning of information system including stakeholder satisfaction, compliance to application control standards etc.)
□ Risk Mitigation

□ Attainment of Goals (comparison of performance to objectives i.e assessment of whether the outcome or output objectives have been achieved as intended)

□ Others, Please Specify:



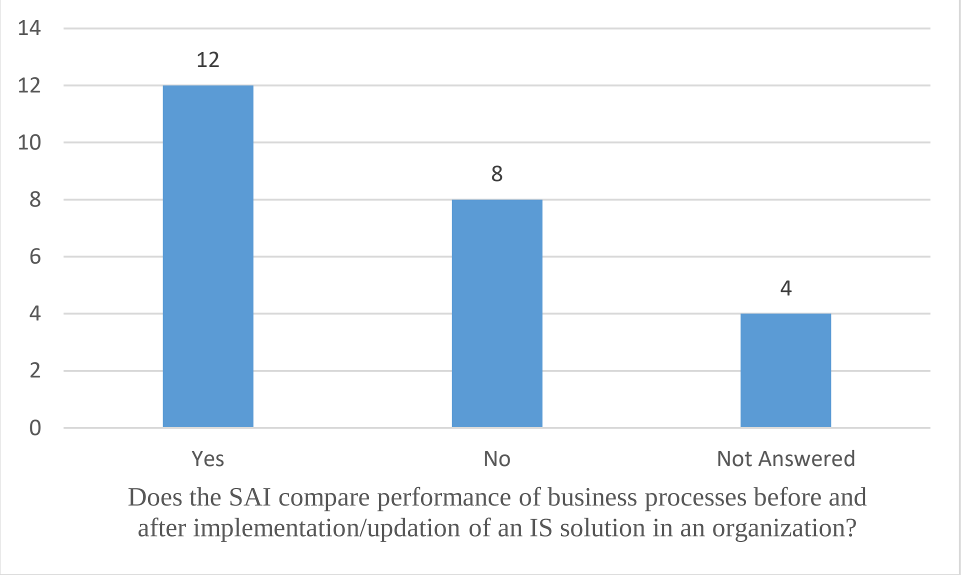


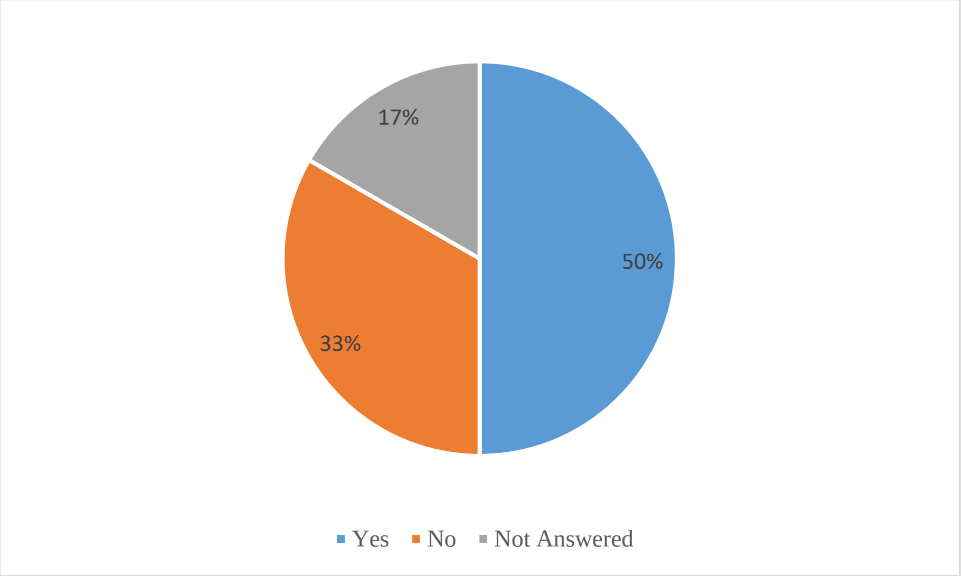
Additional Remarks:

Section 5.3 Execution of IS Performance Evaluation Exercise

5.3.1 Does the SAI compare performance of business processes before and after implementation/updation of an IS solution in an organization?

□ Yes
□ No

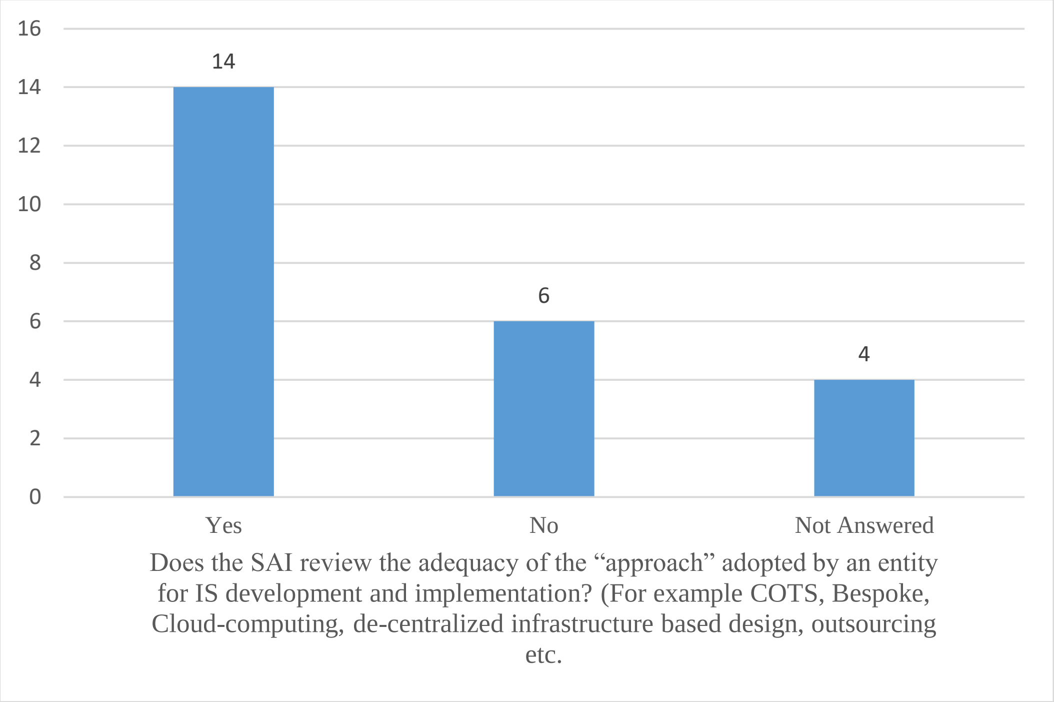


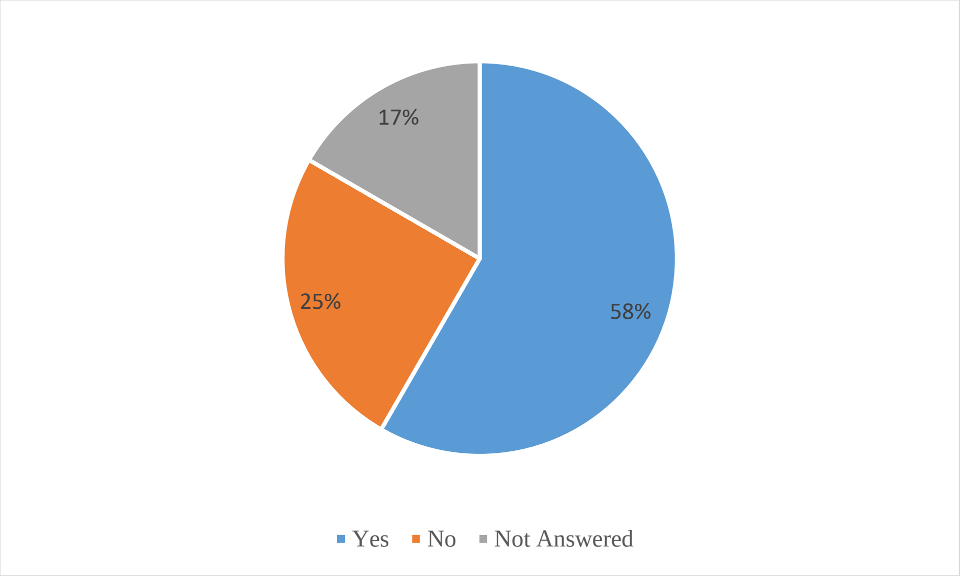


Additional Remarks:

5.3.2 Does the SAI review the *adequacy* of the *“approach”* adopted by an entity for IS development and implementation? (For example COTS, Bespoke, Cloud-computing, de-centralized infrastructure based design, outsourcing etc.

□ Yes
□ No

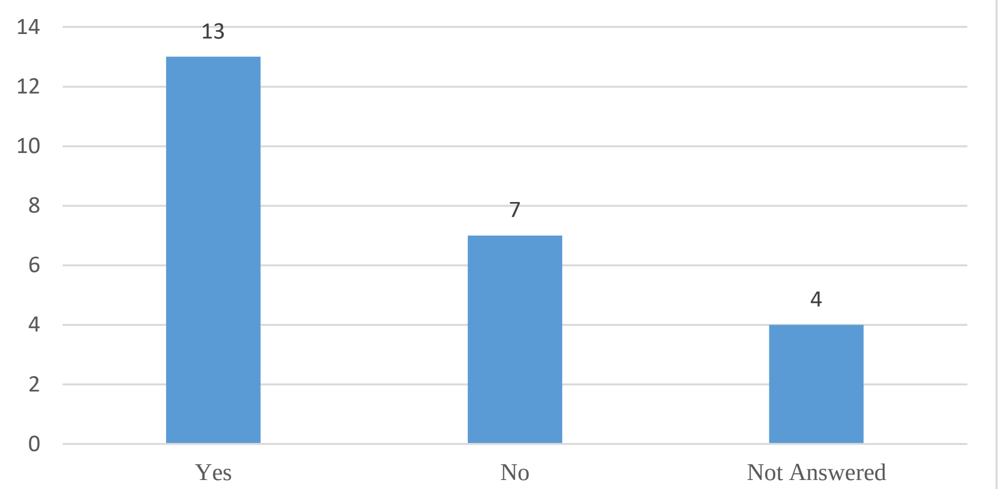




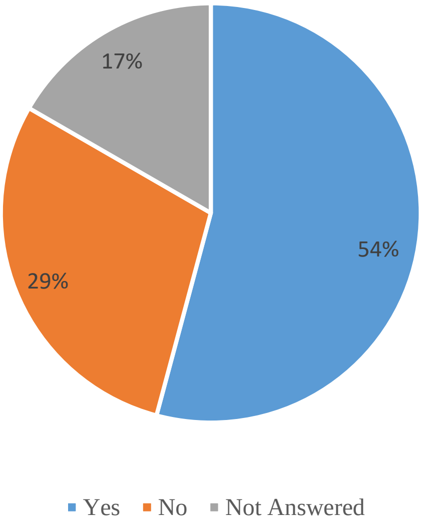
Additional Remarks:

5.3.3 Does the SAI ascertain to what extent an organization's HR resources especially operational staff and line/field offices have the capability to utilize full benefits of an a new IT intervention?

□ Yes
□ No



Does the SAI ascertain to what extent an organization's HR resources especially operational staff and line/field offices have the capability to utilize full benefits of an a new IT intervention?



Additional Remarks:

5.3.4 From the perspective of assessing performance which of following topics/areas are included/focused upon in your SAI's performance evaluation of IS? Kindly put check mark on the "Audited" column.

Please also rate the areas based on what you think is the most frequently assessed and relevant/important to evaluate in your SAI.

