14th Scientific Research Competition of the Arab Organization of Supreme Audit Institutions

On the Topic of:

Audit of information systems and cybersecurity

– Case study on the audit of information systems and cybersecurity of the National Electricity and Gas company -

Prepared by :

MAHMOUDI Mhamed

Director of studies

Court of Counts

-2024-

ABSTRACT:

The audit of information systems and cybersecurity is a vital and contemporary topic in the field of IT auditing, as its importance continues to grow with the increasing cyber threats and the growing reliance on technology in the public sector. This study aims to shed light on the role of Supreme Audit Institutions (SAIs) in evaluating information systems and cybersecurity, with a focus on audit challenges, its importance in strengthening governance and transparency, in addition to best practices, standards, and audit methodologies.

An inductive analytical approach was adopted in this study, presenting a theoretical framework for evaluating information systems and cybersecurity, while reviewing the challenges faced by audit institutions in this field. On the practical side, the study focused on assessing the information systems and cybersecurity of Sonelgaz Distribution Company, defining the objectives, scope, and adopted methodology, utilizing a risk-based assessment approach, collecting evidence, conducting the audit, and analyzing the results. The findings were reviewed with the audited entity, and the audit report was made available to the audit team and the relevant department.

The study resulted in important findings, including:

- - A comprehensive understanding of the fundamental concepts of information systems and cybersecurity auditing and defining the main objectives of IT auditing.
- - Highlighting Algeria's efforts in strengthening cybersecurity governance and developing cybersecurity strategies.
- - The role of IT auditing in protecting against complex and evolving cyber threats, ensuring regulatory compliance, and reducing cybersecurity risks.
- - The role of Supreme Audit Institutions in enhancing information systems oversight in the context of digital transformation, and the necessity of international cooperation, establishing specialized units, training personnel, and adopting best practices and international standards.

In summary, securing information systems and ensuring cybersecurity is a complex process that requires close cooperation between Supreme Audit Institutions, government entities, and the private sector. Effective coordination among these entities is essential to ensure the implementation of best security practices and policies and to develop integrated strategies to address cyber threats. Enhancing the audit of information systems and cybersecurity not only

contributes to achieving transparency and efficiency but also strengthens public trust in institutions, ensures business continuity, and protects sensitive data from cyberattacks. Through this collaboration, a strong governmental and economic system based on data can be built, supporting innovation and promoting economic growth, which ultimately leads to improved public services and achieving the common good with high effectiveness and efficiency.

Keywords: Information systems audit, cybersecurity, Supreme Audit Institutions, risk-based approach, Sonelgaz Distribution Company.

Table des matières

Introduction:

In the wake of the accelerating pace of digital transformation worldwide, information technology infrastructures face increasing security challenges, making cybersecurity a pressing necessity to ensure data safety and privacy. In this context, the need to enhance information systems auditing emerges not only as a defensive measure but also as an integral part of a comprehensive security strategy for institutions and government bodies.

Supreme Audit Institutions (SAIs) play a pivotal role in this process, providing essential oversight and guidance to improve security measures and ensure compliance with international standards and best practices in cybersecurity. Their mission extends beyond evaluating existing policies and procedures; they also contribute to developing effective strategies that enhance early threat detection and response.

Cybersecurity auditing represents one of the fundamental tools used by these institutions to achieve security objectives. Through meticulous and continuous assessment of systems and controls, the effectiveness of implemented security measures and their compliance with standards are verified. This evaluation includes analyzing security vulnerabilities and providing recommendations to enhance security and mitigate risks.

Strengthening information security requires an integrated approach that includes updating policies, developing human competencies, and facilitating systematic risk auditing initiatives. This research aims to explore how enhanced information systems auditing contributes to achieving a higher level of cybersecurity, thereby improving institutions' ability to efficiently and effectively address contemporary security challenges.

In Algeria, entities specialized in information technology and cybersecurity play a key role in supporting these efforts by developing various tools and mechanisms and assessing their impact on achieving higher cybersecurity levels. The Algerian Court of Accounts, as one of the supreme audit institutions, seeks to implement initiatives that align with the national integrated policy aimed at strengthening information systems auditing capabilities and effectively addressing security challenges.

1. Research problem:

With global digital transformation, information technology infrastructures face increasing security challenges, making cybersecurity a critical necessity to ensure data safety and privacy. Supreme Audit Institutions play a pivotal role in this context by assessing and monitoring existing security measures and their compliance with international information security standards and local regulations. Despite the importance of cybersecurity auditing as a key tool for achieving security, public institutions face significant challenges due to technical complexities and ongoing developments in the cyber domain. Based on this, the following research problem is posed:

Can Supreme Audit Institutions enhance their efficiency in cybersecurity auditing to address ongoing challenges in the modern IT environment and contribute to the implementation of the national information security and cybersecurity strategy?

2. Sub-questions :

- What are the fundamental concepts of information systems auditing and cybersecurity, and what is their importance in addressing current challenges?
- What challenges do Supreme Audit Institutions face in auditing information systems and cybersecurity, and what role can they play in overcoming these challenges?
- What are the key steps and practical methodologies that can be followed in evaluating information systems and cybersecurity?

3. Research importance:

Information systems auditing and cybersecurity hold significant importance in today's digital age, forming the foundation for ensuring the safety of sensitive data and information in institutions and public bodies. This research aims to enhance the scientific understanding of information systems auditing and cybersecurity concepts and provide practical guidelines for improving auditing and control performance in this field. The study also seeks to explore how supreme audit institutions can strengthen information security and data protection while ensuring the effective use of modern tools and technologies to achieve impactful auditing results.

Additionally, the research highlights the necessity of adhering to international standards and best practices in information systems auditing and cybersecurity. This contributes to building trust in digital technology usage and achieving information systems auditing and cybersecurity objectives efficiently and effectively.

4. Research objectives:

This research aims to achieve the following objectives:

- Provide a comprehensive theoretical framework explaining the concepts of information systems auditing and cybersecurity and their practical applications.
- Analyze the foundations and objectives of information systems auditing and cybersecurity in the modern digital age.
- Examine the challenges and obstacles facing information systems and cybersecurity auditing in the digital era.
- Conduct an analytical study of the efforts of supreme audit institutions in enhancing information security and data protection.
- Provide practical recommendations for improving auditing and control performance in cybersecurity.
- Emphasize the importance of adhering to international standards and best practices in information systems auditing and cybersecurity.
- Conduct a case study or analyze the results of implementing modern tools and techniques to enhance auditing and cybersecurity.

