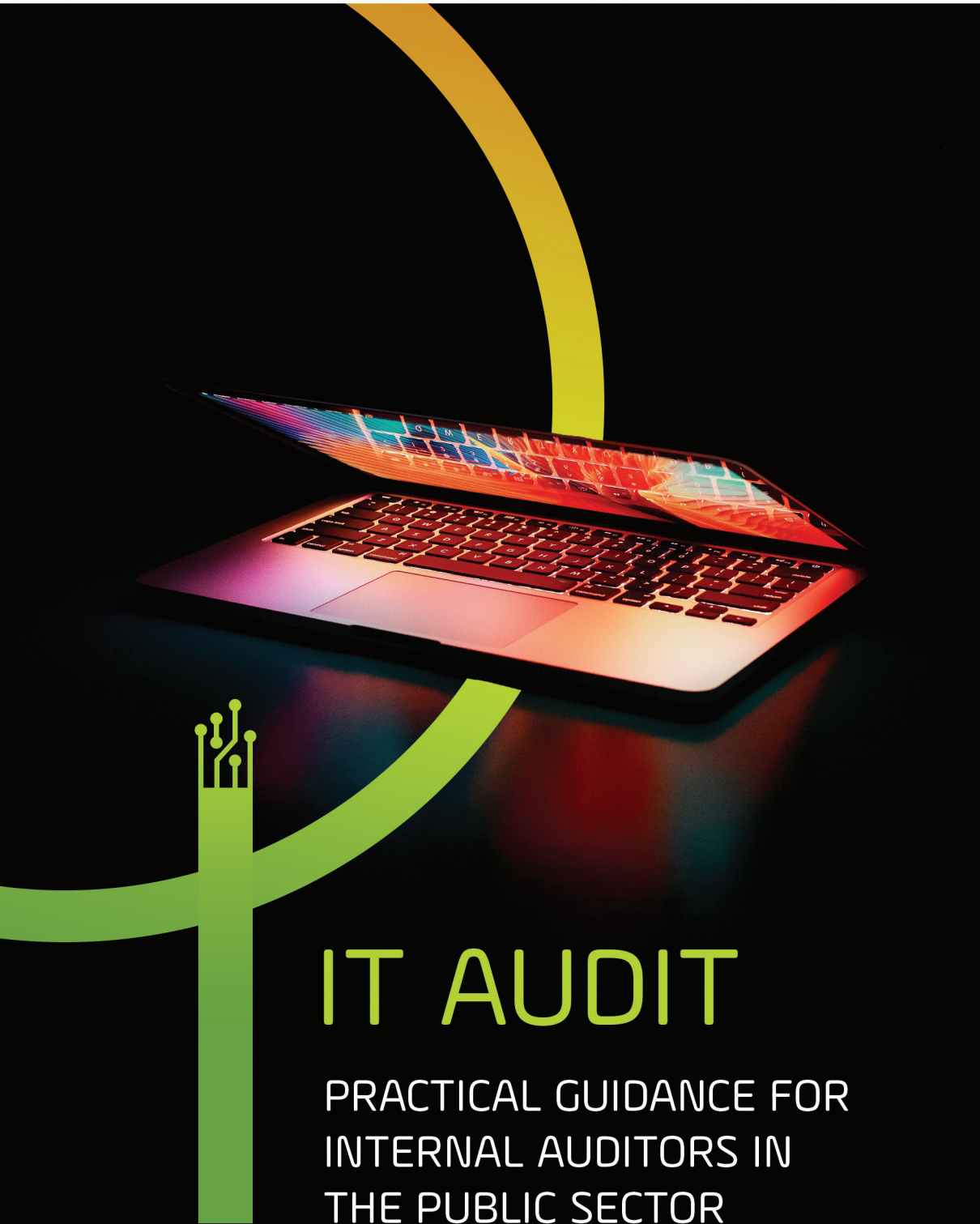
PEMPAL

IACOP Internal Audit Community of Practice



IT AUDIT

PRACTICAL GUIDANCE FOR INTERNAL AUDITORS IN THE PUBLIC SECTOR

Internal Audit Community of Practice (IACOP)
T: +7 495 745 70 00 ext. 2002
E: IACOP@pempal.org
W: www.pempal.org

CONTENTS

ACKNOWLEDGEMENTS

The Internal Audit Community of Practice (IACOP) would like to thank members and experts for their contributions to the preparation of the paper, especially Komitas Stepanyan, IT/cybersecurity risk expert, World Bank consultant, as a key writer of this paper, and Arman Vatyan, PEMPAL Program Leader, World Bank; Richard Maggs, Word Bank consultant; Ljerka Crnković, IACOP Executive Committee Chair, Croatia; Tatjana Trajkovska, IACOP Executive Committee member, CHU Challenges Working Group Leader, North Macedonia and Lusine Grigoryan, IACOP Resource Team, World Bank for their inputs.

GLOSSARY

CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
GTAG	Global Technology Audit Guide
IIA	The Institute of Internal Auditors
IPPF	International Professional Practices Framework
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITAF	Information Technology Audit Framework

WHAT ARE PEMPAL & IACOP?

Public Expenditure Management Peer Assisted Learning (PEMPAL) is a network to facilitate exchange of professional experience and knowledge transfer among public financial management practitioners in countries across the Europe and Central Asia region. The network, launched in 2006, aims to contribute to strengthening public financial management practices in the member countries through developing and disseminating information on good practices and their application.

The network is organized around three thematic communities of practice:

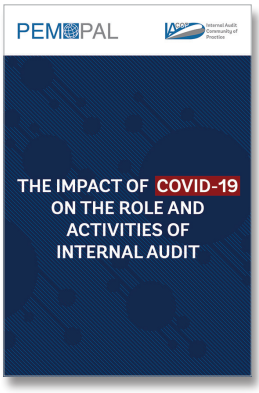
- Budget Community of Practice,
- Treasury Community of Practice, and
- Internal Audit Community of Practice.

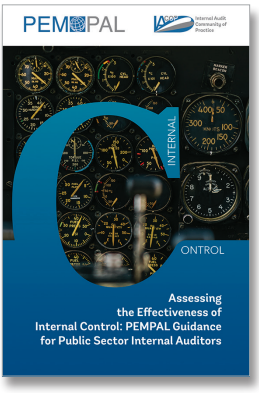
The main overall objective of the IACOP is to support its member countries in establishing modern and effective internal audit systems that meet international standards and good practices, key for good governance and accountability in the public sector.

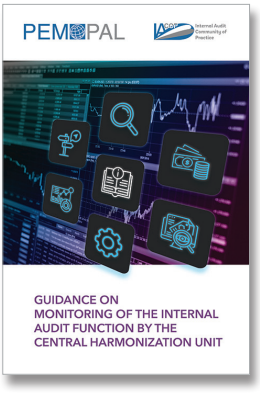
The **key donors** and development partners to the program are the Swiss State Secretariat for Economic Affairs, the Ministry of Finance of the Russian Federation, the European Commission, and the World Bank. The Dutch National Academy for Finance and Economy provides non-financial support.

This document is one in a series of IACOP knowledge products. Others, all available from **www.pempal.org**, include:

- Good Practice Internal Audit Manual Template;
- Good Practice Continuing Professional Development Manual Template;
- Internal Audit Body of Knowledge;
- Risk Assessment in Audit Planning;
- Cooperation Among Public Sector Audit and Financial Inspection Entities;
- Quality Assessment and Improvement Guide;
- PEMPAL Guidance on Internal Audit: Demonstrating and Measuring Added Value;
- The Impact of COVID-19 on the Role and Activities of Internal Audit;
- PEMPAL IACOP Glossary of Terms: Internal Control;
- Key Performance Indicators for Internal Audit Function;
- Assessing the Effectiveness of Internal Control: PEMPAL Guidance for Public Sector Internal Auditors; and
- Guidance on Monitoring of the Internal Audit Function by the Central Harmonization Unit.







PREFACE

This paper is based on materials and discussions at a Smart Interactive Talk with IACOP country auditor members, including IT auditors, which featured a presentation by an information technology audit expert entitled "Virtual Training on IT Audit". The aim was to outline the concept and approach of IT audit and discuss related internal audit areas of focus and concerns. Participants learned about IT annual risk assessments, the IT audit universe, IT audit engagement planning, execution, and reporting, as well as the process to follow-up recommendations. There was also discussion of IT governance challenges in the public sector including strategic IT risk management and how to audit IT Governance in the public sector; critical business application system controls and the supporting IT general controls; Business Continuity Management audit; as well as how to be a strategic adviser to senior management in this digital era.

More information, including the agenda and presentation materials, are available on the PEMPAL website.

EXECUTIVE SUMMARY

Internal audit is an essential component of corporate governance and, in this digital era, Information Technology (IT) audit has become a vital part of internal audit. The development of information and communication technologies and their worldwide use raise new political, economic, cultural, and technological issues and challenges for public sector organization management. Cybercrime is one of the fastest-growing areas of crime.[1] In response, internal audit of information and related technologies has become one of the most important and complex audit topics being performed by public sector internal audit, but one that can be complicated by a lack of necessary skills and competencies in many countries.

This PEMPAL knowledge product aims to provide guidance on a range of questions, challenges, and practical examples of IT audit in the public sector.

Part 1 provides general information about IT audit in the public sector: the different kinds of IT audits, the main objectives of IT audit, the role of IT auditors, and the purpose of IT audit in the public sector (and more widely).

Part 2 considers audit standards, frameworks, and best practices that public sector internal auditors may use during annual planning and risk assessment or for engagement planning, implementation, and testing phases. It includes information on two globally respected frameworks available for IT audit: Global Technology Audit Guides (GTAG®) from the Institute of Internal Auditors (IIA), and IT Audit Framework from the Information Systems Audit and Control Association (ISACA).[2] This section also highlights the three lines model and the challenges of using this model in the public sector, as the "second line" is often missing and internal audit must often audit management functions and activities while working under its direct supervision.

[1] EUROSAI ITWG model adoption for new IT audit framework: e-government cases

[2] ISACA's web site includes many audit programs available for members only.

Part 3 discusses the IT audit universe and IT annual planning and suggests two useful sources for IT auditors: *GTAG 11 - Developing the IT Audit Plan* and ISACA's "Developing the IT Audit Plan Using Control Objectives for Information and Related Technology (COBIT) 2019". This section also considers IT risk assessment and the IT audit universe using the earlier COBIT 4.1 version. Although ISACA has published the new COBIT 19, as IT governance is not very well developed in the public sector, COBIT 4.1 (still one of the best frameworks for IT Governance) can be an appropriate framework to support public sector IT auditors to assess IT governance at a high level.

This part also looks at different approaches to IT audit: vertical audit (looking at applications controls); deep vertical approach (looking at application controls and IT general controls, as the effectiveness of application controls depends on the effectiveness of IT general controls); and horizontal approach (looking at all relevant IT controls such as databases supporting different business processes and applications, for example information security audit, database management system audit, and network audit). Pre-implementation audit is mentioned, as many important projects may continue several years, and IT audit can add value by supporting business-users during the development phase.

Part 4 addresses the steps and methods of IT audit planning and execution. 17 key points are highlighted for effective IT audit planning and execution and methods for testing IT general controls. This part includes "test of design vs. test of effectiveness" and offers examples of different types of testing methods, like observation; inquiry; inspection; corroborative inquiry; system query; re-performance.

Part 5 includes practical examples of IT audit in business continuity management, of IT governance, and of the network.

Business continuity management audit has become even more important given the move to remote working due to the COVID-19 pandemic. This heightens existing cyber risks and introduces new ones to many institutions in the private and public sector. Internal audit must ask whether the internal control environment is sufficient to protect the institution, if there are business continuity plans in place that have been updated based on COVID-19 risks and tested as needed, and whether the entire business continuity management process has ever been audited (including emergency response, crisis management, and business continuity). Several good resources regarding business continuity are mentioned: International Organization for Standardization (ISO) 22301 – *Business Continuity Management Systems*, ISACA's Business Continuity Management Audit/Assurance Program, and GTAG 10 - *Business Continuity Management* from the IIA.

IT governance audit, as set out in the IIA Implementation Standard 2110.A2, requires internal audit to assess whether the IT governance of the organization supports its strategies and objectives. IT governance is seen as one of the most important audit engagements public sector internal audit should include in the audit universe. GTAG 17 - *Auditing IT Governance* provides detailed information about the main components of IT governance and how to get assurance for each component.

Network audit should provide senior management with proper assurance of network availability, which is vital given that the network is the most important component of any institution in today's digital world. It should ensure that network performance (service quality of the network) and network security is sufficient to support the institution's business processes. The network audit may require some comparisons of configuration files. Practical examples of how to compare files and find differences and/or changes are included in this part, as are references to the tools which internal audit can use during the network audit for vulnerability assessment, network device inventory, etc.