Rating: 3- Most relevant, always included in the evaluation
2- Relevant but not often included in the evaluation
1- Not relevant but rarely included in the evaluation

0- Not at all relevant
N/A- The SAI has no authority/mandate to audit the topic
(All evaluations being from performance point of view)

Sr. No.	Area	3. Most relevant, always included in the evaluation	2. Relevant but not often included in the evaluation	1. Not relevant but rarely included in the evaluation	0. Not at all relevant
1	IT Governance	67	26	8	0
2	Development and Acquisition	32	23	3	0
3	IT Operations	34	25	12	0
4	Data Management	27	40	9	0
5	Outsourcing	49	42	9	0
6	Information Security	55	40	12	0
7	Application Controls	22	27	16	0
8	Electronic Government/Electronic Governance/Mobile Governance	11	12	3	0
9	Electronic Commerce	2	6	11	0
10	Business Continuity and Resilience	11	17	7	0

AREA	SUB-TOPICS	Weighted Score (Higher means more relevant)
IT Governance	Business Needs Identification, Direction and Monitoring	44
	Role/oversight of senior management over IS implementation	44
	IT Strategy	45
	Organizational Structure, Policy and Procedures	47
	People and Resources	40
	Risk Assessment and Compliance Mechanism	41
Development and Acquisition	Requirements Development and Management	37
	Project Management and Control	40
	Quality Assurance and Testing	32
	Configuration and Change Management	36
IT Operations	Service Management	29
	Capacity Management	23
	Problem and Incident Management	33

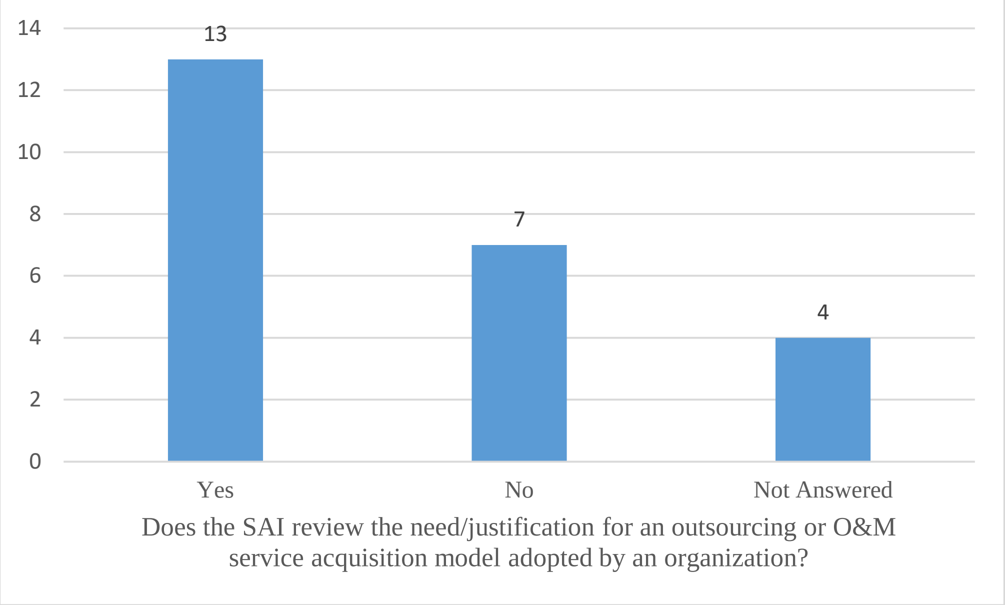
AREA	SUB-TOPICS	Weighted Score (Higher means more relevant)
	User access management	40
	Change Management	39
Data Management	Consistency and reliability of data	37
	Abstraction of data	27
	Ownership of the data	32
	Data storage and recovery	37
	Data Security	37
Outsourcing	Outsourcing Policy	36
	Vendor or Contractor Monitoring	37
	Data Rights	32
	Service Level Agreement	34
	Sustainability of system functions	28
	Security and privacy	39
	Cost Control and Management	34
Information Security	Risk Assessment	36
	Information Security Policy	44
	Communication and Operations Management	33
	Asset Management	35
	Human Resources Security	31
	Physical Security	37
	Access Control	41
Application Controls	Input	33
	Processing	35
	Output	35
	Application Security	33
Electronic Government/ Electronic Governance/ Mobile Governance	Service Delivery	29
	Policy and Enforcement Mechanism	31
Electronic Commerce	E-Commerce Strategies and Security Mechanism	13
	Public Key Infrastructure	16
Business Continuity and Resilience	IT infrastructure sustainability and resilience	34
	HR capacity and resource management	23
	Financial sustainability in the medium and long term	17

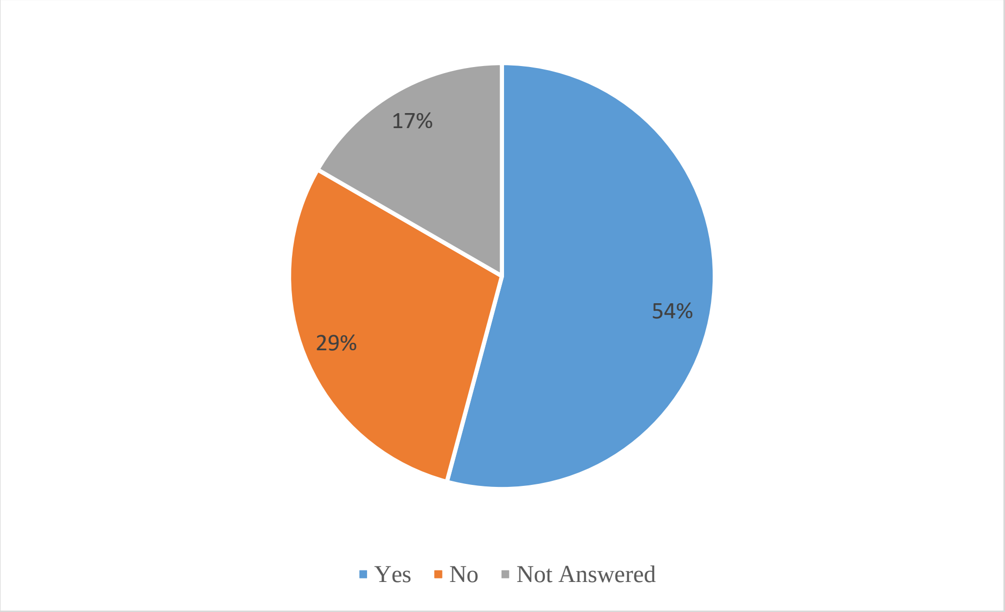
Additional Remarks:

Four (4) out of the 24 SAIs did not submit answers to this question

5.3.5 Does the SAI review the need/justification for an outsourcing or O&M service acquisition model adopted by an organization?

□ Yes
□ No

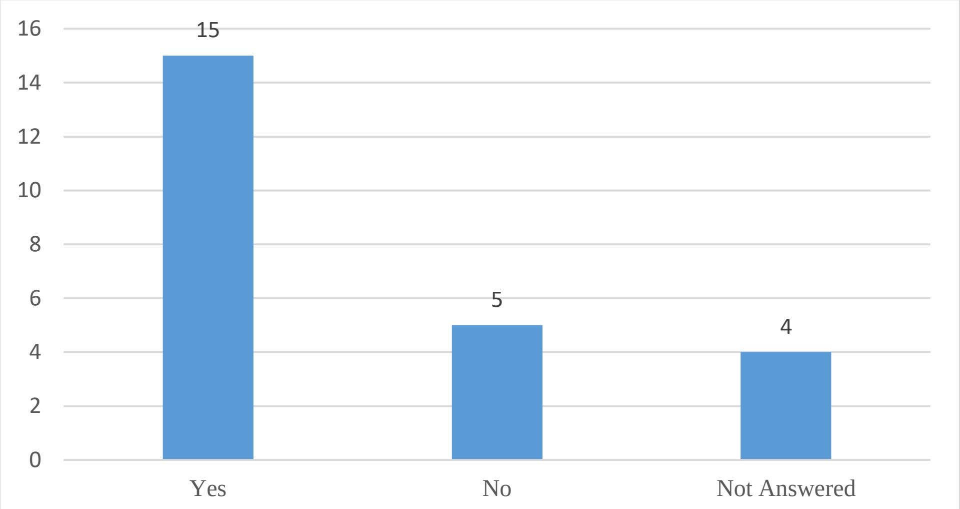




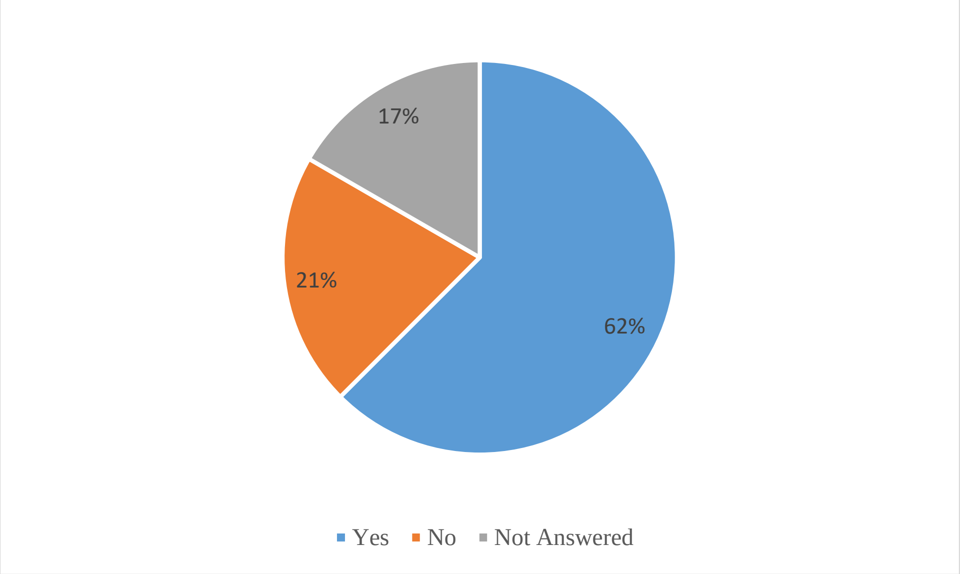
Additional Remarks:

5.3.6 In-case of outsourcing or O&M services acquisition (through SLA/contracts) used by an organization does the SAI review the performance of the 3rd party service provider (especially along the parameters of transparency, adequacy, security and efficiency)?

□ Yes
□ No



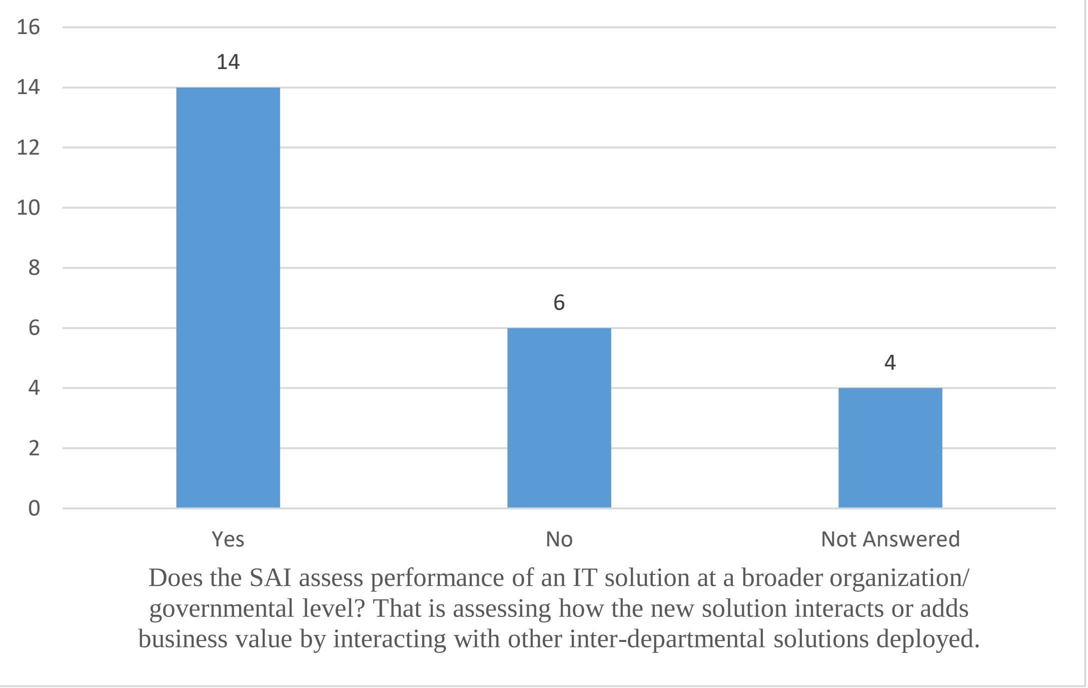
In-case of outsourcing or O&M services acquisition (through SLA/contracts) used by an organization does the SAI review the performance of the 3rd party service provider (especially along the parameters of transparency, adequacy, security and efficiency)?