5. Research hypotheses:

Based on the research problem and objectives, the following hypotheses are proposed:

- **Main hypothesis :**
    - The adoption of information systems and cybersecurity auditing methods and tools by audit institutions contributes to enhancing cybersecurity.
- **Sub-hypotheses :**
    - **First Sub-Hypothesis:** If Supreme Audit Institutions understand and apply fundamental concepts of information systems auditing and

cybersecurity, they will be better equipped to address current challenges effectively.

- **Second Sub-Hypothesis:** If Supreme Audit Institutions adopt key steps and effective practical methodologies in evaluating information systems and cybersecurity, this will enhance audit efficiency and achieve control objectives effectively and efficiently.
- **Third Sub-Hypothesis:** If Supreme Audit Institutions improve procedures and policies related to information systems and cybersecurity auditing, they will contribute to building a secure and reliable government system that aligns with international standards and enhances national cybersecurity.
- **Fourth Sub-Hypothesis:** If coordination and cooperation among different audit institutions are enhanced, their ability to combat cyber threats will be significantly improved.

6. Research methodology:

The study adopts an inductive analytical approach, which is well-suited to the nature of the research. It includes a theoretical framework for evaluating information systems and cybersecurity, reviewing the challenges faced by audit institutions in this field, and analyzing their key roles. The study also explores the concept of cybersecurity governance and examines Algeria's efforts in this domain.

On the practical side, the study focuses on assessing the information systems and cybersecurity of Sonelgaz Distribution Company. It defines the objectives, scope, and adopted auditing methodology, explaining the steps from the planning and preparation phase to the execution phase, utilizing a risk-based assessment approach, evidence collection, audit execution, and result determination. The findings were reviewed with the audited organization, and the audit file was made available to the audit team and the relevant audit chamber.

7. Study Structure:

To achieve the research objectives, and based on the above, the study is divided into theoretical and practical aspects as follows:

8. Theoretical aspect:

- **Chapter One:** General and theoretical framework for evaluating information systems and cybersecurity.
    - **Section One:** Information systems auditing.
    - **Section Two:** Cybersecurity.
    - **Section Three:** Cybersecurity auditing.

9. Practical Aspect:

- **Practical and analytical side of the audit mission:** Evaluation of Sonelgaz Distribution Company's information systems and cybersecurity.

Chapter One: Theoretical framework for evaluating information systems and cybersecurity by supreme audit institutions

Introduction

In the modern digital age, organizations increasingly rely on technology, exposing them to rising cybersecurity threats. This dependence can have severe financial and reputational consequences due to security vulnerabilities. The ease of communication and access to information amplifies these risks, surpassing traditional control mechanisms. Cybersecurity encompasses technologies and practices aimed at protecting information assets from unauthorized access. As cyber threats continue to rise, managing cybersecurity risks has become essential to safeguarding data and ensuring organizational stability.

This chapter aims to provide a theoretical framework for understanding the significance of evaluating information systems and cybersecurity by Supreme Audit Institutions (SAIs). It will cover key concepts of information systems auditing, the objectives and importance of IT auditing, as well as the challenges faced by SAIs in enhancing information security. The chapter will also highlight cybersecurity governance standards, steps toward cybersecurity maturity, Algeria's efforts in this domain, and the methodology for conducting cybersecurity audits effectively.

Section One: Information systems auditing

With the exponential growth of the digital landscape, integrating advanced technologies into the operational framework of the public sector has become a strategic necessity. This digital transformation presents public institutions with new challenges related to complex IT systems. To ensure their efficiency and effectiveness, it is essential to reevaluate mechanisms that enhance their performance. Information systems auditing plays a critical role in protecting sensitive data and ensuring the continuity of government operations effectively, contributing to transparency, accountability, and improved public sector performance.

I. Fundamental concepts of information systems auditing and its importance

Definition of IT Auditing and Information Systems Control

IT audits are an examination of aspects of an organisation's use of IT, including IT infrastructure, policies and procedures, applications, and use of data. IT audits regularly incorporate analysis of systems and controls to ensure that they meet the organisation's business needs without compromising security, privacy, cost, and other critical business elements. IT audits also often involve deriving assurance on whether the development, implementation, and maintenance of IT systems

meets business goals, safeguards information assets, and maintains data integrity. IT audits often involve the identification of instances of deviation from criteria, which have in turn been identified based on the type of audit engagement (e.g., a performance, financial, or compliance audit).[1]

Information technology control can be defined as a set of specific regulatory procedures aimed at ensuring the correct operation and reporting of data so that it can be relied upon.[2]

It is also described as the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that organizational objectives will be met while preventing or detecting and correcting undesirable outcomes.[3]

Furthermore, IT control is defined as methods ensuring that only complete, accurate, and authenticated data is entered and updated in the electronic system.[4] The processing must be executed correctly, and the results must meet expected outcomes while ensuring data integrity.[5]

The Comptroller and Auditor General of India (CAG) defines IT auditing as "the process of gathering and evaluating evidence to determine whether a computer system protects assets, maintains data integrity, enables organizational goals to be achieved effectively, and uses resources efficiently."[6]

IT auditing includes a wide range of audit types, such as financial audits (assessing the accuracy of an organization's financial data), operational audits (evaluating internal control structures), information systems audits (including performance audits), specialized audits (assessing third-party services like outsourcing), and forensic audits. Despite their differences, all these audits share a common objective: assessing the reliability of an organization's IT systems. IT audits also incorporate technology-driven audits that utilize computer-assisted data analysis tools.[7]

---

[1] WGITA – IDI handbook on it audit for supreme audit institutions intosai development initiative, 2022 , P 07

[2] Khodair, Mostafa. *Review of Concepts, Standards, and Procedures.* King Saud University, Riyadh, 1991, p.279.

[3] Dahmash, Naeem & Abu Zar, Afaf Ishaq. *Control Mechanisms and Internal Auditing in IT Environments.* Fifth Annual International Scientific Conference, Faculty of Management and Economic Sciences, Al-Zaytoonah University of Jordan, *Knowledge Economy and Economic Development*, Amman, Jordan, 2005, p. 12.

[4] Mosleh, Nasser Abdulaziz. *The Impact of Computer Usage on Internal Control Systems in Banks Operating in the Gaza Strip*. Master's Thesis, Islamic University, Faculty of Commerce, Gaza, 2007, p. 71.