Part 6 discusses writing the IT audit report. The IIA's International Professional Practices Framework (IPPF) and ISACA's Information Technology Audit Framework (ITAF) set out what to include. It is important that internal audit standards are followed in the writing of all audit reports. IT audit reports can be especially challenging to write, as auditors must effectively discuss technical issues and seek to bring necessary change for the institution, taking into account that in most cases the institution's leadership will likely not have any IT background or deep understanding of IT risks. Key tips included in this section for writing an IT audit report are:

- Keep it simple,
- Keep your objectives in mind,
- Write as a strategic partner of senior management, aiming to help them identify possible improvements to IT strategy, IT risk management, and the IT control environment.

PART 1 BACKGROUND

In today's digital world, it is difficult to imagine a government institution without IT. Many organizations and institutions, regardless of size and area of operation, have come to realize the importance of using IT to keep pace with the current digital world. Governments and public sector entities have invested in IT as they recognize the benefits it can bring to their operations. Given this significant and growing dependency on IT, it is essential that IT systems both provide the required functionality and are reliable, secure, and invulnerable to computer attacks from inside or outside.

An IT audit (sometimes also referred to as **information system audit**) is concerned with IT governance and management, infrastructure and systems, and the operations and related processes of an organization/institution. There are three main types of IT audit:

- Audit to support the financial/budget/performance/statistical information, when the focus is mainly on **application controls** (the set of controls embedded within automated solutions over transactions, sometimes it called controls over the input, processing, and output functions).
- Audit to evaluate compliance to applicable laws, regulations, policies, and standards related to IT, when IT **general controls** are in focus.

- As a performance audit, to determine whether effective governance and management of IT systems are in place, that they are effective, and that IT creates value for institution/organization.

Information/cyber security is a major and important part of IT audit to ensure data and information, the infrastructure, and the network are safe from attack. This focuses on the three cornerstone components of information security:

1. Confidentiality - protecting information from disclosure to unauthorized users. Information such as defense data, health data, contract data, and personal information should be kept private and confidential.
2. Integrity - protecting information from being modified by unauthorized users.
3. Availability - ensuring authorized people have access to the information they require to deliver public services when needed. Denying authorized users access to information is quite a common attack in this digital era. Users can also be denied access to data through natural disasters such as floods, earthquake, hurricanes, or accidents such as power outages or fire.

The IT auditor role includes:

- Participating in the development of high-risk systems to ensure appropriate IT controls are in place.
- Auditing of existing information systems.
- Providing IT support to other auditors.
- Providing IT risk/control consulting services.

Senior management have an expectation that the internal audit activity will provide assurance around all important risks. Many public sector institutions currently lack the required IT knowledge to cover all the above-mentioned activities. As the role of IT audit increases in importance in this digital world, public sector auditors need to rise to this challenge.

COVID-19 and Cyber Resilience

IT audit has never been more important. Restrictions imposed due to the COVID-19 pandemic has initiated an unprecedented shift to online working and digital provision of public services, transforming the way we work. However, remote working heightens existing cyber risks and introduces new ones to many institutions. According to multiple reports from companies involved in threat intelligence, there has been a significant increase in malicious email traffic since the start of the pandemic, often masquerading as official correspondence regarding COVID-19.

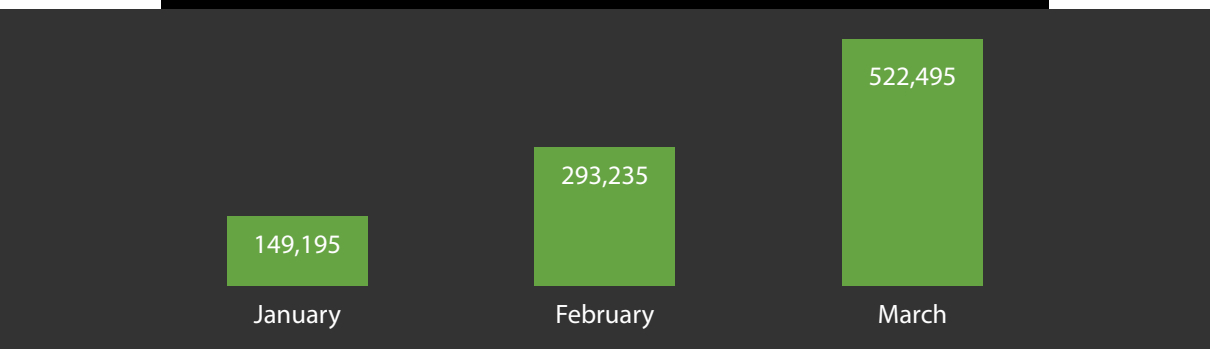
For institutions to survive and thrive in this new-digital world, maintaining cyber resilience is paramount. Some illustrative statistics:

1. 81% of companies now have a crisis response team in place that can act quickly in case of IT-related events.[3]

2. 71% of executives are worried about continuity and productivity during the pandemic.[4]

3. Cybercriminals are taking advantage of the crisis. Over a 24-hour period, Microsoft detected a massive phishing campaign using 2,300 different web pages attached to messages and disguised as COVID-19 financial compensation information that led to a fake Office 365 sign-in page.[5]

Figure 1. Phishing sites detected by Google, 2020



Source: https://transparencyreport.google.com/safe-browsing/overview

[3] Gartner, COVID-19 Bulletin: Executive Pulse, 3 April 2020

[4] Gartner, COVID-19 Bulletin: Executive Pulse, 3 April 2020

[5] https://www.darkreading.com/threat-intelligence/after-adopting-covid-19-lures-sophisticated-groups-target-remote-workers/d/d-id/1337523

4. 54% of human resource leaders indicated that poor technology and/or infrastructure for remote working was the biggest barrier to effective remote working in their organization.[6]

The above statistics should be taken as "call to action" for the public sector. Internal audit must support public sector institutions take proper actions to mitigate risks from increasing digitalization of work processes.

Three key areas for internal audit focus specifically related to the pandemic are:

ACCESS

When working at the office, inside the institution's perimeter, corporate security stops > 99% of threats. When workers are accessing the institution's system from home there are likely more vulnerabilities. Given these increased risks, internal audit should be addressing the following questions:

- Are there clear remote access policies (who, what, when, and how)?
- Is there robust authentication of remote users and devices?
- What about encryption methods?
- Is there proper endpoint security (secure remote access devices)?
- Is there network security monitoring?
- Are proper user awareness campaigns in place?
- Are there additional security controls for critical functions?

CYBER SECURITY

Realistically, it is not a matter of "if" but "when" an institution will come under attack from hackers. It is essential, and much demanded by senior management, that internal audit seek assurance of organizational resilience to cyber-attacks.

[6] Gartner, Coronavirus in Mind: Make Remote Work Successful, 5 March 2020

BUSINESS CONTINUITY MANAGEMENT

The public sector often lacks rigorous business continuity management and it is rarely the subject of regular public sector internal audit. Key assurance questions for boards and for internal auditors are:

- Is the internal control environment sufficient to protect your institution?
- Are business continuity plans in place, updated based on COVID-19 risks, and tested as needed?
- Have you ever audited your entire business continuity management process, including emergency response, crisis management and business continuity?

PART 2

IT AUDIT STANDARDS, FRAMEWORKS, BEST PRACTICES, AND GOVERNANCE

C IT audit standards and frameworks

There is no single best practice framework for IT audit. It is not included in the mandatory guidance provided by the IIA within its IPPF. The IIA has instead produced a series of 16 GTAG[7] that are available for IT auditors to use to help keep pace with the ever-changing and sometimes complex world of IT. ISACA has developed its own framework, tools, technical guides, and other resources for use by IT auditors and offer certification as an ISACA Certified Information Systems Auditor (CISA). While it is not yet common in the public sector to have CISA certified auditors, this is something for senior management to consider going forward or to co-source from the private sector.

GLOBAL TECHNOLOGY AUDIT GUIDES

The GTAG series provide an overview of IT-related risks and controls written in a reader-friendly style, rather than in highly technical language. They can help

[7] https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG1.aspx. GTAG 6 has been deleted from the International Professional Practices Framework (IPPF). Some of its concepts are combined with the 2nd edition of GTAG 4.

internal auditors become more knowledgeable about the risks, controls, and governance issues surrounding technology.

The goal of the first GTAG is to help internal auditors become more comfortable with general IT controls. It aims to enhance communication with those charged with governance (e.g. ministers or audit committee) and the central harmonization unit; and improve the exchange of risk and control ideas with the chief information officer (CIO) and IT management of the organization or the IT shared service (or outsourcing) provider. GTAG 1 describes how members of governing bodies, executives, IT professionals, and internal auditors address significant IT-related risk and control issues and presents relevant frameworks for assessing IT risk and controls. Moreover, it sets the stage for subsequent GTAGs that cover specific IT topics and associated business roles and responsibilities in greater detail.

Although many of the GTAG papers were published some years ago they remain in force and are still useful.

Available Global Technology Audit Guides

1. Information Technology Risk and Controls
2. Change and Patch Management Controls: Critical for Organizational Success
3. Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
4. Management of IT Auditing
5. Auditing Privacy Risks
6. Managing and Auditing IT Vulnerabilities
7. Information Technology Outsourcing
8. Auditing Application Controls
9. Identity and Access Management
10. Business Continuity Management
11. Developing the IT Audit Plan
12. Auditing IT Projects
13. Fraud Prevention and Detection in an Automated World
14. Auditing User-developed Applications
15. Information Security Governance
16. Data Analysis Technologies

THE IT AUDIT FRAMEWORK

ISACA has its own standards and framework for IT audit. The ITAF, 4th edition published October 2020,[8] is a comprehensive IT audit framework that:

- Establishes standards that address IT audit and assurance practitioners' roles and responsibilities, ethics, expected professional behavior, and required knowledge and skills;
- Defines terms and concepts specific to IT audit and assurance;
- Provides guidance and techniques for planning, performing, and reporting of IT audit and assurance engagements.

Based on ISACA material, ITAF provides a single source for IT audit and assurance practitioners to obtain guidance on the performance of audits and the development of effective audit reports. The 3rd Edition incorporated IT audit and assurance standards and guidance effective November 1, 2013.

As many public sector institutions do not have IT auditors, the important standards below may be overlooked. According to ITAF, IT Audit and Assurance Standards Statements, General Standards require:

1001 Audit Charter

1001.1 The IT audit and assurance function shall document the audit function appropriately in an audit charter, indicating purpose, responsibility, authority and accountability.

1004 Reasonable Expectation

1004.1 IT audit and assurance practitioners shall have reasonable expectation that the engagement can be completed in accordance with applicable IT audit and assurance standards and, where required, other industry standards or applicable laws and regulations that will result in a professional opinion or conclusion.

[8] https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4

1006 Proficiency

1006.1 IT audit and assurance practitioners, collectively with others assisting with the audit and assurance engagement, shall possess the professional competence to perform the work required.

1006.2 IT audit and assurance practitioners shall possess adequate knowledge of the subject matter to perform their roles in IT audit and assurance engagements.

1008 Criteria

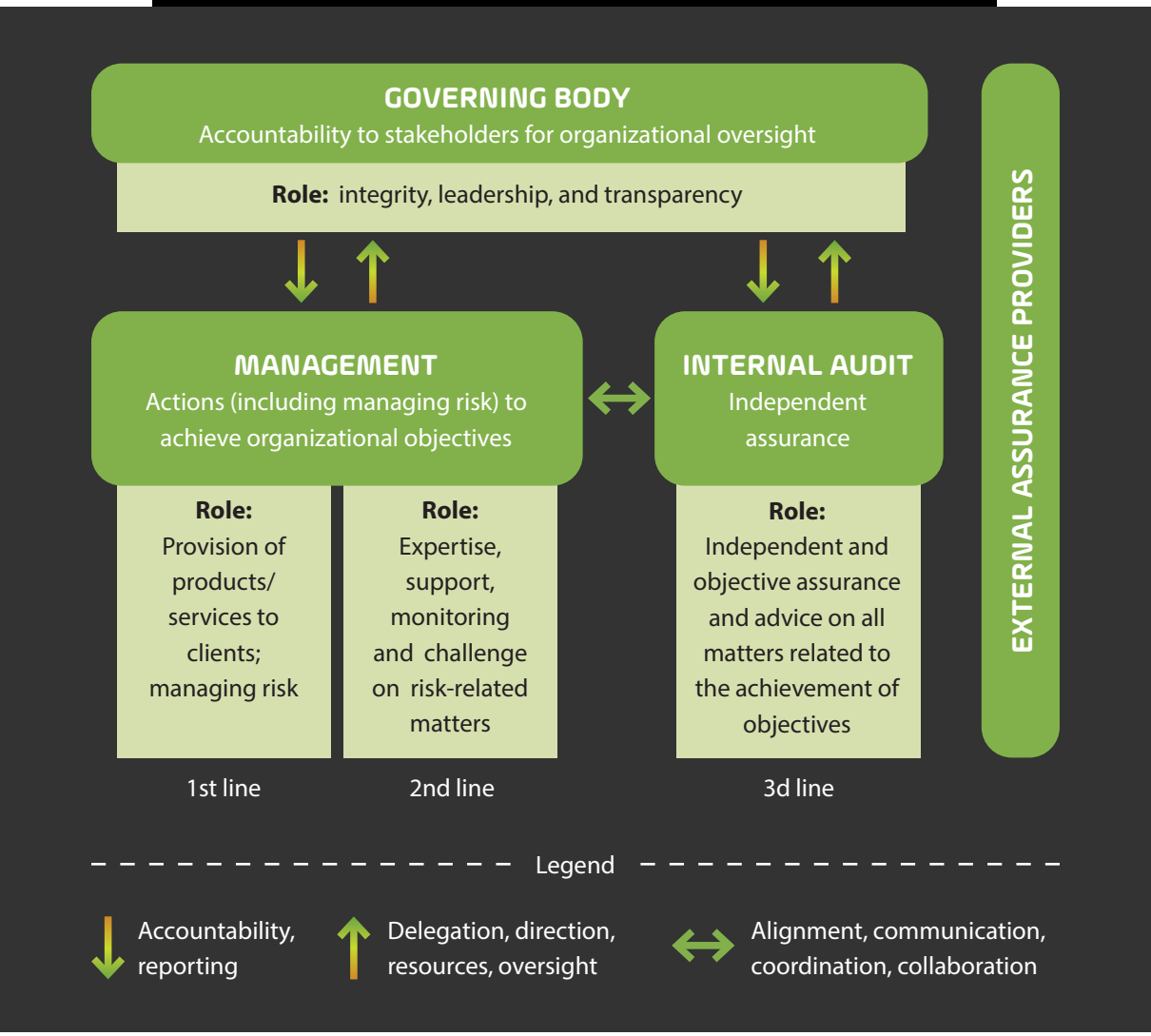
1008.1 IT audit and assurance practitioners shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, reliable, measurable, understandable, widely recognized, authoritative, and understood by, or available to, all readers and users of the report.