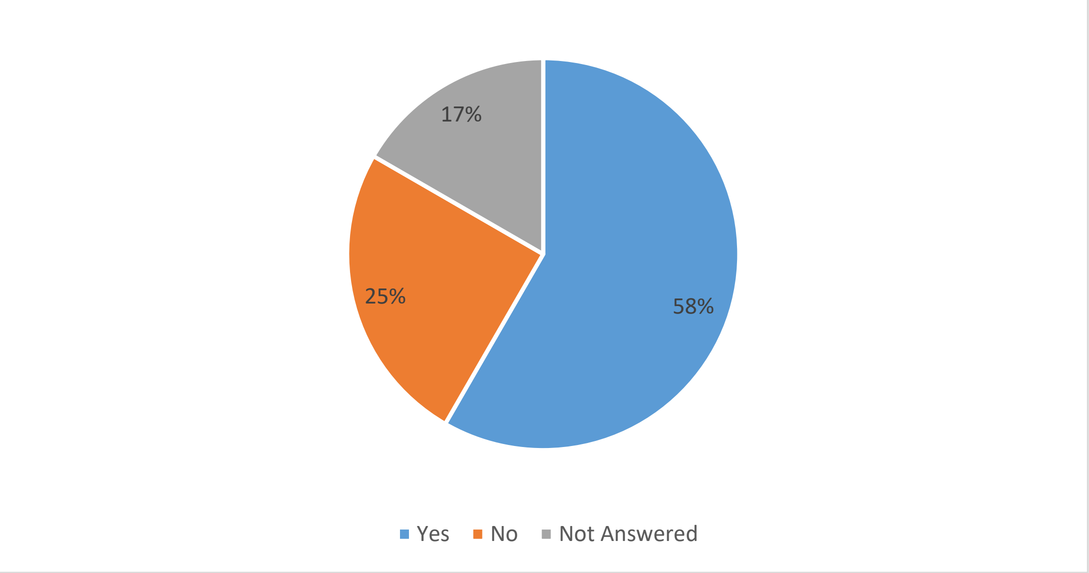
Additional Remarks:

5.3.7 **Does the SAI assess performance of an IT solution at a broader organization/ governmental level? That is assessing how the new solution interacts or adds business value by interacting with other inter-departmental solutions deployed.**

□ Yes
□ No



Does the SAI assess performance of an IT solution at a broader organization/ governmental level? That is assessing how the new solution interacts or adds business value by interacting with other inter-departmental solutions deployed.



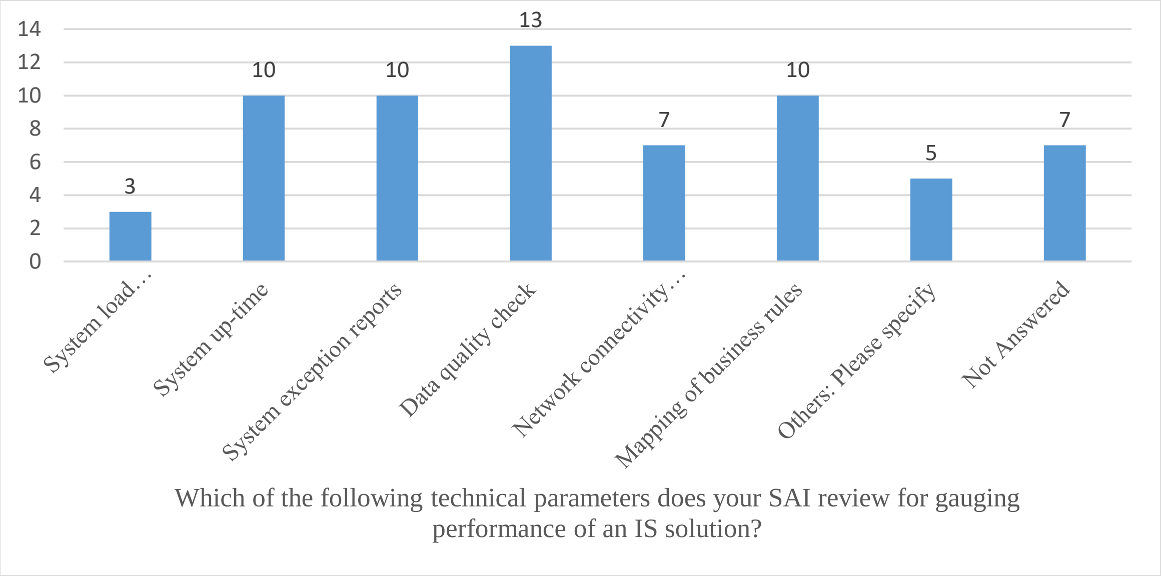
Additional Remarks:

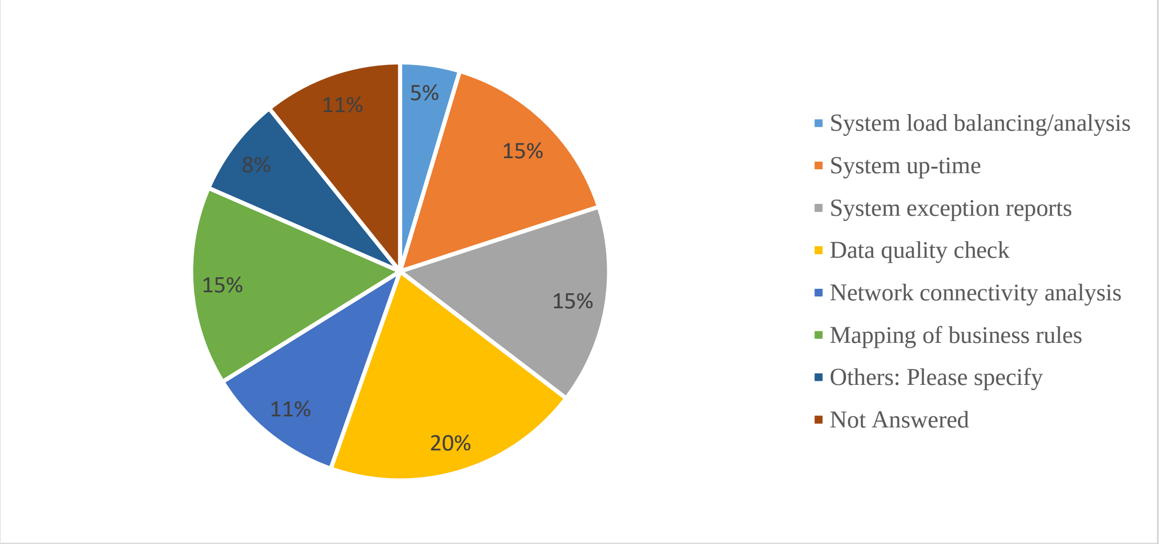
____

5.3.8 **Which of the following technical parameters does your SAI review for gauging performance of an IS solution?**

□ System load balancing/analysis
□ System up-time

□ System exception reports
□ Data quality check
□ Network connectivity analysis
□ Mapping of business rules
□ Others: Please specify:____

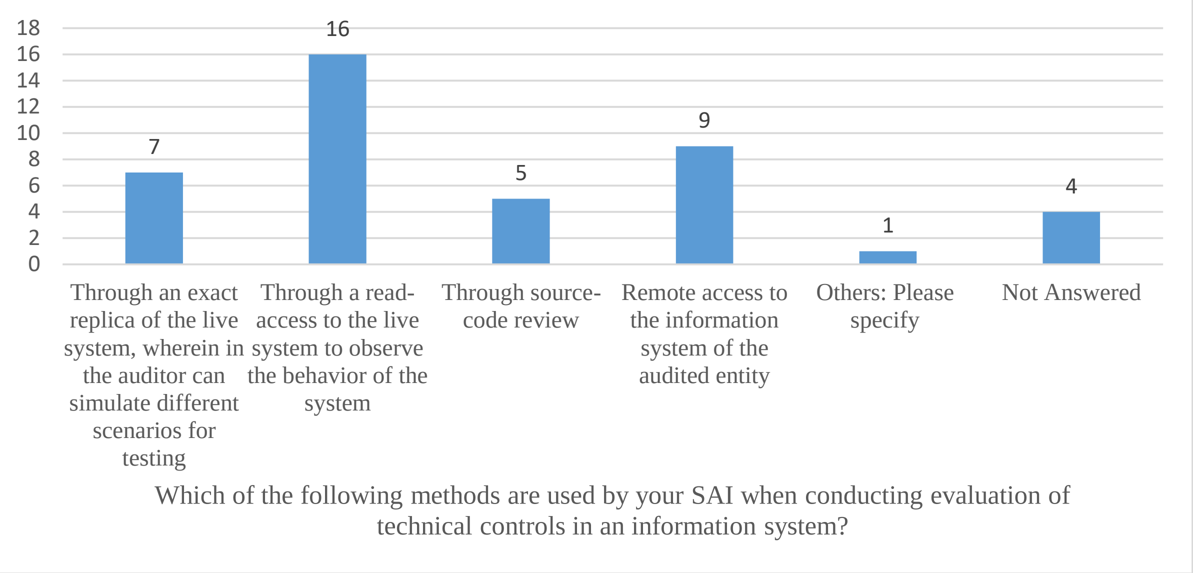


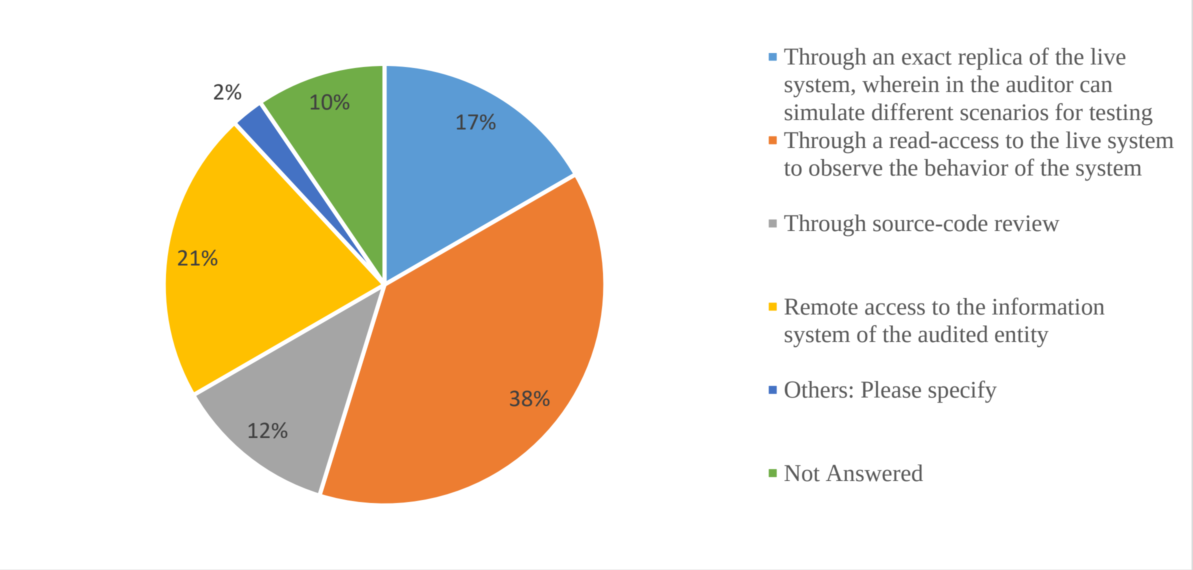


Additional Remarks:

5.3.9 Which of the following methods are used by your SAI when conducting evaluation of technical controls in an information system?

□Through an exact replica of the live system, wherein in the auditor can simulate different scenarios for testing
□Through a read-access to the live system to observe the behavior of the system
□Through source-code review
□Remote access to the information system of the audited entity
□Others: Please specify ____________________



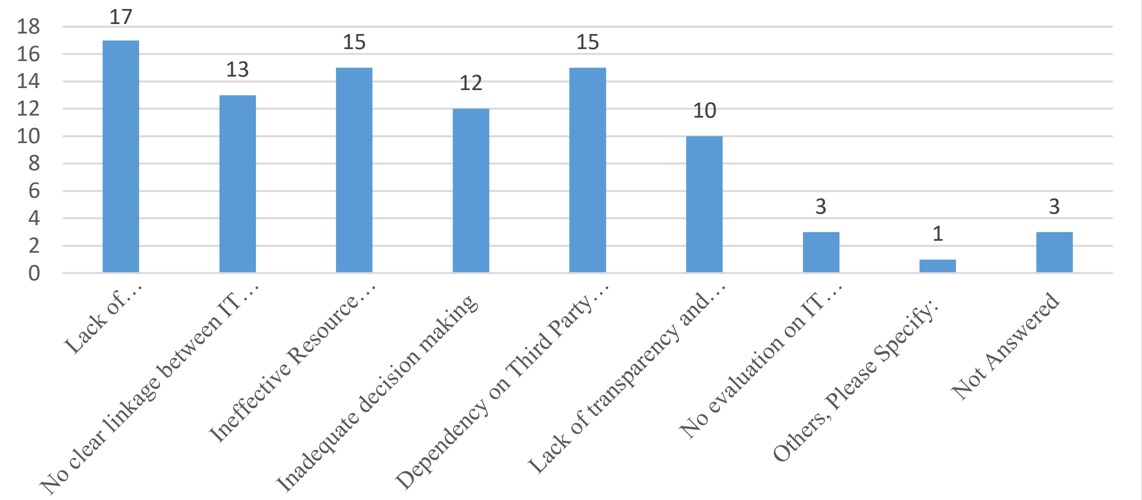


Additional Remarks:

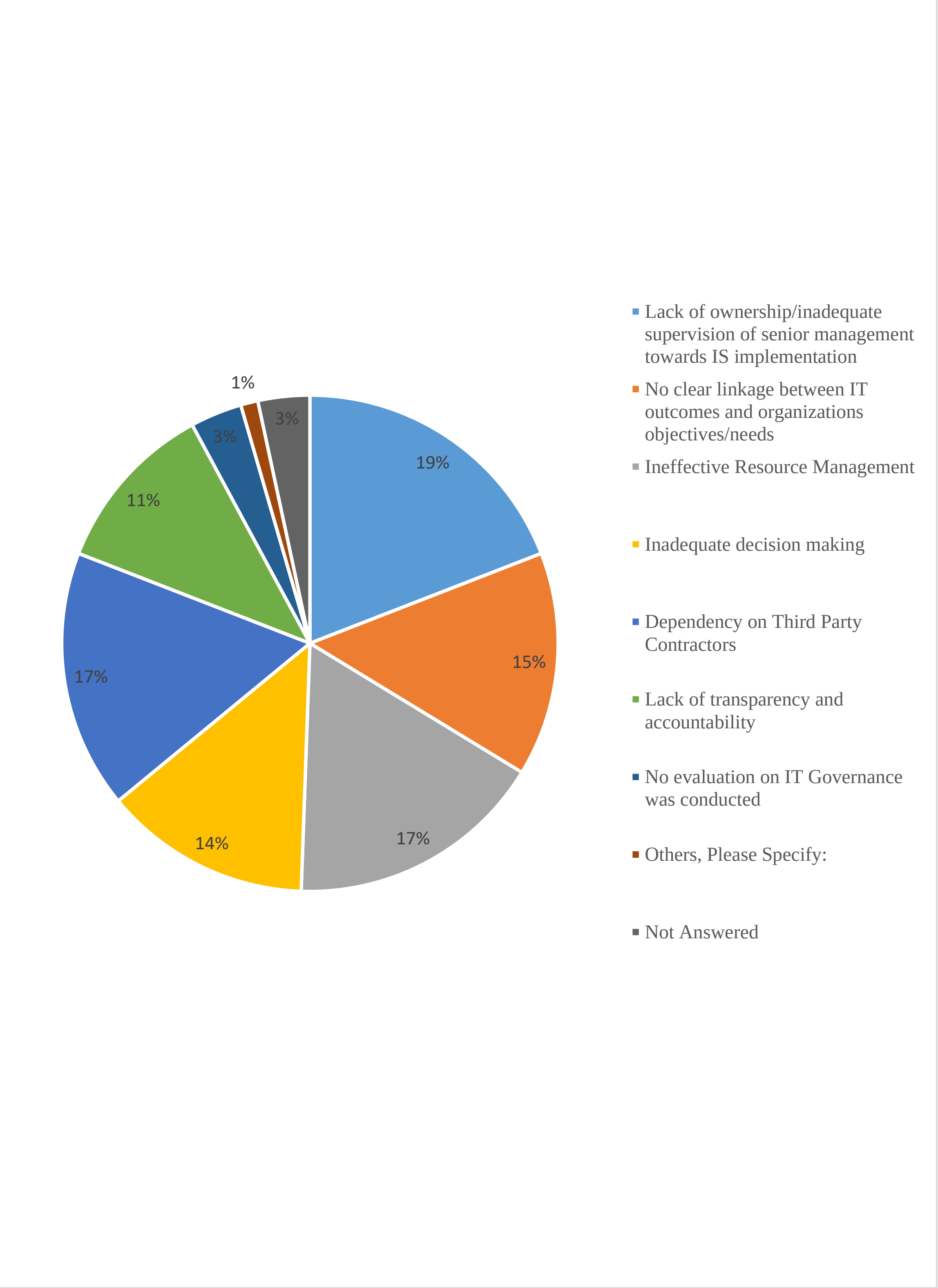
5.3.10 What are the common risks and consequences your SAI observed during the performance evaluation of IS specifically on IT Governance?

□ Lack of ownership/inadequate supervision of senior management towards IS implementation
□ No clear linkage between IT outcomes and organizations objectives/needs
□ Ineffective Resource Management
□ Inadequate decision making
□ Dependency on Third Party Contractors
□ Lack of transparency and accountability
□ No evaluation on IT Governance was conducted
□ Others, Please Specify:

____



What are the common risks and consequences your SAI observed during the performance evaluation of IS specifically on IT Governance?



Additional Remarks:

5.3.11 How does your SAI assess the effectiveness of management in developing/acquiring an IS?

□ Determine whether the organization has an understanding of its needs and requirements and considers them in development/acquisition

□ Observe if proper feasibility was done before developing/acquiring an IS

□ Observe the number of change/system modification requests made by management.

□ Observe if the auditee is managing the vendor adequately

□ Observe if a dedicated team was assigned to liaise and coordinate the IS implementation work with 3rd party

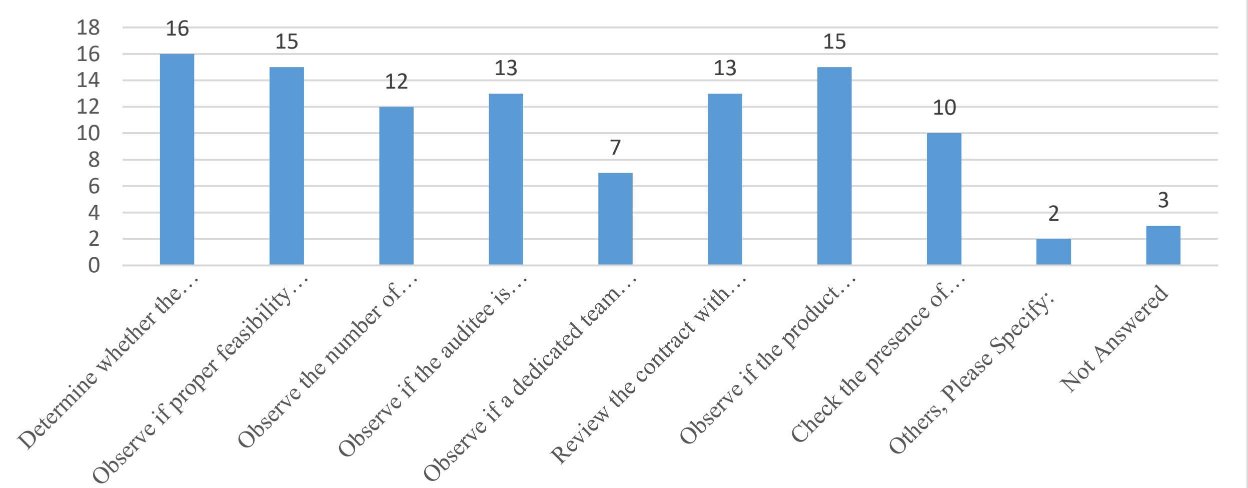
□ Review the contract with vendors

□ Observe if the product developed/delivered was as per the required specifications on an item by item check basis.

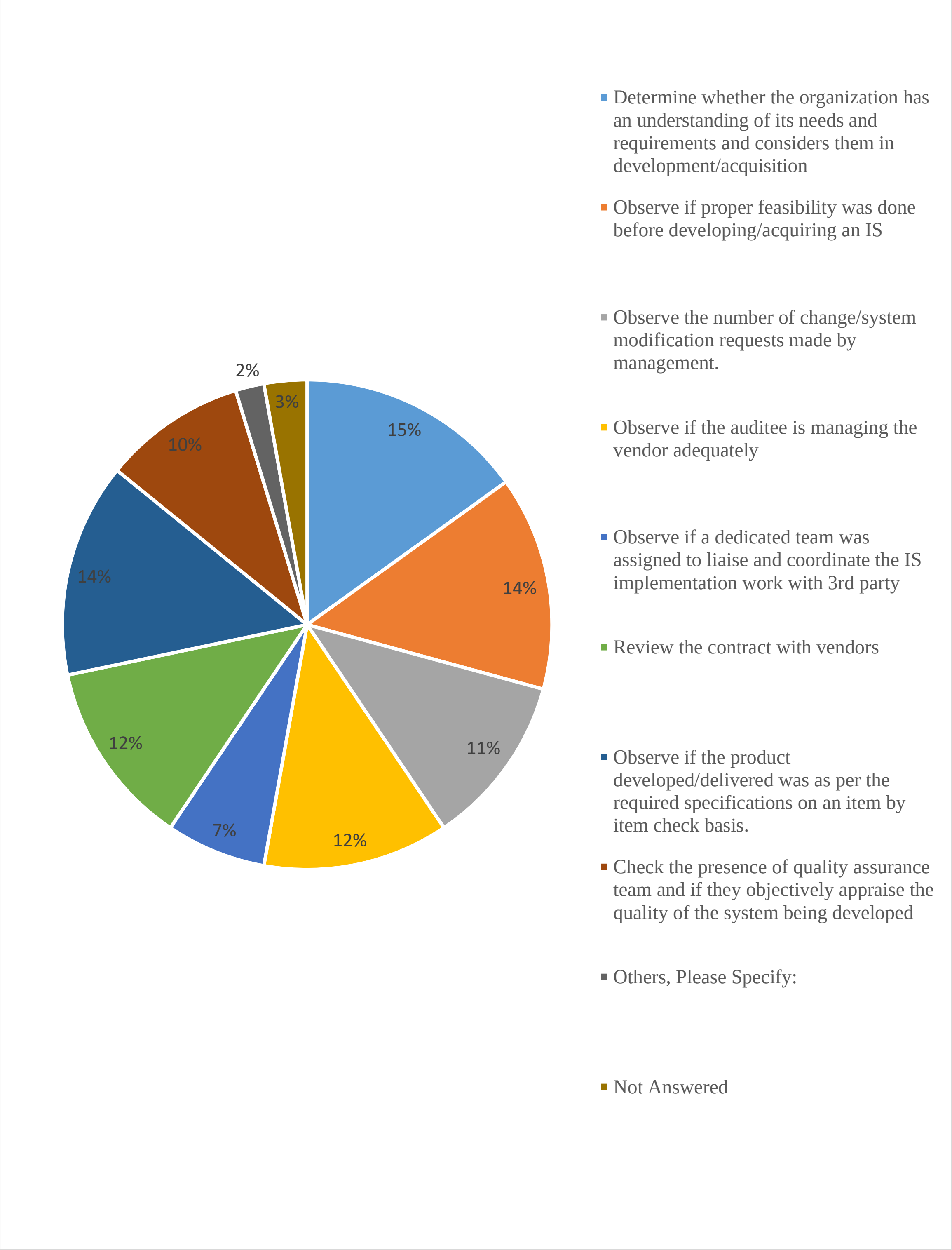
□ Check the presence of quality assurance team and if they objectively appraise the quality of the system being developed

□ Others, Please Specify:

____



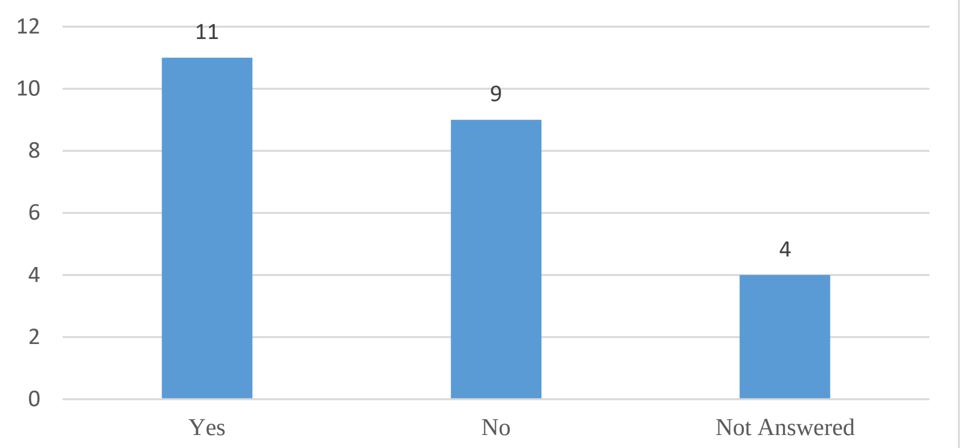
How does your SAI assess the effectiveness of management in developing/acquiring an IS?



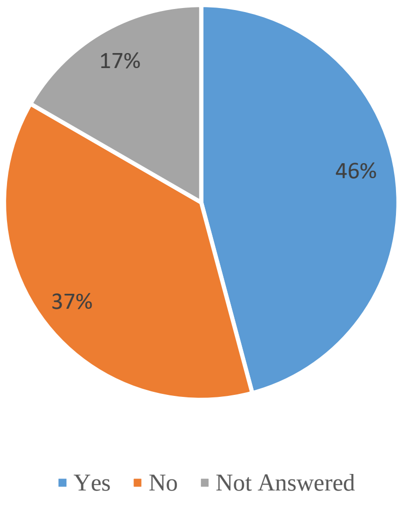
Additional Remarks:

5.3.12 Does the SAI review whether the network infrastructure is sufficient to support the implementation of the IT system, including the needs of the users (e.g. uninterrupted access over intranet, or cloud?