[5] Al-Himyari, Bashir; Al-Qawi, Mohammed; Al-Shammari, Abdelkader. *The Use of IT and Data Auditing with COBIT.* Central Organization for Control and Auditing, Yemen, 2011, p. 6.

[6] Saeed, Howaida Al-Noor. *IT Auditing.* National Audit Office, Sudan, 2011, p. 5.

[7] Comptroller and Auditor General of India. https://cag.gov.in/

The African Organization of Supreme Audit Institutions (AFROSAI) defines IT auditing as the process of ensuring that the development, implementation, support, and maintenance of information systems meet business objectives, protect information assets, and maintain data integrity. In simpler terms, technical auditing examines IT systems and their controls to ensure that they meet business needs without compromising security, privacy, costs, or critical business elements.[8]

In summary, IT auditing is the process of evaluating an organization's technical operations and information to verify that they are effectively and securely used to achieve business objectives. This includes reviewing IT system development, implementation, and maintenance while ensuring compliance with business needs without compromising security, privacy, cost efficiency, or other essential operational factors.

II. The importance of IT auditing

Ensuring the security and safety of an organization's IT environment is a top priority. IT audits help identify vulnerabilities and develop appropriate corrective strategies. These audits ensure compliance with industry standards and regulations, helping organizations avoid penalties and fines resulting from non-compliance.

Additionally, comprehensive IT audits can uncover operational and technological efficiencies, leading to performance improvements and cost savings. For publicly traded companies, conducting audits is also a legal requirement to maintain transparency and investor confidence. Overall, IT audits are essential for ensuring compliance, enhancing security, and driving operational improvements.[9]

- **The role of IT auditing in innovation**

IT auditing plays a crucial role in supporting innovation efforts by assessing an organization's ability to manage risks associated with innovation. Auditors can evaluate the robustness of project management processes and the effectiveness of change management practices, enabling innovation while mitigating risks effectively. By leveraging data analysis techniques and automation, IT auditing

[7] AFROSAI-E INFORMATION TECHNOLOGY AUDIT GUIDELINE – 2017, P5
[8] https://www.auditboard.com/
[9] https://thecodest.co/blog/it-audits-and-cybersecurity/

can enhance its efficiency and effectiveness in assessing digital systems and processes[10].

Furthermore, IT auditing provides valuable insights to management by identifying areas for improvement in digital initiatives.[11] It also plays a proactive role in supporting organizations' digital transformation journeys by offering advisory services and strategic guidance[12]. By staying up to date with emerging technologies and industry trends, IT auditors can help institutions capitalize on opportunities and address challenges related to digital transformation.[13]

- **Integration of IT Auditing with Business Continuity Planning**

IT auditing plays a critical role in ensuring business continuity by assessing the resilience of IT systems and verifying the adequacy of backup and recovery processes. This is achieved through reviewing the results of tabletop exercises and simulations to determine the effectiveness of the business continuity plan in real-world scenarios, focusing on vulnerabilities and areas requiring improvement.

Auditors gather feedback from employees and stakeholders to understand the ease of implementation and effectiveness of the plan, identifying potential challenges. They also assess the plan's alignment with the organization's recovery objectives, ensuring that essential operations, systems, and resources are adequately covered. Furthermore, auditors ensure that the plan remains aligned with evolving business requirements by updating it to reflect changes in technology, processes, and business strategies[14].

Additionally, IT auditing is essential for business continuity planning, particularly for startups operating in cloud computing. IT audits contribute to ensuring the resilience and sustainability of these companies by developing and testing effective plans that help mitigate the impact of disruptive events on critical business functions and IT infrastructure. These plans also help maintain customer trust and compliance with regulations, ultimately enhancing overall business competitiveness.[15]

[10] Deloitte A. 2021. IT audit in the era of digital transformation: How to adapt and thrive. Deloitte Insights.
[11] PwC. 2018. Digital transformation. PwC.
[12] EY, Ajak. 2020. Navigating the risk and regulatory landscape: Technology and digital transformation. EY Insights.
[13] Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.
[14] https://audit.guru/disaster-recovery-and-business-continuity-in-it-audits/#:~
[15] Sathyanarayanan, Kishan. "Disaster Recovery and Business Continuity Preparedness for Cloud-based Start-ups." ISACA Now Blog, 2023

- **The importance of IT auditing in mergers and acquisitions (M&A)**

IT auditing is crucial in mergers and acquisitions (M&A), where two or more companies integrate, often involving the transfer of sensitive information and assets. Cybersecurity auditing assesses risks and vulnerabilities in the cybersecurity posture of the acquired company or investment as part of an M&A transaction.

Companies must conduct cybersecurity audits for several reasons, including protecting against financial losses, ensuring regulatory compliance, safeguarding sensitive information, improving overall security posture, maintaining customer trust, and preventing reputational damage.

The implementation of a cybersecurity audit in M&A involves developing an audit checklist, reviewing security policies and procedures, evaluating the incident response plan, and assessing security technologies and network architecture. By following these steps, companies can enhance their security stance and reduce potential risks associated with cyber threats [16].

- **Enabling IT governance through auditing**

IT governance enablement through auditing refers to the process of enhancing and improving the efficiency and effectiveness of IT governance within organizations. This involves conducting a comprehensive evaluation of current IT governance practices, policies, and procedures to ensure their alignment with organizational objectives and international and local security standards. It also includes assessing the effectiveness and efficiency of technology use in supporting business goals and ensuring compliance with relevant regulations and legal frameworks.

Enabling IT governance through auditing is a critical process for achieving security objectives, regulatory compliance, and competitive sustainability in the era of advanced information technology[17].

- **Ensuring data privacy and protection through IT auditing**

Data protection is a top priority for organizations. IT auditing evaluates the effectiveness of data protection measures and compliance with regulations such as GDPR, contributing to a culture of data awareness within the organization.

Data privacy and information security are among the most pressing concerns for companies. Ensuring the security of data using efficient and cost-effective

[16] https://atlantsecurity.com/cybersecurity-audits-are-necessary-in-the-due-diligence-of-ma-deals/
[17] Auditing IT Governance – Pempal www.pempal.org

methods remains a constant challenge due to the growing complexity of cybersecurity threats and the increasing number of data protection regulations.

As a result, organizations face continuous pressure to secure their IT systems and protect customer data privacy. IT auditing is one of the most effective approaches to achieving these goals, helping organizations assess the effectiveness of their controls and identify potential areas of risk and vulnerability.