IT audit governance

An important aspect of internal audit, including IT audit, is to understand and promote the Three Lines Model of the IIA. Independent assurance through internal/IT auditors is in the third line. However, in many public sector institutions the second line is missing, and it can be challenging for internal audit to avoid being responsible for risk management or even designing and implementing internal controls, different regulations, and internal policies. According to the updated Three Lines Model, internal audit should be aligned with the institution's strategies and objectives and should closely cooperate and collaborate with management to provide independent assurance to the governing body.

In the public sector being independent can be challenging. Many internal audit teams work under the direct supervision of management while auditing the functions and activities of the same management. For example, in many ministries internal audit is not independent by organizational structure–it is challenging to be objective when you audit your management.

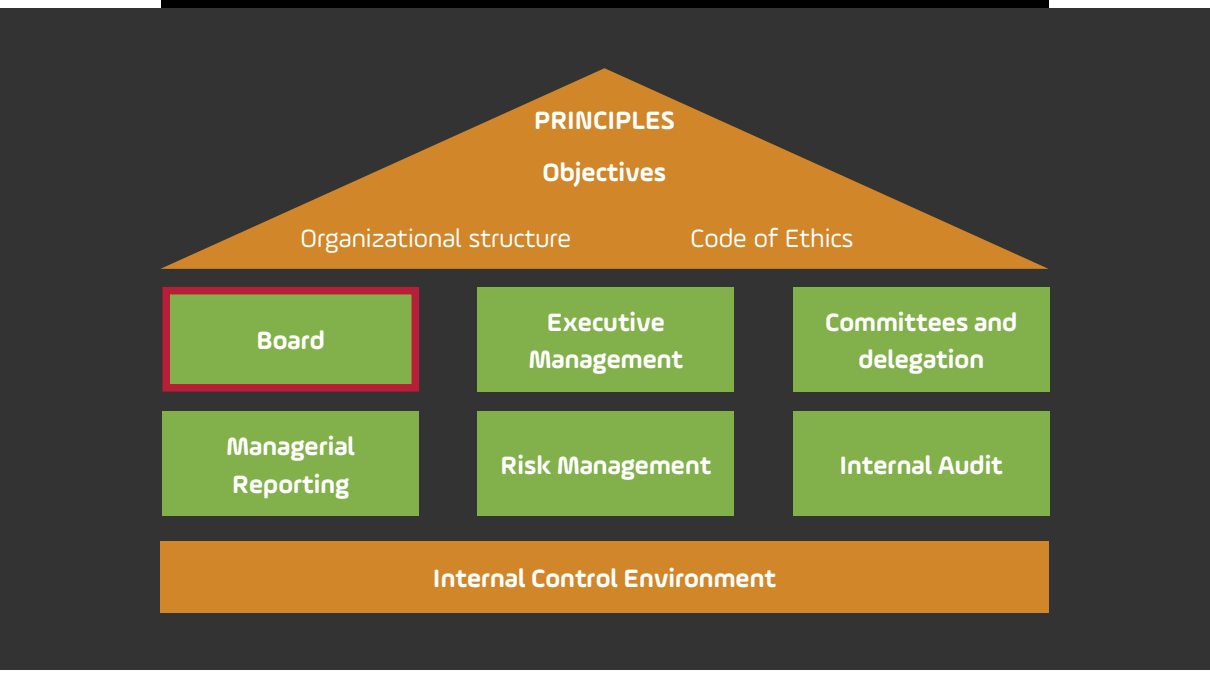
Figure 2. The IIA Three Lines Model



Irrespective of the organizational structure, internal/IT auditors need to understand the governance model and help senior management with governance, risk, and control by providing objective assurance. It is vital for all public sector auditors to understand the institution's governance as well as the institution's principles, objectives, organizational structure (responsibilities and who reports whom), and code of ethics. If these represent the roof (see Figure 3), the internal control environment is the foundation that internal audit needs to fully understand and

objectively report on any issue in this layer. In the governance structure of many public sector institutions, the board (outlined in red in Figure 3) is missing, hence the presence of a strong audit committee is advised, preferably with independent-external members as well as members with IT knowledge to handle and oversee IT related issues.

Figure 3. General Governance model



IT governance framework

IT governance is a subdiscipline of organizational governance consisting of the leadership, organizational structures, roles and responsibilities, policies, and processes which ensure that the organization's IT supports the organization's strategies and objectives. IT governance underpins the organization's regulatory, legal, environmental, and operational requirements to enable the achievement of strategic plans and aspirations.

It is the responsibility of senior management to integrate and institutionalize good IT practices. In the absence of IT governance, the IT auditor should not go into IT infrastructure in any depth, for example to do a network audit.

Several IT governance frameworks exist that can help internal audit develop the most appropriate risk assessment approach for their institution and then develop the IT audit universe and IT annual plan based on the institution's risk-profile. Two of the most common are COBIT and the ISO 27000 series.

COBIT, developed by ISACA, is a good framework for IT Governance. As IT audit is not very well developed in the public sector, COBIT 4.1, or the more recent COBIT 2019,[9] can be used to introduce IT governance processes, develop IT audit universe and IT annual plans, and to assess IT governance at the highest institutional level. COBIT 4.1 links five high level governance focus areas (strategic alignment, value delivery, resource management, risk management, and performance measurement) with processes used by operational management to organize and manage ongoing IT activities (see Part 3).

[9] https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/developing-the-it-audit-plan-using-cobit-2019

PART 3

IT AUDIT UNIVERSE AND IT ANNUAL PLAN

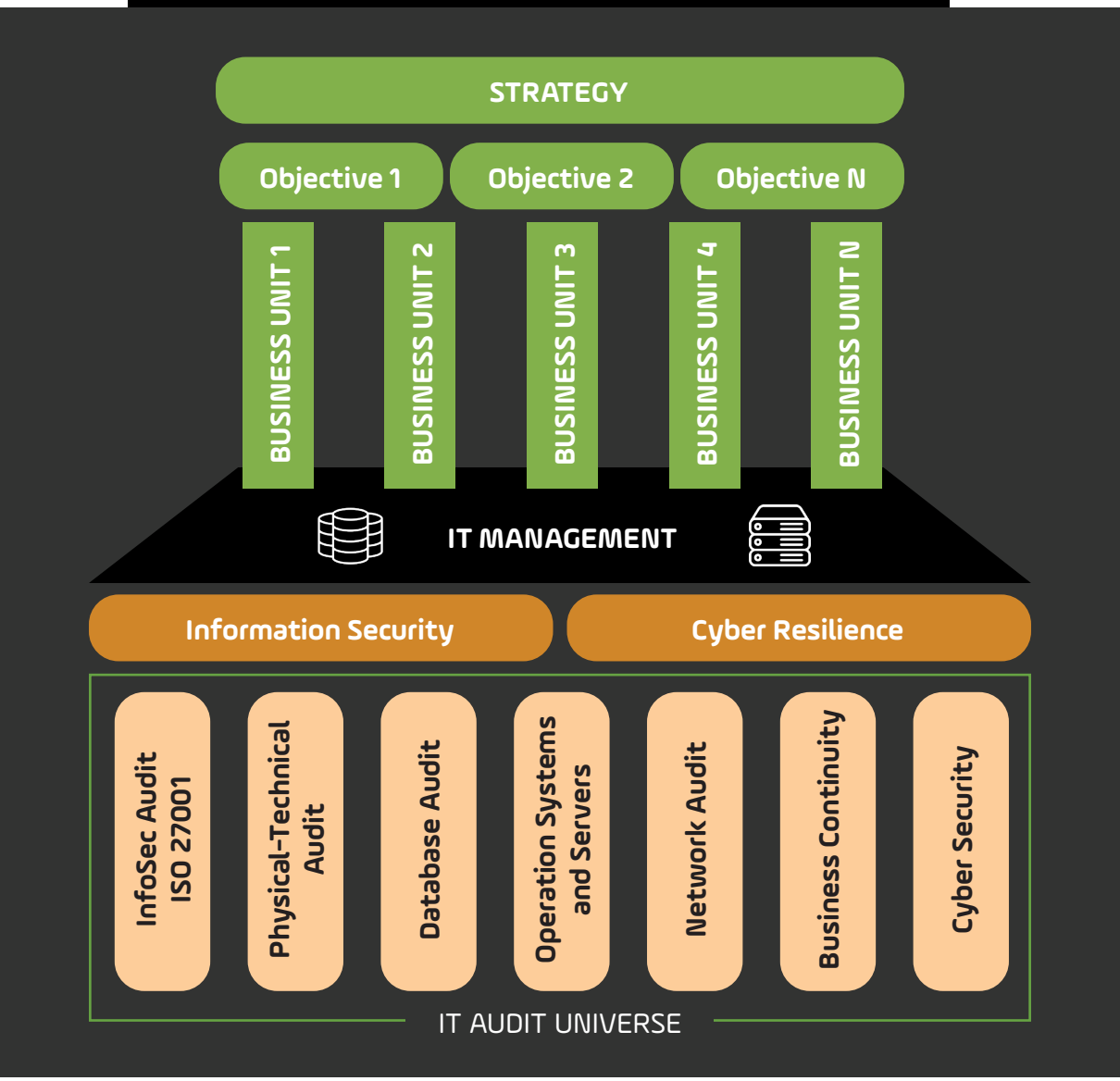
As technology becomes more integral to the organization's operations and activities, a major challenge for internal auditors is how to best approach an organization-wide assessment of IT risks and controls within the scope of their overall assurance and consulting services. Auditors require a good understanding of the organization's IT environment; the applications and computer operations that are part of the IT infrastructure; how IT applications and operations are managed; and how IT applications and operations link back to the organization.[10]

From a governance perspective, IT is a horizontal support function and relates to the organization's main processes and/or activities. IT should also be an enabler, to support and enable main business functions to operate more productively and support business-users with reliable products and services in line with the institution's objectives. For example: budgeting is the main process for a ministry of finance. IT should: provide a proper solution (for example an application) to enable the budgeting process; support all users working with the budgeting-application; and ensure that the entire IT infrastructure (network, databases, operating systems, etc.) functions to meet the institution's objectives.

[10] https://chapters.theiia.org/montreal/ChapterDocuments/GTAG 11 -Developing the IT Audit Plan.pdf

As more public services are digitized and e-government services increase, the importance of cybersecurity grows. Increasingly the focus is on cyber resilience, which the United States National Institute of Standards and Technology defines as: *The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources*.[11] Hence, the IT audit should provide proper assurance on cyber-resilience.

Figure 4. IT Audit Universe approach



[11] https://csrc.nist.gov/glossary/term/cyber_resiliency

Preparing an IT audit universe is not a complex task and there is no "one size fits all" approach. However, the following critical factors need to be addressed:

- Effective IT audit universes incorporate a **risk-based approach that matches each IT item to a business process**, which in turn correlates to the strategic objectives.
- Chief audit executives demonstrate to senior management how the IT audit universe will **add value to each process** under review, as well as how each process can impact the organization's strategic goals and objectives.
- Management is **involved** in identifying and validating the IT audit universe and annual IT audit plan and **supportive** of IT internal audit recommendations.