□ Yes
□ No



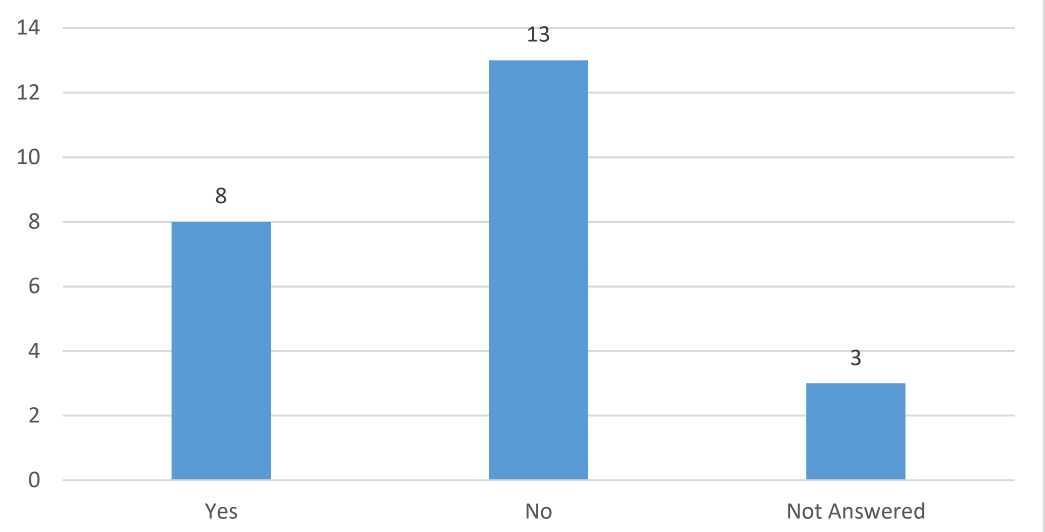
Does the SAI review whether the network infrastructure is sufficient to support the implementation of the IT system, including the needs of the users (e.g. uninterrupted access over intranet, or cloud?



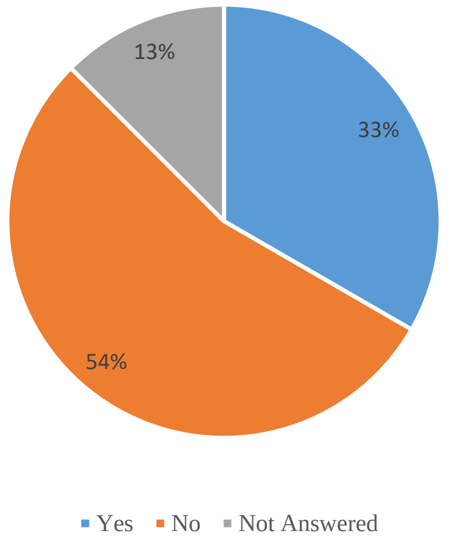
Additional Remarks:

5.3.13 Does the SAI review whether the IS initiative has reduced the HR and allied costs in terms of working hours required to do specific jobs?

□ Yes
□ No



Does the SAI review whether the IS initiative has reduced the HR and allied costs in terms of working hours required to do specific jobs?

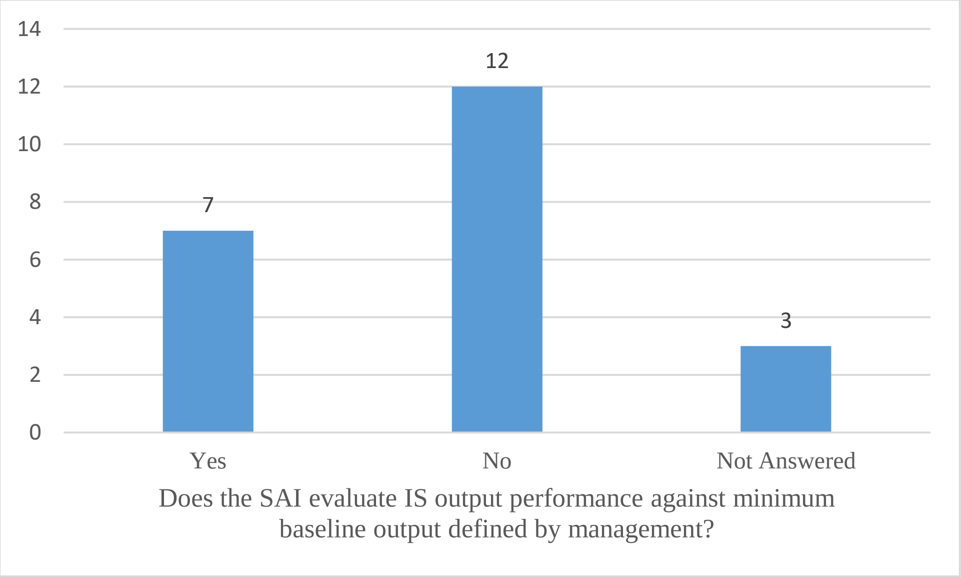


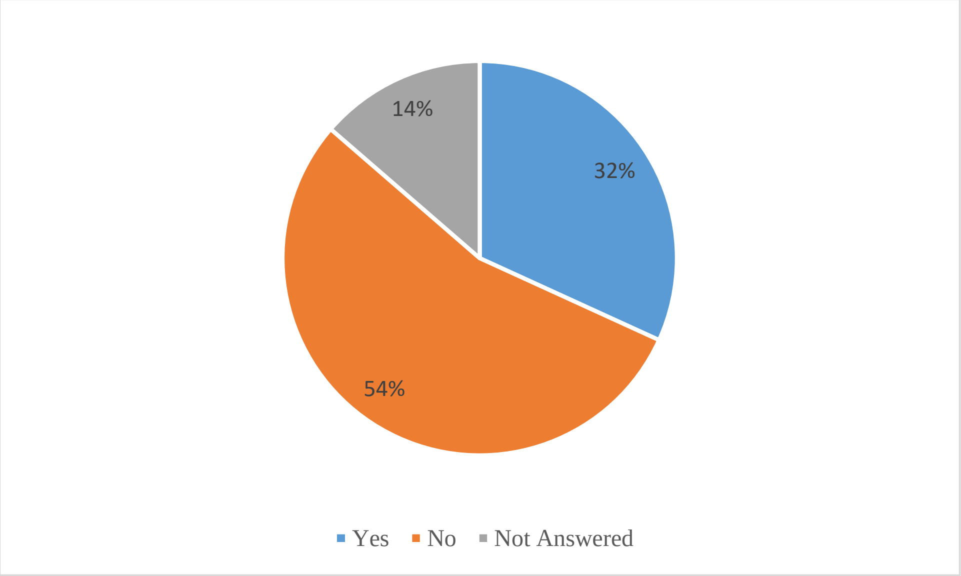
Additional Remarks:

5.3.14 Does the SAI evaluate IS output performance against minimum baseline output defined by management?

For example: An Driving License Issuance solution based on an ideal scenario can process 15 license forms in an hour at one workplace. (other factors remaining constant). Hence if audit finds workplaces with an average processing of 04 licenses per hour, further inquiry would result.

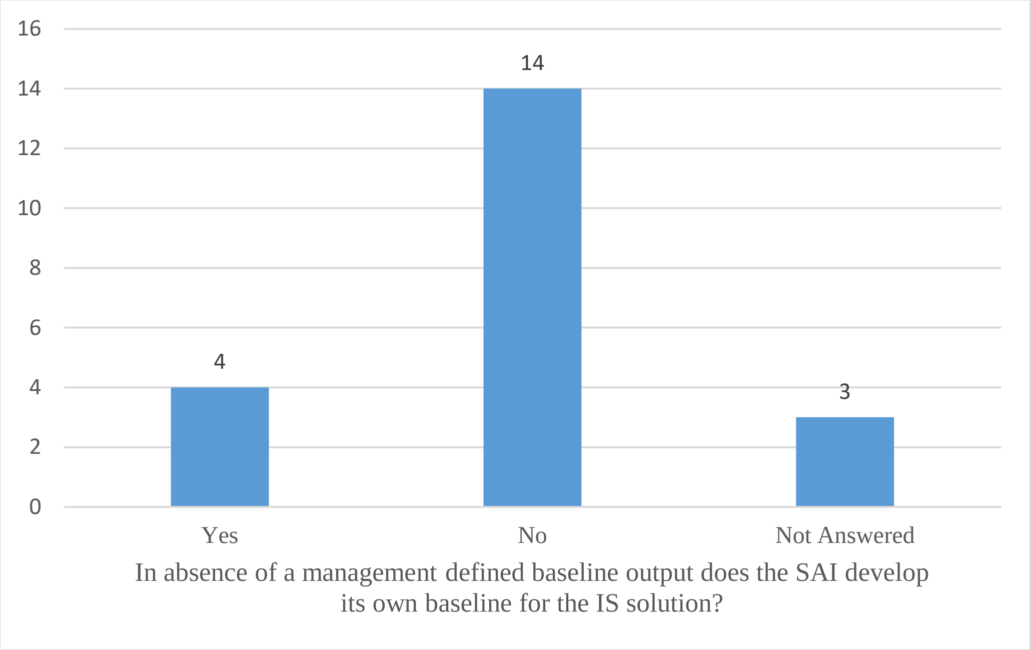
□ Yes
□ No



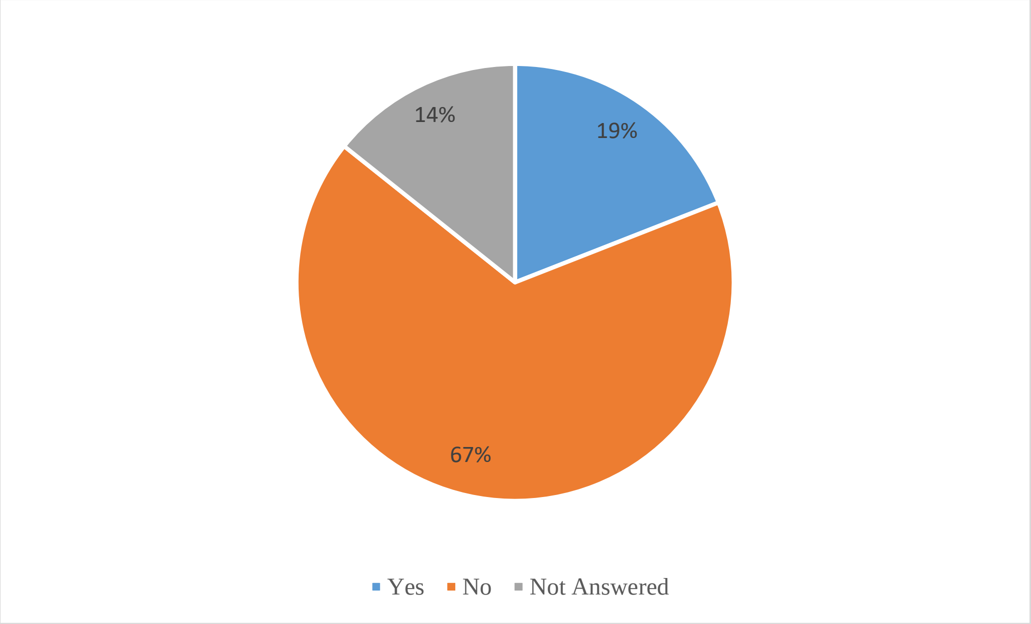


5.3.14 (A) In absence of a management defined baseline output does the SAI develop its own baseline for the IS solution?

□ Yes
□ No



In absence of a management defined baseline output does the SAI develop its own baseline for the IS solution?