IT auditing serves multiple purposes, including:

- Assisting organizations in identifying system or process vulnerabilities.
- Evaluating compliance with relevant regulations and standards.
- Providing a foundation for recommendations and corrective action plans to enhance security measures[18].

- **Evaluating cloud security through it auditing**

With the increasing reliance on cloud computing, IT auditing must adopt a proactive approach toward cloud initiatives. This can be achieved by guiding management as a trusted advisor, participating in early procurement processes to validate business use cases, ensuring the inclusion of audit rights clauses in contracts, and providing objective insights.

IT auditing also helps organizations identify and mitigate risks, offering guidance on the impact of regulations on cloud data security. Additionally, IT audits provide other assurance services, including data migration audits, system implementation audits, control testing, and reviewing Service Organization Control (SOC) reports.

To facilitate cloud auditing, organizations can use available tools such as the Cloud Security Alliance Control Matrix, the Consensus Assessment Initiative Questionnaire (CAIQ), or compliance software solutions to assess the necessary controls for risk mitigation. By leveraging these tools, organizations can proactively focus on their control environment rather than reacting to security issues[19].

- **Impact of IT auditing on digital transformation initiatives**

[18] ISACA. *Managing Data Privacy and Information Security with IT Audits*, 2023. [Available online]: https://www.isaca.org/resources/news-and-trends/industry-news/2023/managing-data-privacy-and-information-security-with-it-audits.
[19] Kim Pham, CIA. *Cloud Computing — What IT Auditors Should Really Know*, ISACA Now Blog, 2022. [Available online]: https://www.isaca.org.

IT auditing provides valuable insights into managing digital transformation initiatives, assisting in assessing transformation strategies, project management capabilities, and change management practices. It ensures that organizations can successfully transition to new digital environments while maintaining compliance, security, and operational efficiency.

- **IT auditing in the context of the internet of things (IoT)**

IT auditing in the context of IoT has become crucial in today's rapidly evolving digital landscape. This type of audit offers an objective and independent evaluation of organizations' technological systems and controls, helping them identify security vulnerabilities, assess compliance with existing regulations and standards, and ensure the effectiveness of adopted controls.

Additionally, IT auditing validates the added value of IoT solutions by assessing the readiness and efficiency of the systems and applications used. IT auditing plays a vital role in ensuring the security and integrity of data within IoT environments by evaluating data transmission security between connected devices, identifying potential risks and weaknesses, and providing recommendations to enhance security controls.

IT auditors must adopt a proactive and meticulous approach when evaluating IoT security, which requires a deep understanding of IoT technologies and the associated challenges[20].

- **Cyber incident response planning through it auditing**

IT auditing assesses an organization's readiness to handle cyber incidents, including the design and effectiveness of incident response plans.

In an era where cyber threats are becoming increasingly complex and widespread, IT auditing has never been more critical. These audits serve as essential tools for securing an organization's IT environment, ensuring regulatory compliance, and mitigating cybersecurity risks.

IT auditing plays a crucial role in evaluating an organization’s preparedness to manage cybersecurity challenges, overseeing vendor management, ensuring high standards in software development, and assessing the security of artificial intelligence technologies. These audits remain fundamental for safeguarding IT environments, regulatory adherence, and reducing the risk of cyberattacks.

Objectives of IT Auditing

The emergence of information technology has transformed the way we work across various fields, including auditing. The widespread use of computers has significantly enhanced operational efficiency. However, this technological advancement has also introduced vulnerabilities closely related to automated business environments. Identifying these new vulnerabilities, minimizing their impact, and implementing appropriate controls require a thorough assessment of internal controls using advanced auditing techniques[21].

The primary objective of IT auditing is to ensure that IT resources enable an organization to achieve its goals effectively while optimizing resource utilization. IT audits may focus on IT applications, processes, governance, enterprise resource planning (ERP) systems, information security, business solution acquisitions, system development, and business continuity. Audits may also assess the added value of IT systems within an organization [22].

Some key objectives of IT auditing include:

- Reviewing IT system controls to ensure adequacy and effectiveness.
- Evaluating the processes involved in specific business functions, such as payroll or financial accounting systems.
- Assessing the performance and security of IT systems, such as railway reservation systems.
- Examining system development processes and related procedures .

According to the Comptroller and Auditor General of India (CAG), IT auditing aims to evaluate processes that ensure asset protection. These assets include [23]:

- **Data**: Covers all types of data, whether internal or external, structured or unstructured, including documents, graphics, and audio files.
- **Application systems**: Comprising both manual and automated processes.
- **Technology**: Including hardware, operating systems, database management systems, networks, and multimedia components.
- **Facilities**: The resources required to host and support IT systems, such as utilities.
- **Personnel**: The skills, awareness, and productivity of employees involved in planning, organizing, acquiring, delivering, supporting, and monitoring IT systems and services (CAG, 2011).

[21] Comptroller and Auditor General of India (CAG), *IT Auditing Standards*, 2011.
[22] AFROSAI-E INFORMATION TECHNOLOGY AUDIT GUIDELINE – 2017, P5
[23] CAG, Official Website, loc. cit.

Additionally, IT auditing aims to ensure compliance with the seven key attributes of data security and management:

- **Effectiveness**: Ensuring that information is relevant to business processes, delivered accurately, consistently, and in a timely manner for usability.
- **Efficiency**: Optimizing the use of resources for maximum productivity and cost-effectiveness.
- **Confidentiality**: Protecting sensitive information from unauthorized access or disclosure.
- **Integrity**: Maintaining the accuracy, completeness, and validity of information in alignment with business expectations.
- **Availability**: Ensuring that information is accessible when required for business operations, thus protecting IT resources.
- **Compliance**: Adhering to applicable laws, regulations, and contractual agreements governing business processes and IT systems.
- **Reliability of Information**: Ensuring that IT systems provide accurate and relevant information for management operations, financial reporting, and regulatory compliance .

Thus, IT auditing is crucial in verifying whether IT processes and resources align effectively to achieve an organization's intended goals while ensuring operational efficiency, compliance, and cost-effectiveness.

III. Challenges and roles of Supreme Audit Institutions (SAIs) in information systems auditing

Supreme Audit Institutions (SAIs) refer to national bodies responsible for ensuring government accountability through external auditing. The mandates, responsibilities, and organizational structures of these institutions vary depending on governance frameworks and national policies. However, a key principle is the independence of SAIs from the government and executive authorities to ensure transparency and integrity[24].