Internal/IT auditors should consider many organizational factors when developing the IT audit universe and the annual IT-audit plan. These will include the complexity of business processes, geographic locations of operations, etc. The following are example of questions to be addressed when developing the IT audit universe:

- What technologies are used to perform daily business functions?
- Is the IT environment relatively simple or complex?
- Is the IT environment centralized or decentralized?
- To what degree are business applications customized?
- Are some or all IT maintenance activities outsourced?
- To what degree does the IT environment change every year?

IT is in a perpetual state of innovation and change. These continuous changes require IT auditors to regularly identify and understand the impact of risks. IT auditors should:[12]

- Perform independent IT risk assessments every year to identify the new technologies that impact the organization.
- Become familiar with the IT department's annual short-term plans and analyze how these impact the IT risk assessment.
- Begin each IT audit by reviewing its risk assessment component.
- Be flexible with the IT audit universe — monitor the organization's IT-related risk profile and adopt audit procedures as it evolves.

[12] GTAG 4: Management of IT Auditing

According to GTAG 11, development of the IT audit universe and annual audit plan consists of four main steps as set out in Figure 5.

Figure 5. Steps to develop the IT audit universe and annual plan[13]

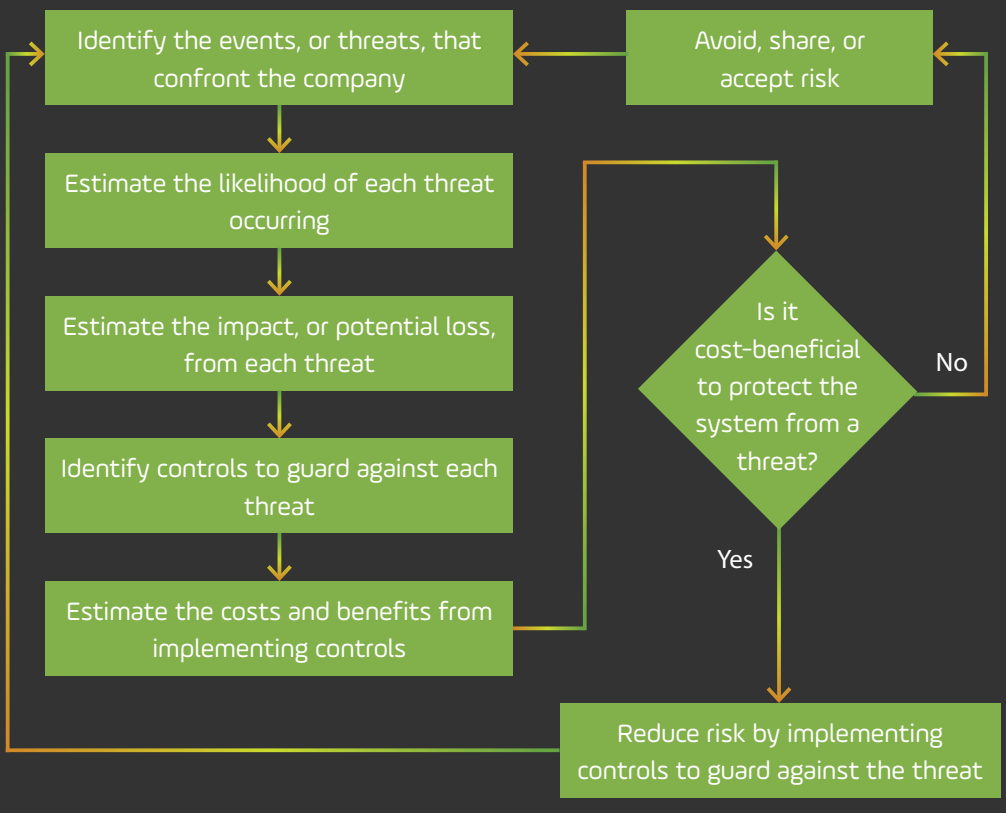
[13] GTAG 11: Developing the IT Audit Plan

IT risk assessment

Management should design effective internal control systems to reduce inherent risk, in this case of IT. IT audit should evaluate internal control systems to ensure that they are operating effectively. The annual risk assessment is the most important part of IT audit in this fast-changing digital world. However, the annual plan which results from the annual risk assessment is not "written in stone" and should be reviewed in a timely manner and updated when new risks arise. As IT risks evolve, IT audit should help management to address them. It is important to assess and understand the cost of IT controls, which requires proper knowledge and expertise.

The risk management process in many public sector institutions is not sufficiently robust. The steps presented in Figure 6 should be taken to address the risks.

Figure 6. Risk management process map



IT audit universe based on COBIT

COBIT 4.1 provides a generic process model (see Figure 7 below) representing all the processes normally found in IT functions that can be used to develop the IT audit universe for any institution.

Figure 7. COBIT 4.1 process model

Answer to each question in 1-4 scale (*1 - not importanat, 4 - very important*)

Process #	Processes	Inherent Risk (H, M, L)	Internal Control (H, M, L)	Residual Risk (H, M, L)	Inherent Risk						Internal Control						SUM of Residual Risk	Periodicity of examination
					SUM of Inherent Risk	Risk factor 1	Risk factor 2	Risk factor 3	Risk factor 4	Risk factor 5	SUM of Internal Control	Control factor 1	Control factor 2	Control factor 3	Control factor 4	Control factor 5		
						25	25	15	25	10		25	25	20	15	15		
Plan and Organise (PO)																		
PO 1	Define a strategic IT plan.	H	H	H	400	4	4	4	4	4	400	4	4	4	4	4	16.0	1 Year
PO 2	Define the information architecture.	L	L	L	0						0						0.0	5 Years
PO 3	Determine technological direction.	L	L	L	0						0						0.0	5 Years
PO 4	Define the IT processes, organisation and relationships.	L	L	L	0						0						0.0	5 Years
PO 5	Manage the IT investment.	L	L	L	0						0						0.0	5 Years
PO 6	Communicate management aims and direction.	L	L	L	0						0						0.0	5 Years
PO 7	Manage IT human resources.	L	L	L	0						0						0.0	5 Years
PO 8	Manage quality.	L	L	L	0						0						0.0	5 Years
PO 9	Assess and manage IT risks.	L	L	L	0						0						0.0	5 Years
…	…	…	…	…	…						…						…	…

For each COBIT 4.1 process, the IT auditor must assess inherent risk and internal control to help determine how often to audit that process. This will vary for different institutions, for example, *PO1 – Define a Strategic IT Plan* may not be one of the most important processes to audit in e.g. a ministry of sport, but for a ministry of finance or ministry of health implementing e-health services, the IT strategy may be very important and should be included in the IT audit annual plan.

The following three major processes should always be included in the IT audit universe to address important and strategic IT risks:

- IT Governance and Management
- Information Security
- Cyber Resilience

Figure 8 presents an IT audit universe approach based on COBIT. Activities and risks within IT that need to be managed are ordered into the domains of plan and organize (PO) - providing direction to solution delivery and service delivery; acquire and implement (AI) providing solutions and seeing them turned into services; deliver and support (DS) - receiving solutions and making them usable for end users; and monitor and evaluate (ME) monitoring processes to ensure that the direction provided is followed.

Figure 8. IT Audit Universe based on COBIT 4.1

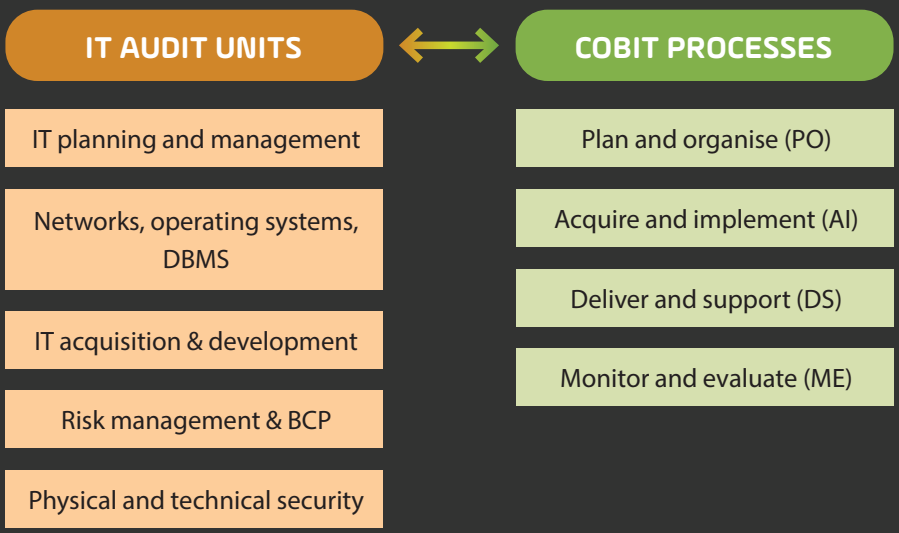


Table 1. Example IT Audit Universe based on COBIT 4.1

Audit Unit	Audit Unit per COBIT	Scheduled for 2018	Scheduled for 2019	Scheduled for 2020
IT planning and management	PO1		X	
	PO2		X	
	PO3		X	
	PO4		X	
	DS3		X	
IT planning and management - monitoring	PO8			X
	M1			X
	M2			X
	M3			X
	M4			X
Networks	DS9	X		X
	DS10	X		X
	DS13	X		X
	AI6	X		X
Databases	DS9	X		X
	DS10	X		X
	DS11	X		X
	DS13	X		X
	AI6	X		X
	AI7	X		X
Operating Systems	DS9		X	
	DS10		X	
	DS13		X	
	AI6		X	
	AI7		X	
Acquisition and development of IT applications	AI1	X		
	AI2	X		
	AI3	X		
	PO10	X		
Business continuity planning	DS1			X
	DS2			X
	DS4			X
	DS8			X

Audit Unit	Audit Unit per COBIT	Scheduled for 2018	Scheduled for 2019	Scheduled for 2020
Information security according to SO27001:2013	DS5	X	X	X
Physical and technical security	DS12	X		X

In the example outlined in Table 1, the IT audit universe consists of nine IT audit units:

1. IT planning and management
2. IT planning and management – monitoring
3. Networks
4. Databases
5. Operating Systems
6. Acquisition and development of IT applications
7. Business continuity planning
8. Information security
9. Physical and technical security

Each IT audit unit is mapped to one or more COBIT processes.

For example, *physical and technical security* is only mapped to the DS12 process, while *IT planning and management – monitoring* is mapped to COBIT ME domain processes M1, M2, M3, M4 and PO8. Information security audit is mapped to DS5 process or the ISO 27000 series could be used, based on the scope and strategic objectives of the institution.

The ISO/International Electrotechnical Commission (IEC) 27001 is part of the ISO 27000 series of standards, that offer best practices to help organizations improve their information security. 27001 is the only standard in the series that organizations can be audited and certified against.

IT audit approach

According to the International Standards for the Professional Practice of Internal Auditing, "*internal auditors are expected to have sufficient knowledge of key IT risks and controls, and available technology-based audit techniques to perform their assigned work*".

There are three main types of IT audit:

- Vertical (or application) approach
- Deep vertical approach
- Horizontal approach

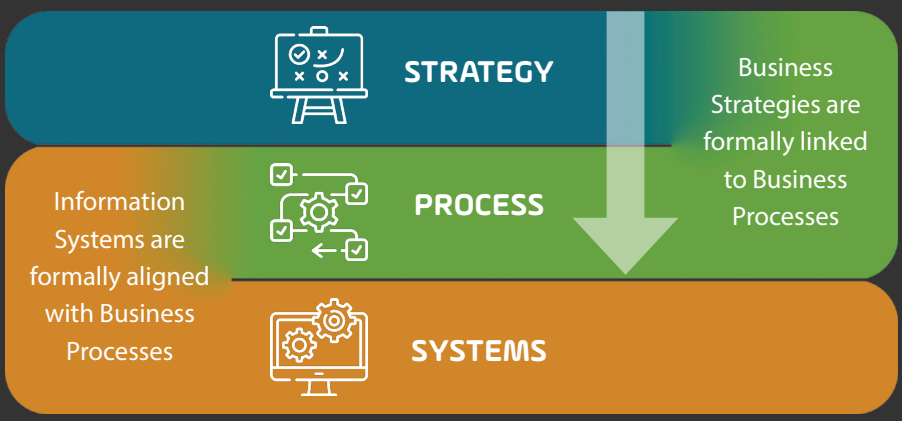
Vertical approach

Looks at applications controls (the controls embedded within automated solutions, sometimes called input-processing-output controls). Application controls are designed to prevent, detect, and correct transaction errors and fraud in application programs.