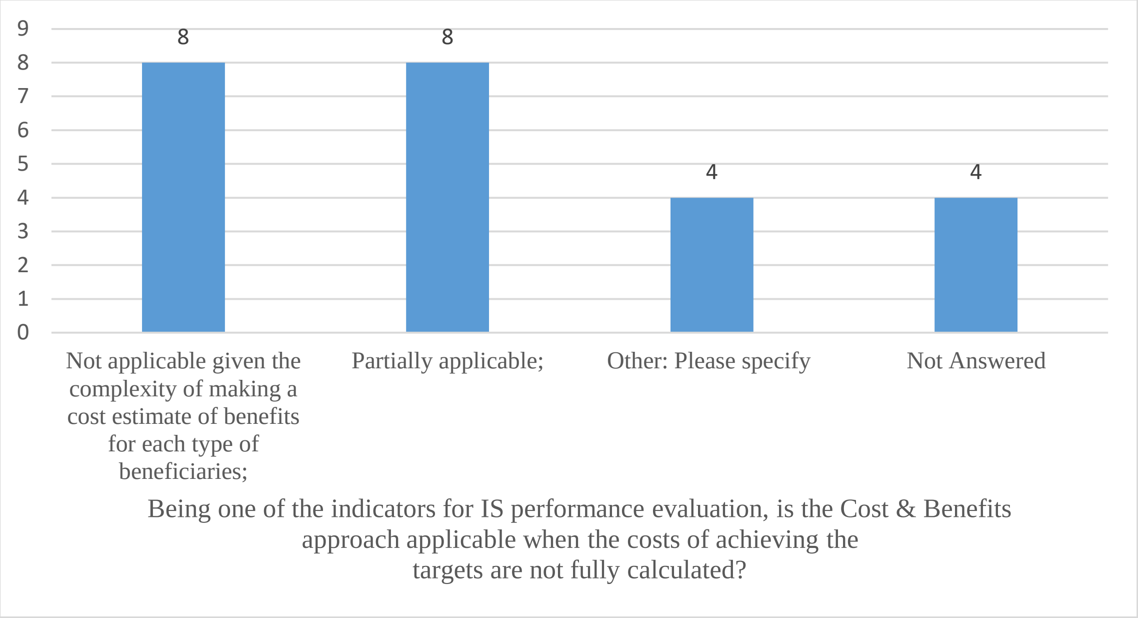
Additional Remarks:

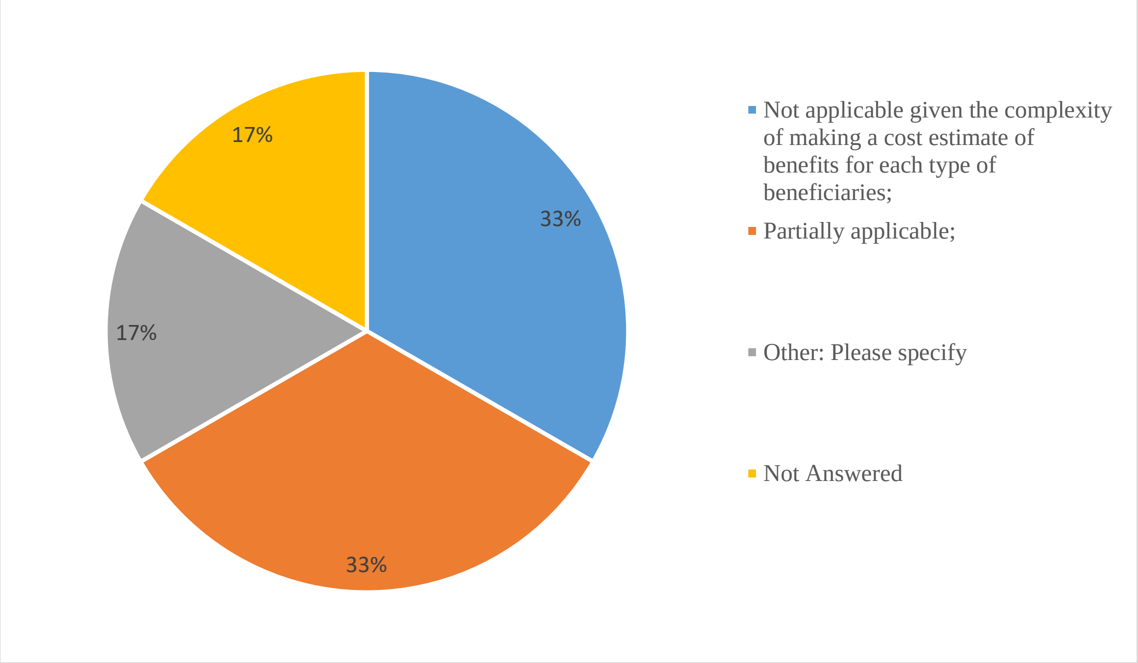
5.3.15 **Being one of the indicators for IS performance evaluation, is the Cost & Benefits approach applicable when the costs of achieving the targets are not fully calculated?**

□ Not applicable given the complexity of making a cost estimate of benefits for each type of beneficiaries;

□ Partially applicable;

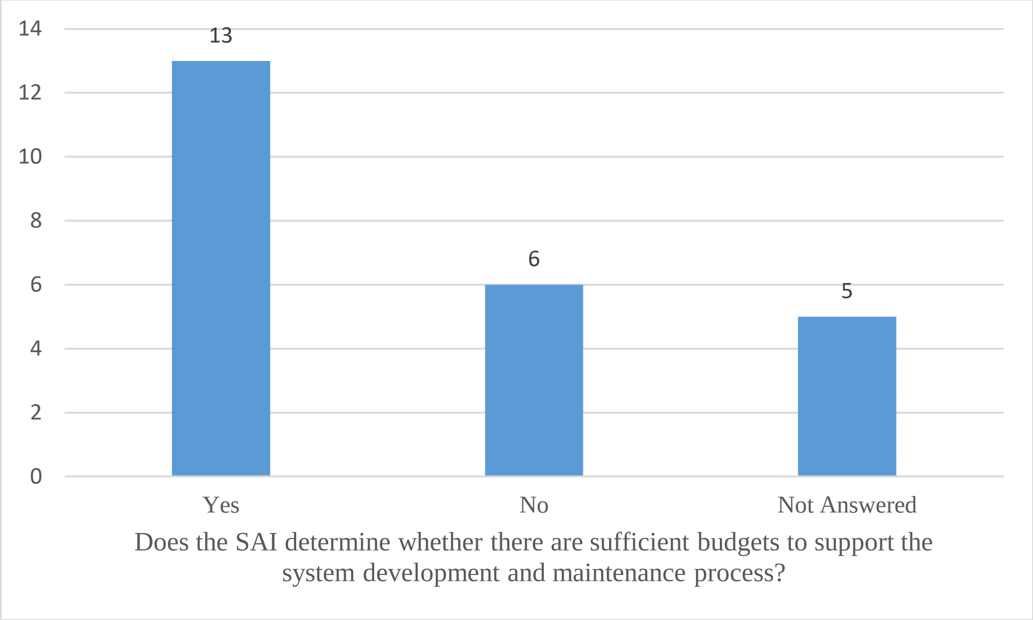
□ Other: Please specify _______________

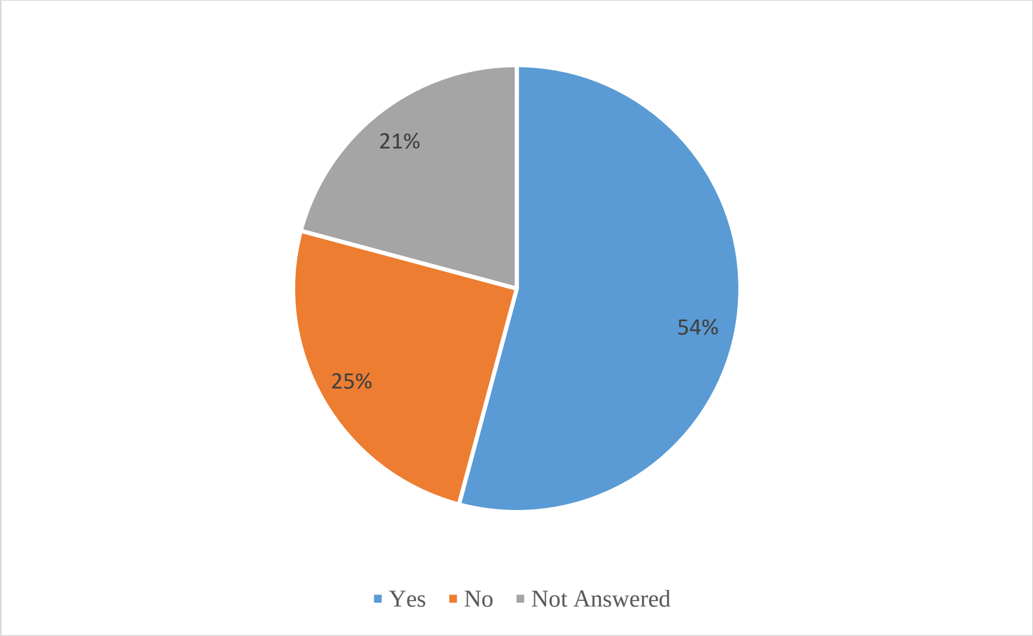




5.3.16 Does the SAI determine whether there are sufficient budgets to support the system development and maintenance process?

□ Yes
□ No

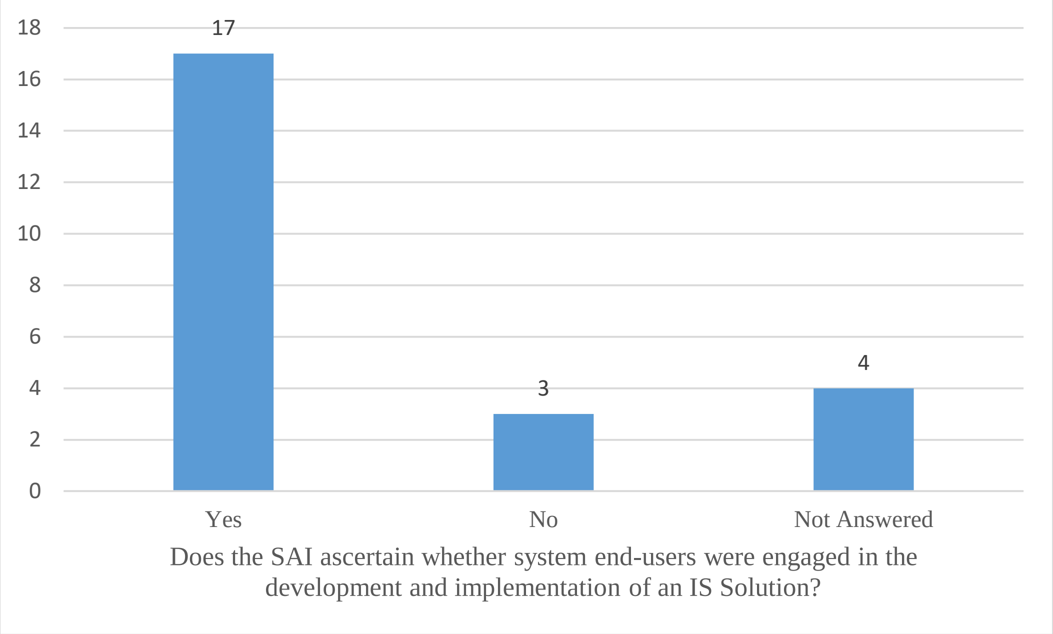


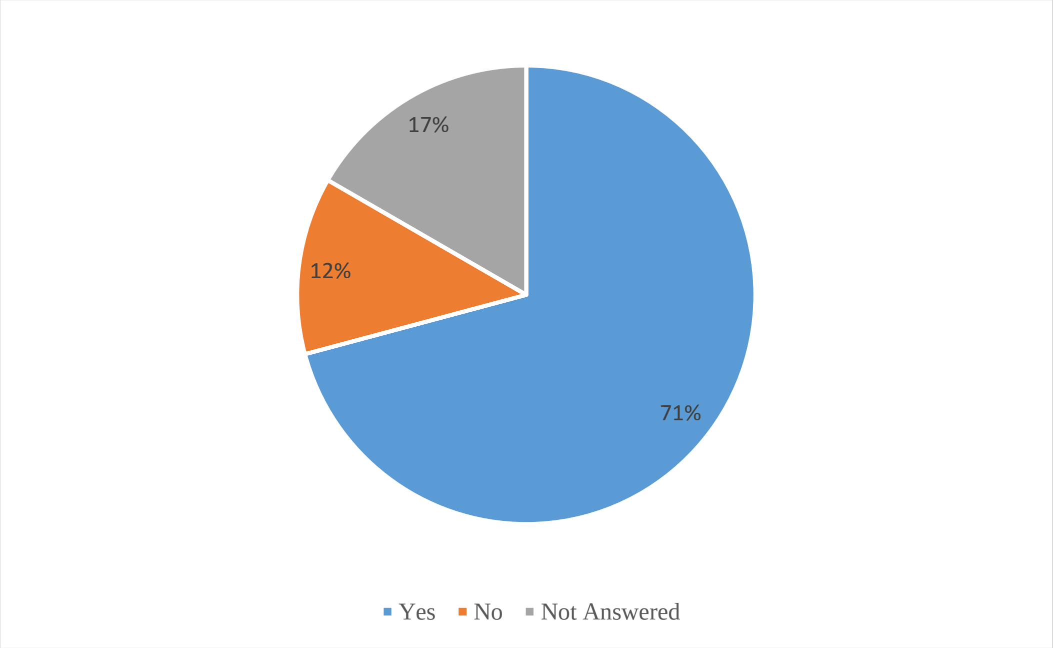


Additional Remarks:

5.3.17 Does the SAI ascertain whether system end-users were engaged in the development and implementation of an IS Solution?