The Arab Organization of Supreme Audit Institutions (ARABOSAI) defines SAIs as "an independent body that conducts all types of auditing in accordance with applicable legislation, with the aim of ensuring the safeguarding of public funds, guaranteeing their efficient and proper use, and reporting on financial accounts and statements to relevant state authorities"[25].

[24] Chatterjee, S. (2018). "Addressing the Challenges of IT Audits by Supreme Audit Institutions." ISACA Journal, Volume 4.

[25] Jabal, Ibrahim. *Auditing Tools Available to Supreme Audit Institutions and Ways to Improve Them.* Cairo: Dar Al-Nahda Al-Arabiya, 2015, p. 86.

1. Challenges in IT auditing by supreme audit institutions

As illustrated in Figure 1, the challenges faced by SAIs in conducting IT audits can be classified into four main categories[26] :

- **Institutional Challenges**: These relate to the lack of sufficient mandate or legislation that enables SAIs to conduct IT audits effectively. Without clear legal authority, SAIs may struggle to access necessary data or enforce their findings.
- **Organizational Challenges**: These involve the internal systems and structures within SAIs that support IT auditing. Many institutions lack the necessary frameworks to integrate IT audits into their broader audit strategies.
- **Professional Staff Challenges**: These pertain to the availability of well-trained personnel with sufficient skills to conduct IT audits. Given the rapid advancements in technology, SAIs must invest in continuous training programs to build capacity in IT auditing.
- **Public Sector Significance**: The increasing digitization of governance and public service delivery necessitates a stronger role for SAIs in ensuring accountability in IT-related processes.

2. The Role of Supreme Audit Institutions (SAIs) in Strengthening Information Systems Auditing

Supreme Audit Institutions (SAIs) play a crucial role in strengthening oversight of information systems. Over the years, the international community of SAIs has made significant efforts to establish robust IT audit functions by addressing various challenges. With technological advancements and digital transformation in government institutions, the need for effective IT auditing has become essential to ensure **transparency, efficiency, and cybersecurity**.

[26] Chatterjee, S. (2018). "Addressing the Challenges of IT Audits by Supreme Audit Institutions." ISACA Journal, Volume 4.

- **SAIs' Mandates for Conducting IT Audits**

The mandate granted to SAIs for conducting IT audits is outlined in the **International Standards of Supreme Audit Institutions (ISSAIs)**, specifically in the **Lima Declaration** [27]. The authority of SAIs to conduct IT audits stems from their general mandate to perform **financial audits, compliance audits, performance audits**, or a combination of these [28]. These powers are typically defined by national constitutions and implemented through relevant legislation.

Some SAIs have **specific mandates** to conduct IT audits. For instance, if an SAI is authorized to audit the tax revenue process, it must also audit the automated aspects of this process based on its primary mandate. This comprehensive approach ensures the effectiveness of both financial and technological audits, thereby enhancing **transparency and accountability** in government operations[29].

- **Peer Support and Knowledge Exchange Among Supreme Audit Institutions (SAIs)**

Through the efforts of the International Organization of Supreme Audit Institutions (INTOSAI), the Working Group on IT Audit (WGITA), and the INTOSAI Development Initiative (IDI), IT auditing capabilities have significantly advanced over the past decades. WGITA was established in Berlin in 1989 to address the concerns of SAIs in IT auditing.

Currently, WGITA consists of 59 member countries and plays a crucial role in shaping the IT audit agenda for SAIs. Over the years, it has supported SAIs in building their expertise and expanding their IT auditing portfolio. Furthermore, WGITA has published several guidelines in this field, including the "WGITA-IDI IT Audit Handbook for SAIs", which is available in multiple languages.

- **Expanding Regional Roles**

In addition to INTOSAI's efforts, regional organizations such as the Arab Organization of Supreme Audit Institutions (ARABOSAI) and the European Organization of Supreme Audit Institutions (EUROSAI) have established specialized committees and task forces to enhance information systems oversight. These regional initiatives aim to improve the efficiency and effectiveness of IT auditing by fostering knowledge exchange and best practices among member countries. By working collaboratively, these organizations strive to enhance the

[27] INTOSAI Lima Declaration, Part VII Section 22
[28] ISSAI 100 Fundamental Principles of Public Sector Auditing
[29] Chatterjee, S. (2018). "Addressing the Challenges of IT Audits by Supreme Audit Institutions." ISACA Journal, Volume 4

professional development of audit institutions and ensure the implementation of high-quality IT audit standards.

- **Quality and standards in IT Auditing**

IT audits have evolved as a **core function within SAIs**, coinciding with efforts to develop and implement **public sector auditing standards**. INTOSAI has played a key role in **establishing the International Standards of Supreme Audit Institutions (ISSAIs)**, which provide a **global framework for public sector auditing** (INTOSAI, 2019).

One of these standards is ISSAI 5310, which was specifically developed to establish a methodology for reviewing information security systems. Additionally, audit guidelines such as ISSAI 5310 and the ISSAI 5100 Manual provide operational guidance for conducting IT audits within the broader framework of the International Framework of Professional Practices (IFPP)[30].

- **Capacity development support for supreme audit institutions (SAIs)**

Between 2013 and 2016, a collaborative program was implemented between the INTOSAI Development Initiative (IDI) and the Working Group on IT Audit (WGITA) to support Supreme Audit Institutions (SAIs) in enhancing their capabilities and performance in IT auditing. This initiative was launched in response to growing challenges faced by SAIs in computerized information systems environments, making it essential to build capacity in IT auditing and to provide recommendations aligned with INTOSAI standards and best practices[31]

- **Training and professional development**

Supreme Audit Institutions have organized training programs for their auditors specializing in IT auditing. These training sessions covered various aspects of IT auditing and involved experts from professional agencies and peer institutions.

Additionally, SAIs encouraged their staff to obtain internationally recognized certifications, such as[32]:
- Certified Information Systems Auditor (CISA®)
- Certified Information Security Manager (CISM®)

[30] http://www.idi.no/en/about-idi/reports
[31] INTOSA**I.** *IDI Performance and Accountability Report Supplement, 2015.*
[32] https://www.idi.no/about-idi/reports

Some SAIs have also provided training for these certifications and covered associated costs, which helped develop a pool of skilled IT audit professionals[33].

- **Advanced Tools and Technologies**

To enhance IT audit efficiency, SAIs have adopted various audit software tools, including:

- Audit Command Language (ACL)
- Interactive Data Extraction and Analysis (IDEA)
- TeamMate Analytics

Additionally, EUROSAI developed a specialized IT audit tool called CUBE, designed to facilitate e-government auditing.