For example, audit of the budgeting process would look at the following supporting application controls:

- Input Authorization,
- Data validation
- Editing procedures

Figure 9. Vertical audit

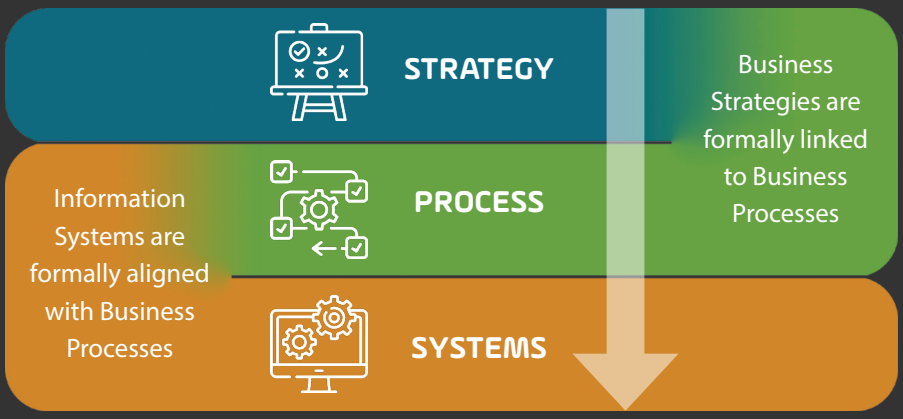


Deep vertical approach

Looks at application controls and IT general controls, as the effectiveness of application controls depends on the effectiveness of IT general controls.

For example, system/software acquisition, development and maintenance; change management; backup & restore etc.

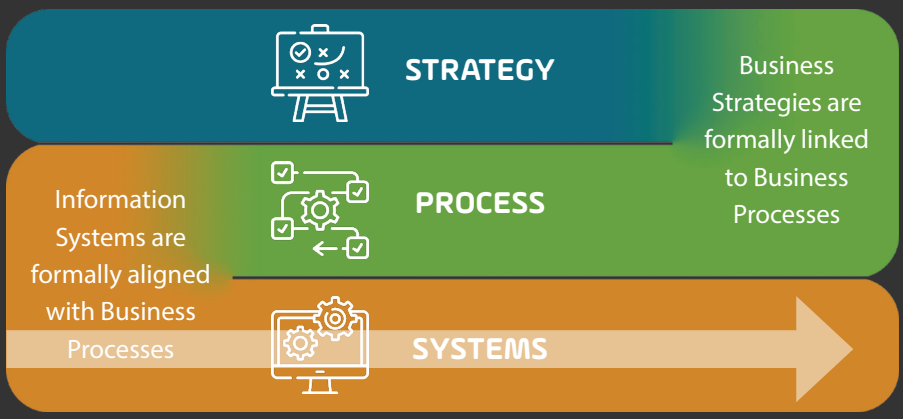
Figure 10. Deep vertical audit



Horizontal approach

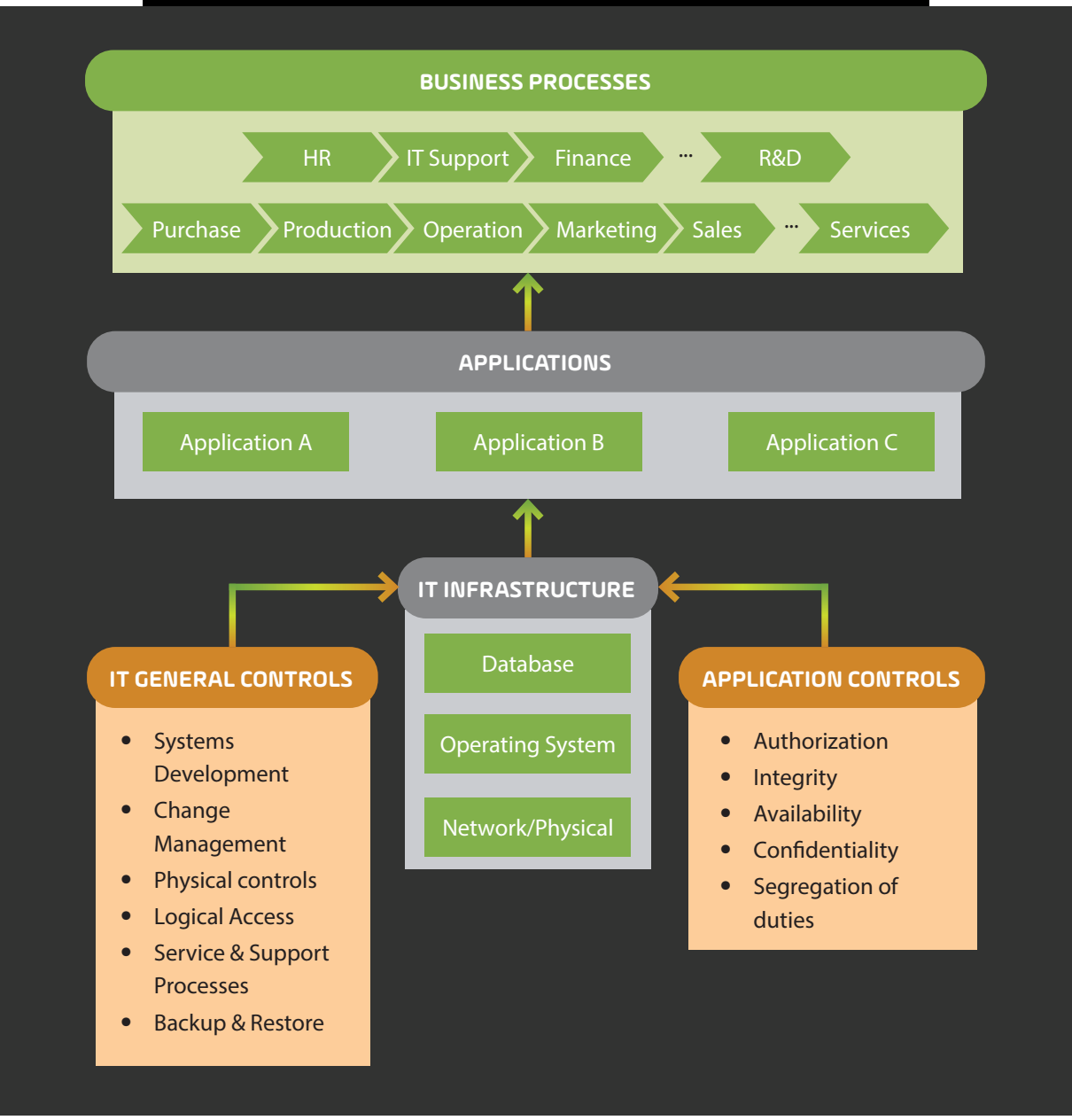
Looks at all relevant IT controls and all databases supporting different business processes and applications. Examples include information security audit, database management system audit, and network audit. Horizontal audit requires deep IT knowledge, and a solid understanding of networks, database management systems, and the entire IT infrastructure.

Figure 11. Horizontal audit



The entire IT audit universe can be summarized in Figure 12.

Figure 12. IT audit universe[14]



[14] https://www.iiacolombia.com/resource/guias/GTAG11.pdf

Pre-implementation audit

The development of IT projects can be expensive and take several years; IT audit can increase its value by supporting this phase. Pre-implementation audit can be relevant during the design and development of new applications, infrastructures, or IT processes or when making any significant changes to those already existing.

This may help to avoid costly changes at a late stage and could ensure that proper controls are built into the project from the design stage of system development.

For pre-implementation audit, the following issues are important:

- Avoid participation in actual design work
- Specify the need for "key controls" but not what precise form they should take
- Separate pre and post-implementation audit teams

The key success factors and challenges for pre-implementation audit are summarized in Table 2.

Figure 13. The value of pre-implementation audit

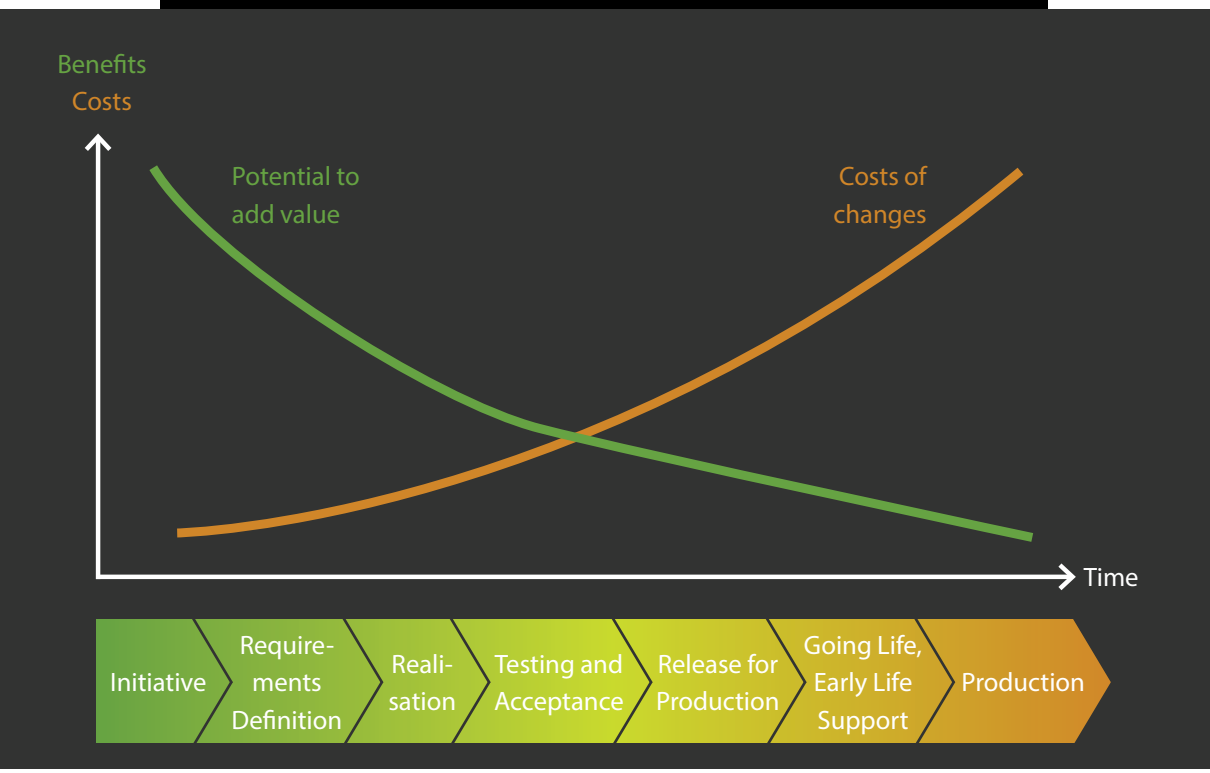


Table 2. Pre-implementation audit success factors and challenges

Critical success factors	Challenges
• Begins during the project initiation phase. • Has good coordination between the project manager and the auditor. • Is performed in parallel with the project. • Reports the results in a timely manner. • Involves senior auditors with relevant expertise, including of project management, and an understanding of the processes to be addressed by the project under development.	• Auditors may be viewed as a member of the project team rather than independent of the team. • Performing pre-implementation audits may impair the auditors' independence. • In a pre-implementation audit an auditor usually gets only draft versions of the documents for review.

PART 4

IT AUDIT PLANNING AND EXECUTION

The planning and execution of IT audit engagement does not differ much from any other operational or financial audit, although IT auditors may require some specific knowledge and expertise (See *Part 3: IT Audit Approach*).

IT audit engagement planning may include the following steps:

Planning

Step 1. Determine initial scope, objectives, timing, and engagement team.

- Determine the audit engagement team requirements.
- Assess compliance with ethical requirements, including independence.

Step 2. Heads up to auditee and/or send Initial Letter

Step 3. Perform initial analysis and data collection

Step 4. Determine time-budget of the engagement

Step 5. Understand the process in detail, finalize audit scope, and create risk control matrix

- Process Description
- Detailed Process Map
- Process Risk
- Audit Control
- Audit Sampling

If there is a large audit team (and the audit is not confidential) encourage discussion of engagement scope and risk assessment results, seeking team members' input.

Step 6. Discuss the scoping and risk assessment of the engagement with the audit team

Step 7. Finalize risk control matrixes and audit program

Step 8. Arrange kick-off meeting with auditee and send fieldwork announcement Letter

C Execution/fieldwork

Step 9. Obtain, analyze, and document information

Step 10. Perform control testing, prepare work-papers, and complete risk control matrixes

- Work-paper
- Audit control
- Audit issue
- Residual risk and risk conclusion

During the fieldwork, it's important to follow the Criteria > Condition > Cause > Effect approach.

Step 11. Complete work-paper first level review and compile issue/finding summary

Reporting and audit closure

Step 12. Complete work-paper second level review and prepare draft report

Step 13. Discuss draft report with auditees and finalize management action plans

Step 14. Finalize audit report and send/present to audit committee or senior management

Step 15. Make final changes to audit report if necessary

Step 16. Issue the final audit report and obtain feedback from auditee

Step 17. Discuss with the engagement team and chief audit executive the overall performance of the team and the lessons learned

Methods for testing IT general controls

Table 3. Methods for testing IT general controls

Testing Method	Testing Method Definition
Inquiry	The examiner inquires (*in writing or verbally*) of the responsible individual as to what procedures are in place to address the control being tested. **This is typically the first step in each test.**
Inspection	The examiner inspects the evidence provided to ensure that it is accurate.
Corroborative Inquiry	The examiner inquires with one individual and corroborates the inquiry separately with another individual.