□ Yes
□ No





Additional Remarks:

Section 5.4 IS Performance Evaluation Reporting

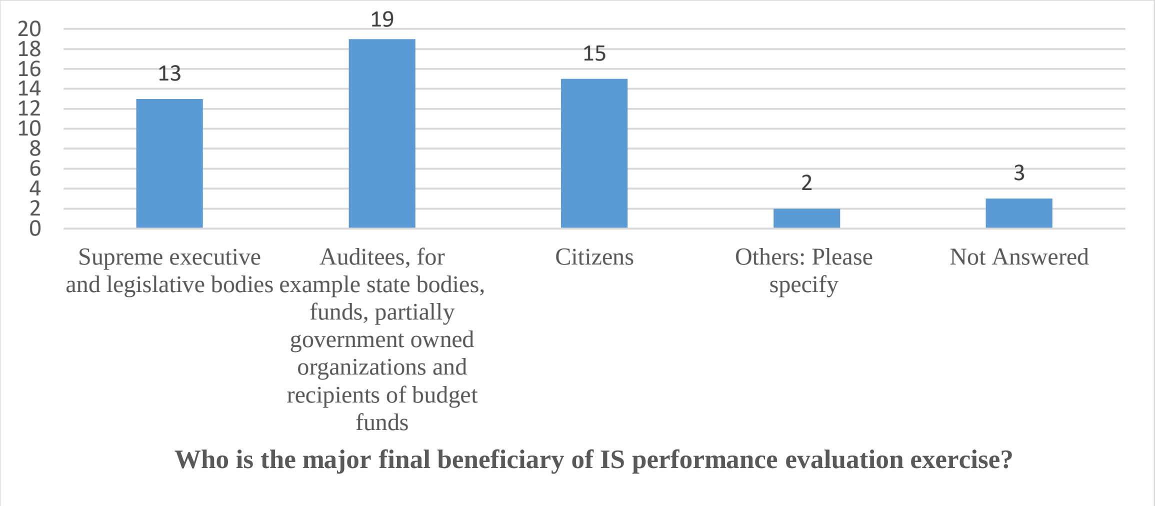
5.4.1 Who is the major final beneficiary of IS performance evaluation exercise?

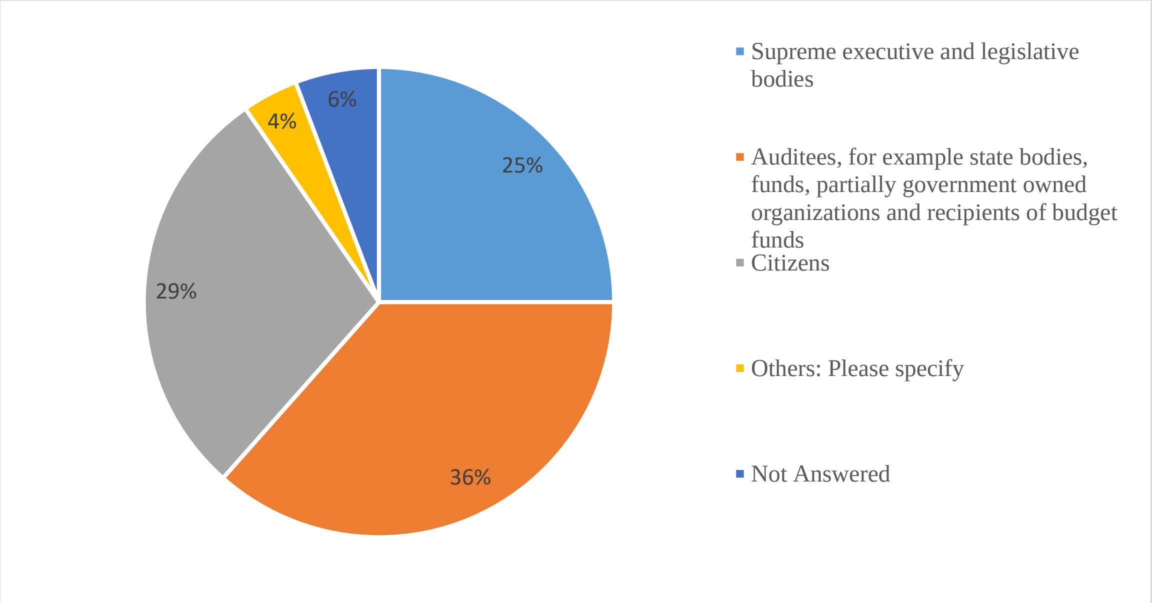
□ Supreme executive and legislative bodies

□ Auditees, for example state bodies, funds, partially government owned organizations and recipients of budget funds

□ Citizens

□ Others: Please specify ____

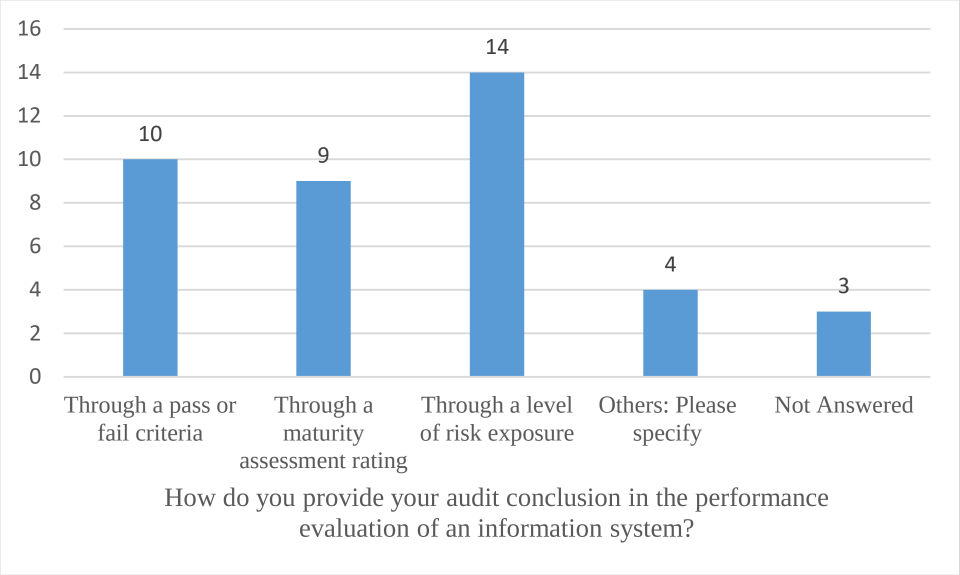


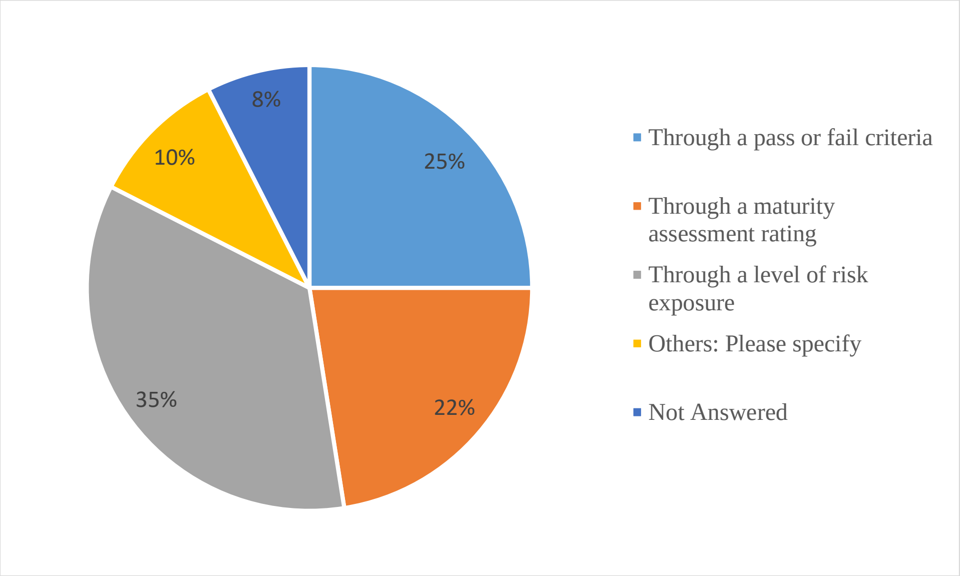


Additional Remarks:

5.4.2 How do you provide your audit conclusion in the performance evaluation of an information system?

□Through a pass or fail criteria
□Through a maturity assessment rating
□Through a level of risk exposure
□Others: Please specify ____

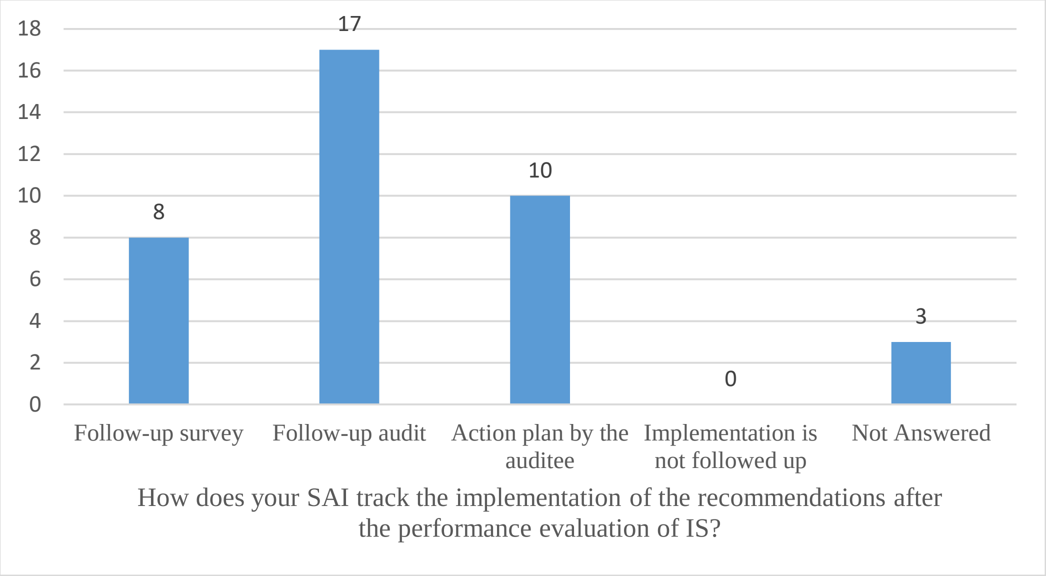


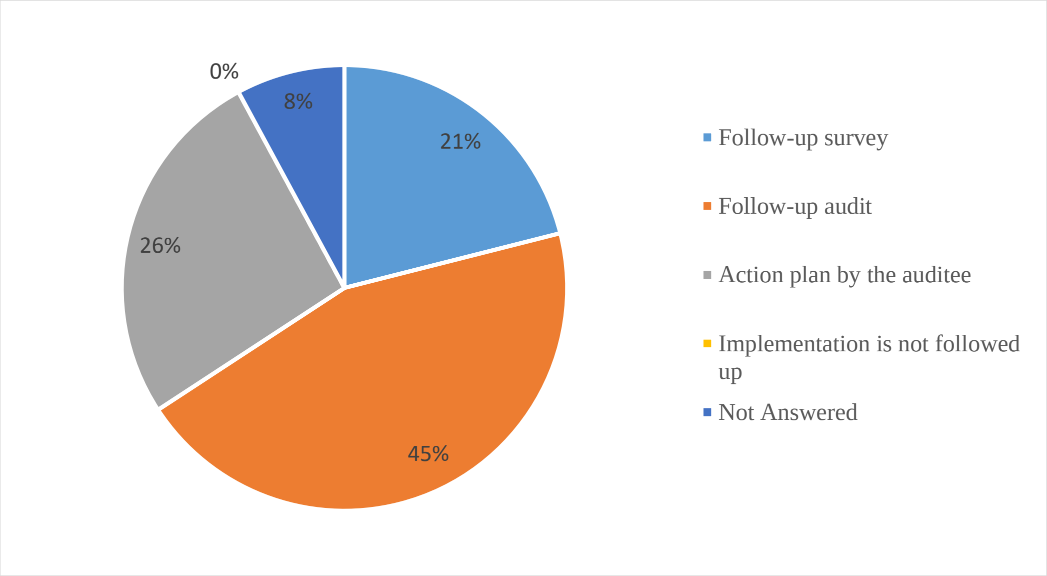


Additional Remarks:

5.4.3 How does your SAI track the implementation of the recommendations after the performance evaluation of IS?

□ Follow-up survey
□ Follow-up audit
□ Action plan by the auditee
□ Implementation is not followed up





Additional Remarks:

5.4.4 What are the important benefits of IS performance evaluation reports for the stakeholders?

Ranking:	Score
Average Benefit	1
Moderate Benefit	2
Major Benefit	3

Sr. No.	**Benefit**	**Ranking**
1.	Harmonizing regulations on public administration digitalization with strategic planning documents, state programs and projects;	**2**