- **Big Data Analytics in IT Auditing**

SAIs play a crucial role in strengthening information systems oversight through the use of big data analytics platforms. These platforms enable the processing and analysis of massive datasets, leveraging a mix of open-source and proprietary software.

Studies indicate that SAIs commonly use a combination of open-source and proprietary tools, favoring:

- IDEA, R, and ACL for data analytics
- Generalized Audit Software (GAS), such as IDEA and ACL, for structured data and Computer-Assisted Audit Techniques (CAATs)

However, some SAIs have started adopting custom programming languages for advanced analytics, including R and Python. This shift reflects an increased awareness of the importance of advanced data analytics for effective oversight [34].

- **Data collection methods in IT auditing**

Most Supreme Audit Institutions (SAIs) have the legal authority to collect data from audited entities. However, data collection procedures are not always clearly defined in regulations. Some SAIs have specific audit laws requiring audited entities to submit government financial transaction data electronically [35].

[33] https://www.idi.no/about-idi/reports

[34] INTOSAI Working Group on Big Data (WGBD) , audit technology , research paper on innovative, September 2022

[35] IDI, 2015, op. cit.

Studies indicate that only 21% of SAIs use the internet for remote data transmission, while others rely on traditional methods such as:
- Manual data collection (25%)
- Read-only access at the audited entity's site (21%)
- Use of removable storage devices (21%) (INTOSAI, 2015).

- **Performance indicators and benchmarking**

The SAI Performance Measurement Framework (SAI PMF) is a global assessment framework that evaluates SAI performance based on ISSAI standards and international best practices. It provides a comprehensive, evidence-based evaluation of an SAI's performance, including its audit function[36].

The **IT Audit Self-Assessment (ITASA)** is a **quality assurance tool** designed as a **workshop** with participation from various organizational levels. The assessment is led by a **peer supervisor from another audit institution**.

Enhancing IT Auditing in Supreme Audit Institutions

- SAIs play a critical role in strengthening IT oversight amid rapid technological advancements and digital transformation. By:
- Developing legislation
- Establishing specialized units
- Training personnel
- Adopting international standards and best practices

SAIs contribute to transparency, efficiency, and cybersecurity. Strengthening collaboration between stakeholders and developing advanced auditing tools enhances the effectiveness of SAIs in protecting data and ensuring smooth, reliable government operations.

Section two: Cybersecurity

In the modern technological era, cybersecurity has become indispensable. Protecting against cyber threats is vital to maintaining the integrity of systems and data. Like many other countries, Algeria faces challenges in the field of cybersecurity. This chapter explores the conceptual framework of cybersecurity and Algeria's efforts in this domain, aiming to enhance technical capabilities and ensure the effective protection of sensitive data and information.

[36] Chatterjee, S. (2018). *Addressing the Challenges of IT Audits by Supreme Audit Institutions.* ISACA Journal, Volume 4, op. cit.

I. Conceptual Framework of Cybersecurity

1. What is Cybersecurity?

The information and technology revolution has led to a shift in the concept of power, moving towards cyberspace with the emergence of the internet and websites. Cyberspace has become one of the most crucial domains where international actors, particularly states, operate.[37] This has significantly influenced the ability of states to use different forms of power, whether hard or soft. As nations increasingly rely on cyberspace for security and military power, many have incorporated it into their national security strategies.[38]

Cybersecurity is a relatively new term for a set of longstanding practices concerning computer network security. However, its definitions often vary and are sometimes contradictory, leading to disagreements among governmental entities worldwide. The meaning of cybersecurity continues to evolve over time. Today, top government agencies in the United States and other countries regard cybersecurity as a major national security challenge. Some researchers argue that the absence of a widely accepted and concise definition that captures the multidimensional aspects of cybersecurity could hinder technological and scientific progress. This prevailing technical view of cybersecurity may lead to the separation of disciplines that should instead work collaboratively to address complex cybersecurity challenges.[39]

- **Authoritative definitions of cybersecurity:**

- **National Institute of Standards and Technology (NIST):**
  - Defines cybersecurity as "the protection of information and systems from cyberattacks through the use of specific technologies, procedures, and tools to ensure the confidentiality, integrity, and availability of information and systems."
- **ISO/IEC 27001:**
  - Describes cybersecurity as "the deliberate efforts to protect internet usage and the connected infrastructure, including software, hardware, and data, from cyberattacks and electronic intrusions."
- **American Institute of Certified Public Accountants (AICPA):**
  - Defines cybersecurity as "a set of multiple activities that involve protecting systems, networks, software, and data from cyber threats, as well as recovering systems after attacks occur."

[37] Khalifa, Ihab. *Electronic Power and the Dimensions of Transformation in the Concept of Power. Awraq* (Papers), Issue 12, 2014, p. 20.
[38] Ibid, p. 22.
[39] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, No. 4 (10), October 2014. Previously cited.

- **World Economic Forum (WEF):**
  - Defines cybersecurity as "a collection of technologies, processes, and practices designed to protect networks, devices, software, and data from attacks, damage, or unauthorized access."

2. Definition of cybersecurity governance

"Cybersecurity governance" or "IT governance" refers to the mechanisms used to manage information security and regulate security systems within an organization to achieve its objectives. Cybersecurity governance is an ongoing process and an integral part of an organization's culture, aligning with its strategic goals. It defines tactical and operational security rules, such as implementing appropriate controls. Thus, it ensures compliance with applicable standards and consistency in implementing regulatory frameworks. Whether an organization is subject to NIST 800-53, ISO/IEC 27000, or the Payment Card Industry Data Security Standard (PCI DSS), it must adhere to specific requirements and adopt best cybersecurity practices. Developing policies, guidelines, and procedures serves as the foundation for a governance framework and the establishment of a comprehensive security program to ensure the application of security principles, measures, and controls within the organization [40].

According to the ISO/IEC 27001 standard from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), IT governance is defined as "the system by which an organization directs and controls security governance, establishes the accountability framework, and provides oversight to ensure appropriate risk mitigation, while management ensures the implementation of controls to mitigate risks"[41].

Cybersecurity governance specifically refers to the application of governance principles to the provision, management, and monitoring of security services within a national context. Additionally, the concept of cybersecurity governance is based on the idea that the security sector must adhere to the same high standards imposed on other public sector service providers. Failure to meet these standards can undermine a country's political, economic, and social stability[42].