Testing Method	Testing Method Definition
System Query	The examiner tests that automated controls within an IT application are operating as expected. Examples of these kinds of controls may be: • That a predefined exception will be identified appropriately by the system (this exception may be associated with completeness and/or accuracy of input, processing, and output of the application) • That logical access configuration within the application are set in a way that establishes segregation of duties and otherwise provides for the authorization of transactions.

Test of design vs. test of operational effectiveness

Test of design determines whether the controls, if operating properly, can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements. Procedures the IT auditor may perform to test and evaluate design effectiveness include inquiry, observation, and inspection of relevant documentation. Performance of these procedures might provide evidence that can be used to test the effectiveness of the control.

Test of effectiveness involves evaluating whether internal control is operating as designed. Procedures the IT auditor may perform to test and evaluate test of operating effectiveness include inquiry, observation, and inspection of relevant documentation.

IT auditor questions on testing:

Test of design = Was the control designed appropriately?

Test of operational effectiveness = Was the control consistently performed? Was the control performed by a person who had the necessary authority and qualifications to perform the control effectively?

EXAMPLES

Audit Term	Test Step
Inquiry	Inquire of the IT Operations Manager to gain an understanding of how user IDs are assigned to new users within each critical application.
	Test Results
	Inquired with the IT Operations Manager, Joe Smith, on March xx, 20xx, and noted that accounting application and active directory user IDs are administered by the IT Department. It is noted that new users are assigned a unique ID based on the standard protocol of first initial and last name.

Audit Term	Test Step
Inspection	Obtain and inspect the "Backup and Restore Policy" to determine if the policy clearly defines procedures in place for restoring and testing backups for critical systems.
	Test Results
	Obtained and inspected the "Backup and Restore Policy" from the company's intranet on March xx, 20xx, and noted that page 5 of the policy details the procedures for restoration testing as follows: **"A structured test of the restore process will be performed to verify the quality and reliability of all backup tapes. All test details including the scope of the test, procedures and results will be documented in the ticketing system to maintain a record of the testing history."**

Inquiry alone is never sufficient to provide a level of certainty that a **control is operating effectively.** It should always be used in conjunction with one or more of the other procedures. As a result, the inquiry step will only have a conclusion if an exception was noted during the inquiry.

Audit Term	Test Step
Corroboration	Corroborate the inquiry of the IT Operations Manager with the Database Administrator. Test Results Corroborated the inquiry of the IT Operations Manager, Joe Smith, with the Database Administrator, Angelina Jolie, on March xx, 20xx, and noted that user IDs are administered by the IT Department. It was noted that new users are assigned a unique ID based on the standard protocol of first initial and last name.

Audit Term	Test Step
System Query	Perform a system query to obtain the security configuration for Windows Active Directory and inspect that there is proper configuration to require a password with a minimum of 8 characters, that is complex (1 upper case, 1 lower case and a special symbol), and is set to expire after 90 days. Test Results Examiner observed the Windows Active Directory administrator, Jim Carey, perform a system query to obtain the security configuration on June xx, 20xx. Examiner inspected the password configurations and noted that the system was properly configured to require a password with a minimum of 8 characters that is complex (*1 upper case, 1 lower case and a special symbol*) and that is set to expire after 90 days.

Audit Term	Test Step
Observation	Observe the Support Services Supervisor create a work order in the ticketing system. Perform a system query to obtain the audit history log from the system to determine if the work order created by the Supervisor is appropriately tracked in the system.
	Test Results
	Examiner observed as the Support Services Supervisor, Donald Trump, performed work order #8937 in the Remedy ticketing system on January xx, 20xx and noted that all modifications made by Donald to work order #8937 were captured by the Remedy ticketing system.

Audit Term	Test Step
Re-Performance	Execute a system query to obtain a list of inventory items acquired during the 20xx fiscal year. Judgmentally select a sample of 15 items. Re-perform the calculation of the average cost of the items to determine that the average cost of parts is properly calculated by the accounting system.
	Test Results
	The Inventory Manager, John Smith, executed a system query to obtain a list of items acquired during the 20xx fiscal year on June xx, 20xx. Auditor judgmentally selected a sample of 15 items and re-performed the calculation of the average cost of parts on June xx, 20xx and noted the following...

During observation, evidence must be retained that supports the control being observed. Observation is a weaker form of assurance than the other procedures and should be performed in conjunction with other procedures where possible. Re-Performance is not typically performed as part of IT general controls testing.

Practice Exercise

Control Description: Only authorized individuals have administrator access to accounting application on the application level.

For the control description above, answer the following questions:

1. What pieces of evidence should be obtained?
2. How do you determine the sample size?
3. What testing steps are necessary to test this control?

Sample Size: The sample size for a system access control depends on the criticality of system; number of user accounts etc.

Testing Steps:

1. Inquire with IT to gain an understanding of how the security is configured in the accounting application.
2. Observe IT generate a system query to obtain the list of accounting application users.
3. Compare the list of administrators to the IT organization chart or active employee listing to determine if user access is in line with job responsibilities.
4. Inquire with IT Management to determine if the individuals with administrator access are appropriate.

PART 5

THREE EXAMPLES OF IT AUDIT

C Business continuity management audit

Business continuity management aims to minimize the financial and other impacts to a business caused during a disaster or business disruption and is a significant concern for all institutions, but too often the public sector lacks sufficiently rigorous business continuity management. A business continuity plan may exist, but there can be a lack of senior management engagement that is essential for the plan to work effectively.

Internal audit may consider business continuity management but often only from a disaster recovery perspective. This addresses the restoration of computer systems and attendant applications, data, and connections to full functionality under a variety of damaging or interfering external conditions but can miss wider issues or even mundane occurrences that impact business continuity such as a failed disk, failed server and/or database, loss of communication lines etc. The most important part/activity/process of business continuity management is business impact analysis. Internal audit should carefully study if this has been done during development of the business continuity plan.

There are at least three frameworks that may be used by internal audit to plan and execute effective business continuity management audit engagement:

- ISO 22301 – Business Continuity Management Systems
- Business Continuity Management Audit/Assurance Program – ISACA
- GTAG 10 Business Continuity Management - IIA

According to ISO 22301, the business continuity management system is part of the overall management system that establishes, implements, operates, monitors, reviews, maintains, and improves business continuity. For ISO 22301 auditing of business continuity is more focused on management (and less about technologies) and hence is not a typical IT audit.

IIA defines business continuity management as an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity of services through personnel training, plan testing, and maintenance.

Important terms for business continuity management audit

Business continuity: capability to recover critical business processes.

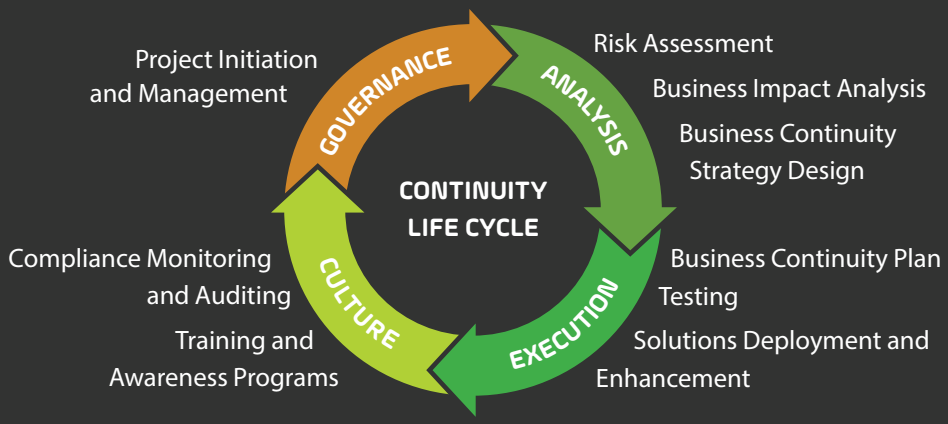
Business continuity plan: documented procedures that guide organizations/institutions to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

Business impact analysis: process of analyzing activities and the effect that a business disruption might have upon them.

Emergency response: first actions that focus on avoiding, deterring, and preventing disasters and/or preparing the organization to respond to a disaster. The goal is lifesaving, safety, and initial efforts to limit the impact to asset damage.

Crisis management: managing external/internal communications and senior management activities during a disaster. The goal is to effectively coordinate the response, resources, and internal and external communication.

Figure 14. The business continuity life cycle



The business continuity management life cycle consists of 4 main areas: governance, analysis, execution, and culture. All parts are important.

For internal audit it is important to understand if the mentioned culture is in place, if the institution's employees really understand and feel themselves as part of that culture, and if the institution's senior management really encourage this culture.

The business continuity management audit should ensure the institution has a swift emergency response to save human lives; proper crisis response capabilities, and access to the resources, services, and activities required to ensure the continuity of critical business functions.

Figure 15. An indicative timeline of business continuity actions

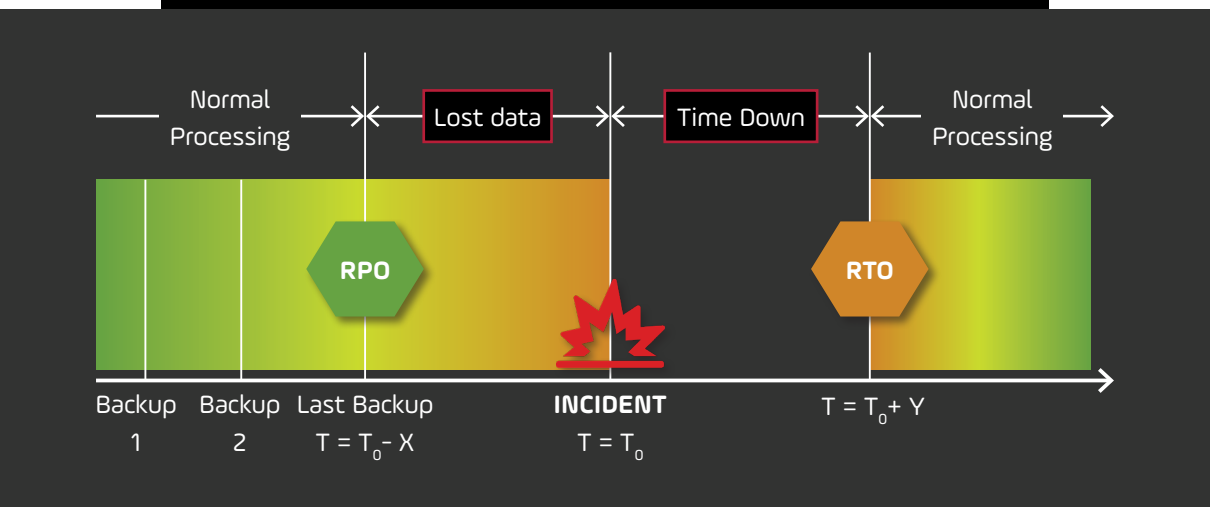
Internal audit should ensure that proper business impact analysis has been done and recovery time objectives (RTO) and recovery point objectives (RPO) (see Figure 15) of each critical business process have been defined during the **Analysis** stage (see Figure 14).

Here ISO 22301 and IIA have similar definitions.

Table 4. ISO 22301 and IIA comparison

	RTO - recovery time objective	RPO - recovery point objective
ISO 22301	Period of time following an incident within which: • product or service must be resumed • activity must be resumed • resources must be recovered	Point to which information used by an activity must be restored to enable the activity to operate (*"maximum data loss"*).
IIA	Processing Gap: Lag time between the disruption point and resumption of normal processing.	The data that will be lost, destroyed, or otherwise unavailable, after successful recovery

Figure 16. Illustration of RPO and RTO



During the business continuity management audit, the following questions should be addressed:

- Does the organization's leadership understand the current business continuity risk level and the potential impacts of likely degrees of loss?
- Can the organization prove the business continuity risks are mitigated to an approved acceptable level?
- If an unacceptable business continuity risk exists but executive management has decided to assume the risk, are the relevant high level officials aware that management has decided not to mitigate the risk?
- Has the decision to accept the risk been properly documented?

Auditing IT Governance

Performing IT governance audit on a periodic basis is vitally important due to the tremendous amount of investment by institutions in IT and information security. IIA Implementation Standard 2110 – *Governance; A.2 Assessing information technology governance* states that "the internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives."[15] Internal auditors following the IPPF should conform with Implementation Standard 2110.A2 by performing IT governance audit.