2.	Creating a clear and consistent legal framework for regulating relations associated with the creation, development, operation and decommissioning of information systems that meets the needs and is in line with the future developments in this area;	**4**
3.	Developing the procedure and methodology for a regular comprehensive audit *of the outcomes* of creating and developing information systems;	**3**
4.	Improving IT processes, including the identified weaknesses, for example: the need to improve the evaluation criteria of completeness, quality, openness and availability of information system data;	**1**
5.	Conducting public monitoring of state spending on all information systems for the entire life cycle in each public body.	**5**

Sr. No.	**Benefit**	**3 Major Benefit**	**2 Moderate Benefit**	**1 Average Benefit**
1	Harmonizing regulations on public administration digitalization with strategic planning documents, state programs and projects;	9	6	2
2	Creating a clear and consistent legal framework for regulating relations associated with the creation, development, operation and decommissioning of information systems that meets the needs and is in line with the future developments in this area;	7	5	5
3	Developing the procedure and methodology for a regular comprehensive audit *of the outcomes* of creating and developing information systems;	8	7	3
4	Improving IT processes, including the identified weaknesses, for example: the need to improve the evaluation criteria of completeness, quality, openness and availability of information system data;	14	5	0
5	Conducting public monitoring of state spending on all information systems for the entire life cycle in each public body.	8	3	4

Weighted Scores

Sr. No.	**Benefit**	**3 Major Benefit**	**2 Moderate Benefit**	**1 Average Benefit**	**Total**
1	Harmonizing regulations on public administration digitalization with strategic planning documents, state programs and projects;	27	12	2	41
2	Creating a clear and consistent legal framework for regulating relations associated with the creation, development, operation and decommissioning of information systems that meets the needs and is in line with the future developments in this area;	21	10	5	36

3	Developing the procedure and methodology for a regular comprehensive audit *of the outcomes* of creating and developing information systems;	24	14	3	41
4	Improving IT processes, including the identified weaknesses, for example: the need to improve the evaluation criteria of completeness, quality, openness and availability of information system data;	42	10	0	52
5	Conducting public monitoring of state spending on all information systems for the entire life cycle in each public body.	24	6	4	34

Section 5.5 Issues & Challenges

5.5.1 What are the different types of challenges your SAI has experienced in conducting performance evaluation of IS? ***(A list of challenges and ranking is***

added for your review)

Ranking:	Score
Minor Challenge	1
Moderate Challenge	2
Major Challenge	3

□ No challenges

□ Others, Please Specify: ________________________

I **Sr. No.**	II **Nature of Challenge**	III **Yes**	IV **No**	V **Ranking (*“if III = yes”*)**
1	Absence of SAI’s mandate			
2	Lack of human resources			
3	Lack of required skills or expertise and trainings within the SAI			
4	Insufficient formulation of government policy/rules such as insufficient regulatory frameworks over IS implementation			
5	Lack of established auditing standards/guidelines for performance evaluation of information systems			
6	Lack of technical resources (eg. Insufficient equipment, infrastructure)			
7	Insufficient/Unreliable data from the auditee			
8	Restriction in the access of data			
9	Ensuring confidentiality and integrity of data received from auditee organization			
10	Difficulty in validating reported data			
11	Weak awareness of the auditee on IS controls			
12	Insufficient funds to obtain required hardware/software for the performance evaluation of information systems			

13	Most audited entities are not automated or using information systems			
14	Difficulties in obtaining information from third party/ alternative (independent) sources for purpose of cross verification			

 Sr. No.	II **Nature of Challenge**	III **Yes**	IV **No**
1	Absence of SAI's mandate	**2**	**18**
2	Lack of human resources	**9**	**11**
3	Lack of required skills or expertise and trainings within the SAI	**16**	**4**
4	Insufficient formulation of government policy/rules such as insufficient regulatory frameworks over IS implementation	**10**	**10**
5	Lack of established auditing standards/guidelines for performance evaluation of information systems	**6**	**14**
6	Lack of technical resources (eg. Insufficient equipment, infrastructure)	**8**	**12**
7	Insufficient/Unreliable data from the auditee	**10**	**10**
8	Restriction in the access of data	**7**	**13**
9	Ensuring confidentiality and integrity of data received from auditee organization	**6**	**14**
10	Difficulty in validating reported data	**11**	**9**
11	Weak awareness of the auditee on IS controls	**13**	**7**
12	Insufficient funds to obtain required hardware/software for the performance evaluation of information systems	**7**	**12**
13	Most audited entities are not automated or using information systems	**3**	**17**
14	Difficulties in obtaining information from third party/ alternative (independent) sources for purpose of cross verification	**13**	**7**

I **Sr. No.**	II **Nature of Challenge**	3 Major Challenge	2 Moderate Challenge	1 Minor Challenge
1	Absence of SAI's mandate	**1**	**1**	**0**
2	Lack of human resources	**5**	**5**	**1**
3	Lack of required skills or expertise and trainings within the SAI	**5**	**11**	**1**
4	Insufficient formulation of government policy/rules such as insufficient regulatory frameworks over IS implementation	**4**	**6**	**1**
5	Lack of established auditing standards/guidelines for performance evaluation of information systems	**2**	**1**	**3**

I	II	3	2	1
Sr. No.	**Nature of Challenge**	Major Challenge	Moderate Challenge	Minor Challenge
6	Lack of technical resources (eg. Insufficient equipment, infrastructure)	**2**	**3**	**5**
7	Insufficient/Unreliable data from the auditee	**4**	**6**	**2**
8	Restriction in the access of data	**5**	**1**	**1**
9	Ensuring confidentiality and integrity of data received from auditee organization	**3**	**2**	**1**
10	Difficulty in validating reported data	**4**	**2**	**6**
11	Weak awareness of the auditee on IS controls	**1**	**10**	**4**
12	Insufficient funds to obtain required hardware/software for the performance evaluation of information systems	**0**	**5**	**3**
13	Most audited entities are not automated or using information systems	**1**	**1**	**1**
14	Difficulties in obtaining information from third party/ alternative (independent) sources for purpose of cross verification	**5**	**6**	**3**

Weighted Scores

I	II	3	2	1	
Sr. No.	**Nature of Challenge**	Major Challenge	Moderate Challenge	Minor Challenge	Total
1	Absence of SAI's mandate	3	2	0	5
2	Lack of human resources	15	10	1	26
3	Lack of required skills or expertise and trainings within the SAI	15	22	1	38
4	Insufficient formulation of government policy/rules such as insufficient regulatory frameworks over IS implementation	12	12	1	25
5	Lack of established auditing standards/guidelines for performance evaluation of information systems	6	2	3	11
6	Lack of technical resources (eg. Insufficient equipment, infrastructure)	6	6	5	17
7	Insufficient/Unreliable data from the auditee	12	12	2	26
8	Restriction in the access of data	15	2	1	18
9	Ensuring confidentiality and integrity of data received from auditee organization	9	4	1	14
10	Difficulty in validating reported data	12	4	6	22
11	Weak awareness of the auditee on IS controls	3	20	4	27

I Sr. No.	II Nature of Challenge	3 Major Challenge	2 Moderate Challenge	1 Minor Challenge	Total
12	Insufficient funds to obtain required hardware/software for the performance evaluation of information systems	0	10	3	13
13	Most audited entities are not automated or using information systems	3	2	1	6
14	Difficulties in obtaining information from third party/ alternative (independent) sources for purpose of cross verification	15	12	3	30

Additional Remarks:

5.5.2 From the below list, kindly put check mark on the column "Necessary" if you think the development is needed in your SAI, on "Planned" if there are plans to implement this development and on "Implemented" if the attribute is present in your SAI, for the conduct of performance evaluation of IS.

Type of development	**Necessary (Identified)**	**Planned (to be implemented)**	**Implemente d**
Creation of an audit department focused on the performance evaluation of information system	4	1	15
Integration of information systems audit with other audits	7	1	15
Training in recent IT developments and standards	10	5	7
Training in the process of performance evaluation of information system	11	4	8
Development of performance measures	9	2	8
Exchange of knowledge with other SAIs	11	5	7
Peer review of audit processes by other SAIs	11	2	4
Process evaluation by external experts	9	2	6
Others: Please Specify________________			

Additional Remarks:

Section 5.6 Miscellaneous

5.6.1 What are the Key Lessons Learned by your SAI during the performance evaluation of Information Systems?

5.6.2 What is the most important expected outcome from the WGITA Guidance in question?

Ranking:	Score
Average	1
Significant	2
Most significant	3

Sr. No.	Expected outcome	Ranking
I	Audit program with checklists	**2**
II	Indicative good practices for an operating IT system	**3**
III	Common CAATs queries for testing application controls and data quality	**4**
IV	Best practices for IS performance evaluations	**1**
V	Inclusion of findings from PEs of IT systems in other SAIs	**5**

Sr. No.	Benefit	3. Most significant	2. Significant	1. Average
I	Audit program with checklists	10	8	3
II	Indicative good practices for an operating IT system	6	10	5
III	Common CAATs queries for testing application controls and data quality	7	8	5
IV	Best practices for IS performance evaluations	12	8	2
V	Inclusion of findings from PEs of IT systems in other SAIs	4	6	10

Weight

Sr. No.	Benefit	3. Most significant	2. Significant	1. Average	Total
I	Audit program with checklists	30	16	3	49
II	Indicative good practices for an operating IT system	18	20	5	43
III	Common CAATs queries for testing application controls and data quality	21	16	5	42
IV	Best practices for IS performance evaluations	36	16	2	54
V	Inclusion of findings from PEs of IT systems in other SAIs	12	12	10	34

Section 5.7 Insights

5.7.1 SAI Policies and Procedures pertaining to IS Performance Evaluation

1. Almost all respondents do Information Systems Performance Evaluations (ISPE) but only 25% of the respondents actually perform these evaluations on a large-scale, regular basis.
2. Most ISPE are conducted as part of a more mainstream audit engagement (i.e., Financial, Compliance, Performance) rather than as a separate audit exercise or an Information Systems Audit.

3. When it comes to methodology, most ISPE exercises do not have their own specific methodology or guideline and would follow the general performance audit methodology. Most SAI respondents also use international/ regional standards and best practices (e.g., ISO, COBIT, and ITIL) for ISPE.

5.7.2 Planning for the IS Performance Evaluation Exercise

4. Risk-Based audit planning is cascaded in ISPE, there being more engagements originating from an integrated risk process of selection rather than from requests from other entities.
5. The objectives and planning considerations of ISPE are almost the same as that of Performance audits, but with Information Systems (IS) as the audit subject matter.
6. Most ISPE exercises are conducted after the implementation of the IT solution being implemented (post-audit) but nearly half also perform the exercise during the IT solution’s implementation

5.7.3 Execution of IS Performance Evaluation Exercise

7. There are many areas that are frequently assessed by the respondent SAIs in the conduct of ISPE. Among them, the areas of IT Governance and Information Security Policies are deemed most relevant and most frequently assessed, while the areas of Electronic Commerce and Business Continuity are deemed least relevant and least frequently assessed.
8. Similarly, the ISPE exercises do not focus much on the technical parameters when gauging the performance of an IS solution but rather on its governance, i.e., how it was acquired, implemented, and how it adds value to the organization and its users. Interestingly, despite this focus on implementation, more of the SAIs answered that they do not assess the performance of the IS initiative in terms of how it improved productivity (e.g., increased output against a baseline)
9. When doing ISPE, less than half of the respondents believe that the Cost and Benefits approach is applicable when assessing the costs of achieving targets. Most of the respondents do assess whether budgets are sufficient to support any system development and maintenance process.

5.7.4 IS Performance Evaluation Reporting

10. Most respondents believe that their auditees are the foremost beneficiaries of ISPE.
11. More than half of the respondents provide their ISPE audit conclusions through the presentation of a level of risk exposure. Less than half of the respondents use objective measurements like maturity ratings or Pass/Fail criteria when presenting their conclusions.
12. Most respondents track the implementation of their audit recommendations through follow-up audits rather than through follow-up surveys or action plans. This is similar to how it is done in Performance Audits
13. The foremost benefit of ISPE, as identified by the respondents, is the improvement of IT processes, including the identification of weaknesses

5.7.5 Issues and Challenges

14. The foremost challenge of ISPE, as identified by the respondents, is the lack of required skills or expertise and trainings within SAIs. Next to this are the challenges of a.) difficulty in obtaining information from third party/ alternative (independent) sources for purposes of cross verification; and b.) weak awareness of the auditee on IS controls.
15. As to development, most SAI respondents answered that they already have an audit department performing ISPE and/or have integrated IS audits with other audit streams. Many SAIs also emphasized the necessity of capability building (i.e., trainings, development, knowledge exchange, and peer reviews)

5.7.6 Miscellaneous

16. The most sought outcome by the respondents from the WGITA Guidance are listings of “best practices for IS performance evaluations”. This is followed by “audit programs with checklists”