[40] Okiok. (2018). *Gouvernance & Conformité | Sécurité de l'information | OKIOK - Sécurité dans un monde en changement.* Retrieved from https://www.okiok.com
[41] Swinton, B., & Hedges, M. (2019). *Cybersecurity Governance: A Strategic Framework for Managing Cyber Risk.*
[42] Brantly, A. F., & Puyvelde, D. V. (2019). *Cybersecurity Governance: Enhancing Security Through Risk Management.*

II. The Path to Cyber Maturity

With the increasing complexity of threats and risks, many organizations face significant challenges in implementing effective cybersecurity governance. The infographic "Cyber Risk Management: A Crisis of Confidence" by CMMI Institute and ISACA highlights that business leaders recognize the importance of mature cybersecurity for thriving in the modern digital economy. However, they often lack the necessary insights and data to ensure efficient and effective cyber risk management.[43]

Studies indicate that damages caused by cybercrime are expected to cost the world $6 trillion annually by 2021, compared to $3 trillion in 2015, according to Cybersecurity Ventures. Furthermore, 87% of C-Suite executives and board members lack confidence in their company's cybersecurity capabilities.

So how can decision-makers trust this uncertain landscape, especially amid the COVID-19 pandemic? The first step for most organizations is to implement a strong cybersecurity governance program[44].

1. Steps to Implement Cybersecurity Governance:

There are **seven key steps** decision-makers should follow to establish an effective cybersecurity governance program:

1. **Assess the Current State:** Evaluate cyber risks to identify vulnerabilities and create a roadmap to address them.
2. **Develop, Review, and Update All Cybersecurity Policies, Standards, and Procedures:** Establish a clear cybersecurity governance framework with well-defined expectations.
3. **Approach Cybersecurity from a Business Perspective:** Identify the data that needs protection, align cyber risks with enterprise risk management, and prioritize cybersecurity investments in relation to other business investments.
4. **Enhance Cybersecurity Awareness and Training:** Ensure that employees are well-informed about security risks and their responsibilities in cybersecurity. Organizations must provide staff with the necessary skills, qualifications, and training programs to protect their information and technological assets.[45]

[43] Managing Cybersecurity Risk: A Crisis of Confidence. (2020). CMMI Institute and ISACA
[44] https://cybersecurityventures.com/annual-cybercrime-report-2017/
[45] https://ega.ee

5. **Cyber Risk Analytics:** Cybersecurity teams must define, document, and approve a methodology for managing cyber risks, considering confidentiality, availability, and integrity of information assets.[46]
6. **Monitoring, Measurement, Analysis, Reporting, and Continuous Improvement:** Establish periodic assessment schedules, measure key cybersecurity performance indicators, analyze data, and develop improvement plans. Regular reporting on cybersecurity maturity and risk posture to decision-makers is essential.
7. **Leadership Commitment:** Cybersecurity governance must be a **top priority** for senior management. Policies, standards, and processes should align with **enterprise security priorities** to ensure cybersecurity focus remains consistent despite changing business initiatives.[47]

III. Algeria's Efforts in Cybersecurity Governance

Algeria is working to strengthen cybersecurity governance through various initiatives and policies aimed at protecting its digital infrastructure and addressing increasing cyber threats. These efforts include:

1. Algeria’s National Information Security Strategy

- **Developing a National Cybersecurity Strategy**

Algeria has launched a national cybersecurity strategy to enhance national capabilities in combating cyber threats and improving coordination among relevant entities. In this context, on June 7, 2023, the President of the Republic chaired the opening ceremony of the National Cybersecurity Conference, organized by the Ministry of National Defense under the theme: *"The National Cybersecurity Strategy: Towards a Cyber-Resilient Algeria."*

The conference highlighted the importance of strengthening cybersecurity in light of rapid digital advancements and reviewed Algeria's digital landscape and the threats facing national information systems. The key pillars identified for the National Cybersecurity Strategy included:

- The current cybersecurity landscape in Algeria
- Protection of critical infrastructure
- Cyber resilience
- International cooperation
- Geopolitics of cyberspace
- Public-private partnerships

[46] Ibid
[47] https://searchsecurity.techtarget.com

- Strengthening national capabilities.

- **Initiatives by the High Commission for Digitalization**

The High Commission for Digitalization, affiliated with the Presidency of the Republic, has launched several initiatives aimed at drafting a national digitalization law and developing a National Digitalization Strategy with a vision extending to 2034. This strategy includes a five-year implementation plan (2024-2029) and the establishment of strategic digital network infrastructure through a participatory and consultative approach[48].

- **Workshops and Study Days**

Workshops and study sessions have been organized to discuss key aspects of the National Digitalization Strategy, involving various stakeholders in the field. These initiatives aim to raise awareness and facilitate knowledge exchange on cybersecurity best practice[49].

Through these efforts, Algeria reaffirms its commitment to enhancing cybersecurity governance and ensuring an effective cybersecurity framework, which contributes to protecting digital infrastructure and supporting the country's digital transformation.

2. Strengthening Cybersecurity Legislation and Regulations

Algeria has reinforced its cybersecurity laws and regulations to provide the necessary legal protection for electronic data and penalize violators. These enhancements include several laws and regulations governing IT-related activities and cybersecurity, including:

- **Law No. 09-04 of 2009**: Establishes special rules for the prevention and combat of IT-related crimes, aiming to set necessary measures to prevent cybercrimes.
- **Accession to the Arab Convention on Combating Information Technology Crimes**: Signed on **December 21, 2010**, and ratified through **Presidential Decree of September 8, 2014**. This convention aims to prevent and combat cybercrimes in Arab countries.
- **Law No. 15-04 of 2015**: Defines general regulations related to electronic signatures and certification, ensuring the necessary legal framework for their implementation.

[48] https://mns.gov.dz/static/ajax/activiter_ministre.html
[49] Ibid

- **Law No. 18-04 of 2018**: Establishes the general rules governing postal and electronic communications, including the definition and application of standards for setting up and operating electronic communication services.
- **Law No. 18-07 of 2018**: Concerns the protection of natural persons regarding the processing of personal data, setting specific regulations for safeguarding such information.
- **Law No. 05-18 of 2018**: Regulates e-commerce and establishes general provisions for conducting online business transactions.
- **Presidential Decree No. 20-05 of January 20, 2020**: Establishes a **National Information Systems Security Framework (RNSI)** aimed at unifying cybersecurity governance within national institutions.