GTAG® 17 - Auditing IT Governance[16] offers guidance to assist internal auditors in providing assurance services over IT governance. It provides a high-level description of IT governance processes, practices, and terminology to help internal auditors understand the concept of governance and recognize the characteristics of good governance processes.

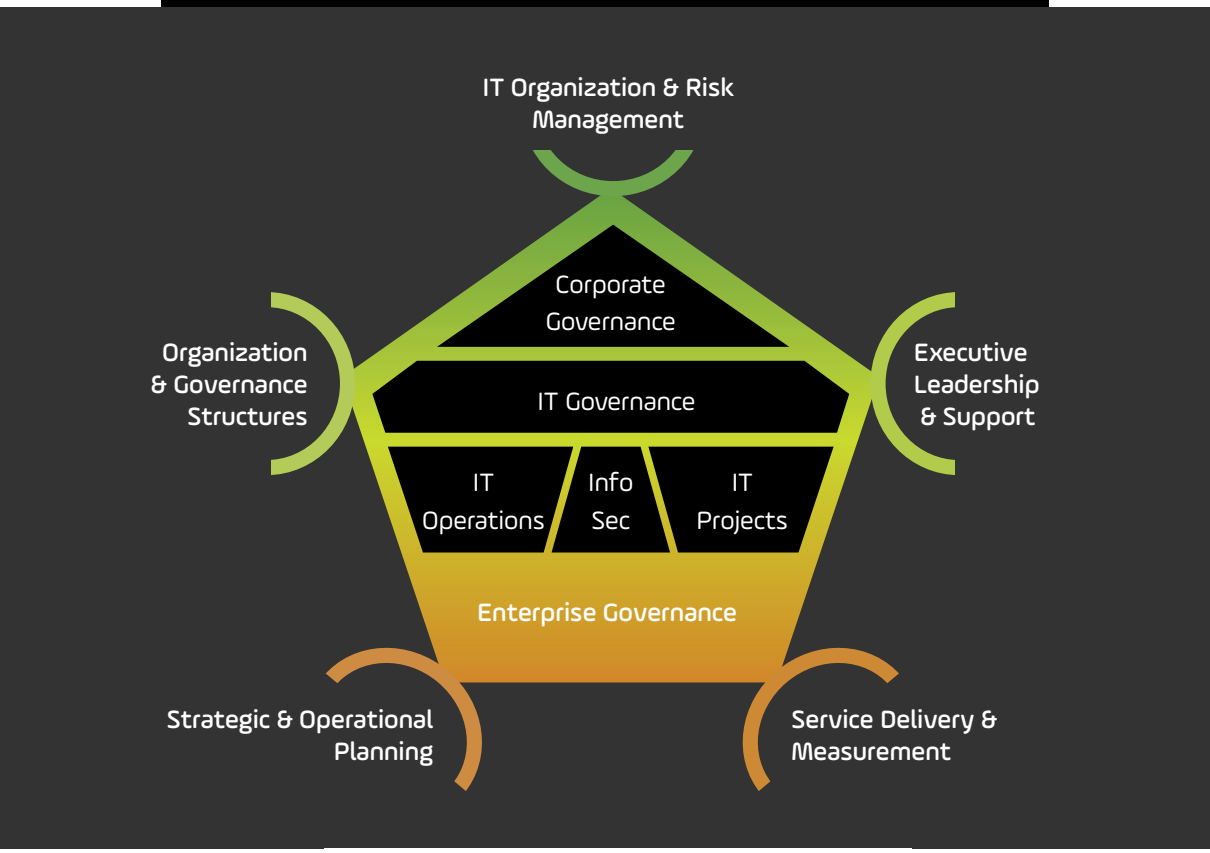
Figure 17 illustrates the five main components that comprise IT Governance:

- Organization & Governance Structures
- Executive Leadership & Support

[15] https://na.theiia.org/standards-guidance/topics/pages/governance-risk-and-control.aspx

[16] https://na.theiia.org/standards-guidance/Member%20Documents/GTAG-17-Auditing-IT-Governance.pdf

Figure 17. The five components of IT governance



- Strategic & Operational Planning
- IT Organization & Risk Management
- Service Delivery & Measurement

Although IT governance audit is a very specific type of audit, it is more about governance and less about technology and does not necessarily require specific and deep IT knowledge. Every experienced internal auditor should be able to provide IT governance audit. Of the five main components, only "Service Delivery & Measurement" may require some IT knowledge.

When auditing IT governance, the following questions should be addressed:

ORGANIZATION AND GOVERNANCE STRUCTURES

- Are roles and responsibilities clearly defined and communicated, and are organization leaders empowered and held accountable for results?
- Is there a CIO in place, and is he/she a member of the senior management team?
- Is the structure of the organization such that the IT function can efficiently and effectively help enable the achievement of the organization's objectives?
- What decision bodies are in place to enable alignment of organization needs with IT services and do they have adequate empowerment and accountability?
- Are organizational needs and IT service requirements defined in strategic and tactical plans and monitored? Do the CIO and senior management meet and discuss progress on plans regularly?

EXECUTIVE LEADERSHIP AND SUPPORT

- Does senior management have clearly defined and communicated roles and responsibilities for the IT function with respect to the organizational achievement of strategic and tactical goals?
- Are the roles and responsibilities of the CIO clearly defined and communicated?
- Is the CIO a member of the senior management team? Does the CIO meet with the board and the senior management team on a regular basis to discuss IT service delivery related to strategic and tactical plans?
- Does IT have adequate funding to meet the organization's needs?

STRATEGIC AND OPERATIONAL PLANNING

- Do the board and senior management view IT as a strategic organizational partner?
- Does the strategic plan of the organization include how IT is required to support and enable value creation?
- Is the strategic plan supported by individual tactical operating plans that take into account IT requirements and deliverables?
- Are key performance indicators used by senior management to measure and monitor the effectiveness of the IT function?

- Are strategic IT investment decisions based on accurate cost benefit analyses and evaluated after implementation to determine whether the projected return on investment has been realized?
- Are lessons learned factored into future IT investment decisions?

SERVICE DELIVERY AND MEASUREMENT

- Do the board and senior management have a clear understanding of IT costs and how they contribute to achievement of the organization's strategic objectives?
- Do leaders of the organization measure IT value and deliverables? How?
- How do IT costs compare to other comparable organizations?
- Is CIO performance measured by financial and nonfinancial data?
- What sourcing arrangements are in place, and how are these measured and monitored?

IT ORGANIZATION AND RISK MANAGEMENT

- To what degree are organizational processes automated?
- How complex is the IT infrastructure and how many applications are in use?
- Are there standard IT hardware, software, and service procurement policies, procedures, and controls in place?
- How mature are IT management processes and are recognized frameworks used (*COBIT, ITIL, ISO 20000, ISO27001*, etc.)?
- How are risks managed in relation to meeting organization needs, security, and compliance requirements?

Responses to these key questions provide the internal auditor with a foundation on which to build and to understand how best to scope and execute an IT governance audit.

Network Audit

Network is the most important component of any institution in today's digital world and senior management require proper assurance that the institution's business processes are able to be effectively supported by:

- Network availability
- Network performance (service quality of the network)
- Network security

Network audit refers to the process of gathering, analyzing, and studying network data, with the purpose of assessing the network's health.

IMPORTANT STEPS TO BE TAKEN

Step 1: Study and understand the institution's network at policy level. At a minimum, the following policies and documents need to be reviewed:

- Network schematics (physical and logical)
- Network security policy
- Remote access policy
- Configuration management policy
- Change management policy
- User management policy
- Internet access policy
- Email and communications policy
- Bring your own device policy
- Backup and restore policy

Step 2: Interview with CIO and chief information security officer (CISO) of the institution to get broader view how they manage institution's network, what are key risks and/or considerations.

Step 3: Study the latest risk assessment and analysis report and the latest network vulnerability scan report. Ensure, if process is in place for continues vulnerability assessment and analyses and if identified vulnerabilities have been mitigated properly.

Step 4: Identify control objectives and risk-controls and prepare risk-control matrix. At least the following control-objectives should be addressed:

- Network infrastructure, capacity and security supports the IT strategic plans that are closely aligned with the business objectives.
- IT and information security responsibilities have been appropriately defined and communicated.
- Mechanisms have been established to identify and react to internal and external risks.
- Network security controls have been implemented to safeguard institution's IT resources and data.
- Network security devices are appropriately managed.
- IT assets are adequately protected in the network.
- An appropriate change management has been implemented.
- User account access privileges are authorized.
- Authentication and authorization controls exist for access to the operating and significant application systems.

RISK CONTROL MATRIX

A risk-control matrix should be developed, identifying for each risk the controls that could mitigate or eliminate it and how should it be tested.

Table 5. Example Risk-Control Matrix

Risk	Control	Testing procedure
Absent or insufficient IT risk assessment.	Risk identification *(both internal and external)* is documented in a risk management guide.	Confirm that mechanisms have been established to identify and react to risks, both internal and external: • Interview with CIO and CISO • Study risk management guide • Study identified high risk • Study implemented controls

Risk	Control	Testing procedure
Insufficient controls for new user setup and account termination.	User management guide is in place.	• Interview with human resources • Select key staff and check their account setup and termination
Lack of IT administrative policies, procedures, and password configuration standards.	Password policy is in place.	• Interview with network admin • Check and confirm if password complexity requirement has been implemented and followed for all network devices
Insufficient change management process.	Change management process and relevant procedures are in place.	• Interview with CISO, network admin. • Confirm that change management requirements are followed for any change in the network, device configurations, firewall rules, etc.
Unauthorized access to server room.	Access to server room granted only appropriate personnel. Camera system is in place.	• Study recordings to check for any unauthorized access. • Study access logs.

IT auditors need to obtain different evidence to test different controls.

Example 1

Control Description: Only senior admins have root access to network devices

What pieces of evidence should be obtained? How is the sample size determined? What testing steps are necessary to test this control?

The sample size for a root (*administrator*) access control depends on the criticality of system, number of user accounts, number of network devices, etc.

For testing the above control, the following steps would be taken:

- Inquire with IT to gain an understanding of how the security is configured.
- Observe IT generating a system query to obtain the list of users with root permissions.
- Compare the list of senior administrators to the IT organization chart to determine if user access is in line with job responsibilities.
- Inquire with IT Management to determine if the individuals with administrator access are appropriate.
- Analyze event-logs to see if there are any anomalies.

Example 2

Control Description: Automated configuration management tools have been implemented to manage the backup and retention of all network devices. Backup logs are reviewed every time after any configuration change and documented in the "Configuration Backup Log" check sheet.

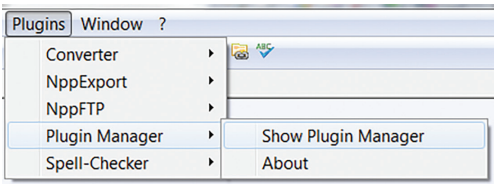
What pieces of evidence should be obtained? How is the sample size determined? What testing steps are necessary to test this control?

The sample size for configuration change management control is based on the entire population of changes, criticality of network devices, number of network devices etc.

For testing the above control, the following steps would be taken:

- Obtain backup schedule from the automated tool from the network administrator.
- Randomly select a sample of days.
- From sample, obtain history file and determine that jobs were run according to policy.
- Obtain configuration backup log check sheet and determine that jobs were run according to backup schedule.
- If jobs were not run according to policy, determine that they were investigated and resolved.

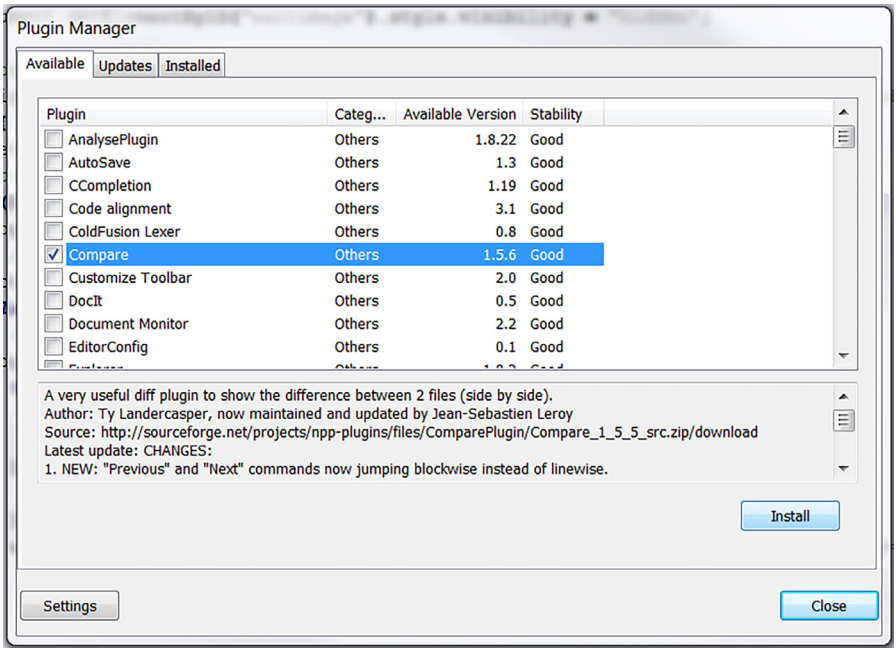
PRACTICAL EXAMPLE OF COMPARING CONFIGURATION FILES



During the configuration management control testing, or for other purposes, IT auditors may use Notepad++. Notepad++ is a free source code editor and Notepad replacement that supports several languages and runs in the MS Windows environment.[17]

Notepad++ has a useful plugin to compare the contents of two files (*for example the actual configuration firewall and the backup of configuration*).

1. Open the Plugin Manager from the Plugins menu.
2. Select the Plugin "Compare" and click Install.
3. After successful installation, open both files to be compared as two separate tabs in Notepad++.
4. From the Plugins menu select Compare -> Compare.



[17] https://notepad-plus-plus.org/

For example, there are two files: The first file (*Firewall.conf*) is the current configuration of the main firewall, and the second file (*Firewall.conf_Backup*) is the backup of the configuration, which network admin may need to use to restore from the backup. The objective is to test and ensure that the backup of the firewall configuration is up to date and contains all changes, so that in case of restoration the firewall can operate properly.

Figure 18. Extract from Notepad++

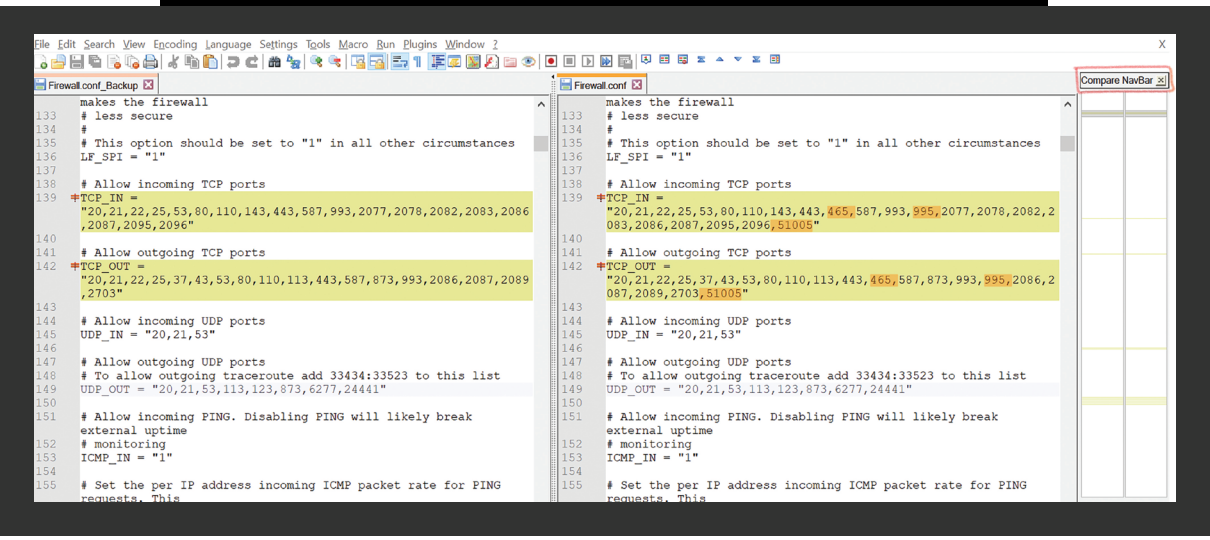
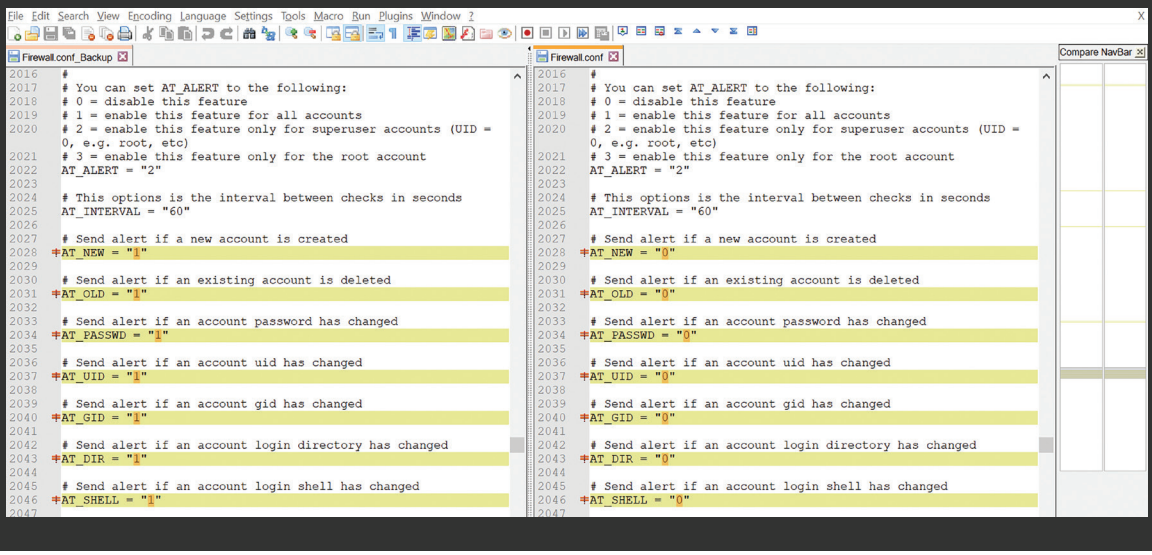


Figure 18 shows a screenshot of the file comparison where "Compare NavBar" (in the red box top-right) indicates that there are some changes in the compared files on different lines.

The first difference highlighted is line 139. This relates to line 138 "Allow incoming TCP ports". Some ports (465, 995 and 51005; highlighted by Notepad++ in orange) are allowed in the current Firewall.conf (right side), which are not allowed in Firewall. conf_Backup (left side). This is an interesting finding and the IT auditor needs to understand how, why, and who allowed these ports. It could be an unauthorized change in the firewall configuration.

A further screenshot (Figure 19) displays the last block of changes. As seen in the file comments, this block is about setting different alerts. If the set parameter is 1, then it is enabled for all accounts, if the set parameter is 0, then the feature is disabled.

Figure 19. Extract from Notepad++



Line 2028 in the backup config has an alert for new account creation set to 1, meaning enabled. However, in the actual config it is set to 0, which means alerts will not be sent when a new user is created. This is repeated for lines 2031, 2034, 2037, 2040, 2043, and 2046, alerts will not be sent according to the current config, while in the backup file all alerts are enabled.

The IT auditor should use this information to carefully analyze the situation, understand the root-causes, and document all the evidence.

TOOLS FOR NETWORK AUDIT

Other tools that may be useful during the network audit include:

1. **Spiceworks Inventory** - Network inventory tool that automatically discovers network devices.

2. **Network Inventory Advisor** - Inventory scanning tool compatible with Windows, Mac OS, and Linux devices.

3. **Nessus** - Free vulnerability assessment tool with over 450 configuration templates and customizable reports.

4. **ManageEngine Vulnerability Manager** - This package of system security checks sweeps the network and checks for security weaknesses. Runs on Windows and Windows Server.

5. **Netwrix Auditor** - Network security auditing software with configuration monitoring and automated alerts.
6. **Nmap (*Zenmap GUI*)** - Open-source port scanner and network mapper available as a command-line interface.
7. **OpenVAS** - Vulnerability assessment tool for Linux users with regular updates.
8. **Metasploit** - Penetration testing tool that identifies weaknesses in your network.

Of these seven tools most are easy to use and do not require specific or deep IT knowledge, only the final one **Metasploit** is more a complex tool and needs experience and specific knowledge to use it.

PART 6

REPORT WRITING: RECORDING TECHNICAL ISSUES IN BUSINESS LANGUAGE

Writing a good report is vital to ensure public sector IT audit findings and recommendations are understood. Most readers are unlikely to have any IT background (and will maybe lack understanding of IT risks) so the report must be clear, accessible, and well explained.

The report should be focused on helping the institution's management understand the critical issues and make appropriate decisions by:

1. Providing an opinion on the IT risk management arrangements in respect of the area reviewed and
2. Recommending improvements, where appropriate.

While writing an IT audit report, you should remember that you are the strategic partner of your institution's top management, and you should help them to have a better IT strategy, IT risk management, and IT control environment.

The IPPF and ITAF both set out what should be included in the IT audit report. The ISACA article, "*IS Audit Basics: The Components of the IT Audit Report*"[18] is also very useful on this.

[18] https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/is-audit-basics-the-components-of-the-it-audit-report

The IT audit report should follow general internal audit standards and it is important to know not only how to write a good IT audit report but also how to talk about technical issues and how to bring change in the institution.

Factors to consider when writing the IT audit report include:

- Know the target audience (management, senior executives, or the audit committee) and write the report for them. Auditees may like long, detailed reports, but audit committee members may prefer them concise and focused.
- Will the report be presented in person and, if so, how much time is available for the presentation?
- Consider the content. If you were the recipient of the report, would it spur you into action?
- Does your report focus on the future rather than the past?
- Do the findings, conclusions, and recommendations really represent the key issues?
- Are all your recommendations practical enough to implement?

> If external audit usually looks back to verify the current state, internal audit should look at the current control environment to predict future risks and help senior management to be prepared to deal with them.

The report structure, style and presentation are the key components of any IT audit report. Nearly all audit reports require some change. The report will highlight a problem and recommend action which should be taken to change things. To achieve results, you will need to be a mixture of a salesperson, judge and diplomat.

The magic tip of any report is: **Keep it simple!**

Any IA report should be accurate & objective:

- Based on sufficient audit evidence, free from errors, distortions, fact-based.
- Credible, impartial, based on relevant facts and circumstances, as well as on balanced assessments.

It should also be clear & concise:

- Clear connection between obtained evidence and conclusions, based on criteria-condition-cause-effect approach.
- Clear links to other relevant documents.

- Present the essence of the problem without long sentences, repetition of words, unnecessary details, and mysterious terms and jargon.
- Whenever it's possible use tables, charts and other visual tools.
- Exaggerated prose, overuse of adjectives, and flamboyancy should be avoided.

The IT audit report should be:

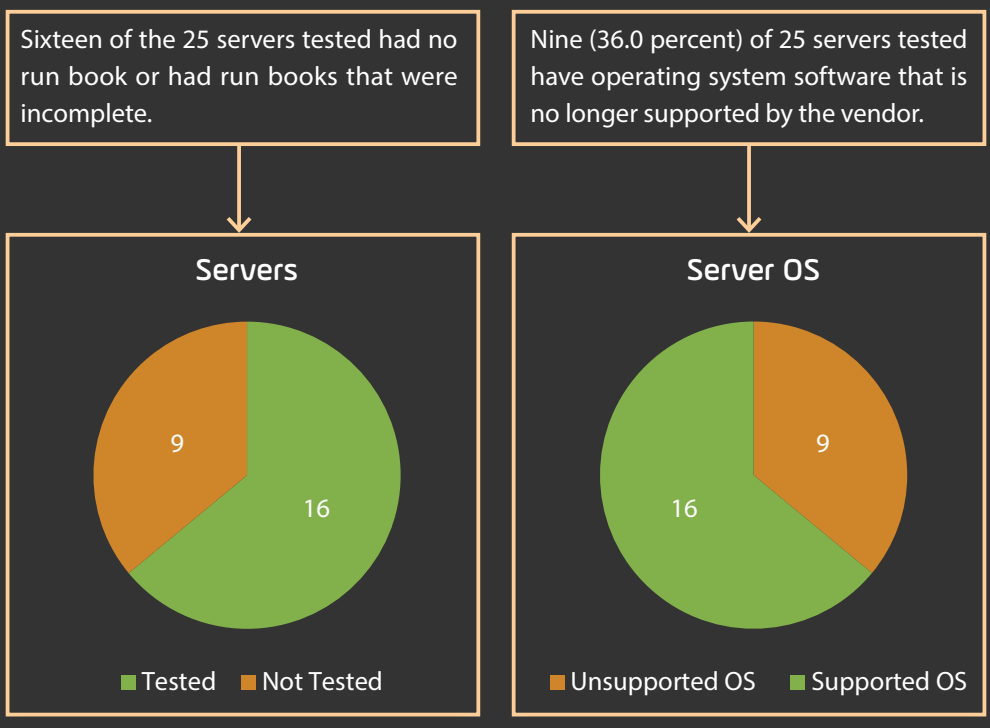
Constructive

- Useful for the auditee.
- Contain positive findings.
- Able to contribute to the necessary changes.

Complete

- Include all information relevant to the target users.
- Contain the necessary and sufficient information to substantiate conclusions and recommendations.

Figure 20. Example of using charts instead of long sentences



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Economic Affairs SECO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

MINISTRY OF FINANCE
OF THE RUSSIAN FEDERATION

European Union