Additionally, the **National Information Security Framework (RNSI)** was introduced by the Algerian government to harmonize cybersecurity governance across public institutions. The framework defines the minimum security requirements for managing, mitigating, and reducing the impact of potential cyber threats. It also establishes security controls and best practices that organizations must adopt. The framework emphasizes **user training and awareness**, ensuring regular assessments of security controls to maintain compliance with regulatory obligations and to respond proactively to emerging cyber threats[50]**.**

3. Structural and Institutional Framework

To ensure the effective and serious implementation of various measures aimed at achieving cybersecurity, Algerian policymakers have entrusted this mission to specialized bodies and centers within the country's sovereign institutions. These include:

- **Central Directorate for Combating Cybercrime**:
  - Operates under the Ministry of the Interior (General Directorate of National Security).
  - Extends its activities beyond Algeria by collaborating with Interpol, AFRICOM, and law enforcement agencies in major countries.
  - At the national level, it coordinates with forensic police units and central crime offices.
- **Center for the Prevention of Cybercrime and Virtual World Offenses**:
  - Falls under the General Command of the National Gendarmerie (Ministry of National Defense).

[50] https://www.mdn.dz/site_principal

    - Its activities and responsibilities largely mirror those of the National Security Department, both locally and nationally.
    - Coordination between the two entities is managed directly under the jurisdiction of the Public Prosecutor within the relevant district.
- **National Institute of Forensic Evidence and Criminology of the National Gendarmerie**:
    - Operates under the authority of the General Command of the National Gendarmerie.
    - Leverages scientific expertise and advanced laboratory testing to fulfill its mission.
    - Employs cutting-edge technologies to investigate cybercrimes, identify perpetrators, and support judicial proceedings.
- **National Agency for Information Systems Security (ANSSI)**:
    - A public administrative institution with legal personality and financial autonomy, operating under the Ministry of National Defense.
    - Responsible for various tasks, including defining accreditation methods for cybersecurity audit service providers to extract relevant information ensuring the security of national infrastructure.
- **National Authority for the Protection of Personal Data**:
    - Ensures compliance with Law No. 18-07 governing the processing of personal data.
    - Guarantees that information and communication technologies do not infringe on individuals' rights, public liberties, or privacy.

IV. Supreme Audit Institutions and Cybersecurity

In the wake of the rapid digital transformation accelerated by the **COVID-19 pandemic**, **Supreme Audit Institutions (SAIs)** have encountered new challenges in managing an unprecedented volume of data, increasing their exposure to **cyber threats**. Consequently, it has become essential for SAIs to adopt a **proactive cybersecurity approach** to safeguard their **systems and data**. To enhance the **cyber infrastructure of SAIs**, the following **comprehensive plan** is recommended[51]:

[51] https://medium.com

1. Prioritizing risk assessment and modeling

- SAIs should emphasize the importance of risk modeling and assessment to accurately identify and protect their critical assets and operational systems.
- Engage in advanced risk modeling techniques to assess the likelihood and impact of various cyber threats.
- Implement a systematic risk assessment framework to classify risks based on their severity and significance.

2. Developing advanced cyber incident protocols

- SAIs are advised to develop robust cyber incident protocols to ensure swift detection, reporting, and analysis of cyber intrusions.
- This may require establishing a sophisticated incident response strategy or collaborating with regulatory bodies to enhance reporting standards.

3. Strategic alliances with cybersecurity experts

- To stay ahead of the evolving cyber threat landscape, SAIs should strengthen collaboration with leading cybersecurity experts.
- Integrate cutting-edge security technologies, including Artificial Intelligence (AI), Machine Learning (ML), and advanced cloud security protocols**.**

4. Attracting and strengthening cybersecurity talent

- SAIs should consider strategic recruitment of professionals with deep expertise in cybersecurity or invest in upskilling programs for existing personnel, thereby building a strong cybersecurity risk management team.

5. A Holistic Approach to Risk Assessment

- Beyond technological vulnerabilities, SAIs are encouraged to conduct comprehensive risk assessments that consider social, human, and environmental factors.
- This holistic approach should include the potential consequences of cyber breaches on human rights, environmental sustainability, and macroeconomic stability.

6. Recommendations for Strengthening SAIs' Cybersecurity Posture

- Remain vigilant about emerging cyber threats.
- Adopt a multi-layered security architecture.
- Encourage the use of strong authentication mechanisms.
- Ensure regular data backups and redundancy.
- Conduct periodic audits of security protocols.
- Facilitate continuous cybersecurity training for staff.
- Develop a precise contingency plan for managing cyber incidents.

By following this strategic framework, Supreme Audit Institutions can ensure the resilience and security of their operations in the face of escalating cyber challenges in the digital era.

Chapter Three: Cybersecurity Auditing

With the rapid advancement of technology and the increasing reliance of institutions on digital systems, cybersecurity has emerged as a fundamental pillar for protecting sensitive data. As cyber threats targeting critical information infrastructure continue to escalate, cybersecurity auditing has become essential to ensure the efficiency, resilience, and security of these systems.

As an integral part of any security strategy, cybersecurity auditing requires a systematic approach that enables Supreme Audit Institutions (SAIs) to evaluate the effectiveness of security controls and ensure compliance with standards and policies.

Auditors play a key role in identifying vulnerabilities and providing recommendations to enhance cybersecurity posture and mitigate potential risks. Achieving a high level of cybersecurity demands ongoing collaboration between auditors and security officials to maintain compliance with best practices and respond effectively to emerging threats.

This, in turn, fosters trust among stakeholders, customers, and partners in an organization's ability to manage cybersecurity risks efficiently.

This chapter will explore both the theoretical and practical foundations of cybersecurity auditing, with a special focus on the role of Supreme Audit

Institutions in this domain and how they can enhance cybersecurity oversight across various sectors.

I. Fundamental concepts of cybersecurity auditing and its importance

1. Understanding cybersecurity auditing

cybersecurity auditing is a critical process that enables organizations of all sizes to identify and mitigate cybersecurity risks. It involves a systematic and thorough examination of an organization's information security controls to assess their effectiveness in protecting sensitive data and systems[52].

Cybersecurity audits act as checklists that help organizations review and verify their security policies and procedures . These audits allow organizations to evaluate the adequacy of security measures and ensure compliance with regulatory frameworks. Conducting cybersecurity audits proactively strengthens threat management strategies. While external service providers often conduct cybersecurity audits to maintain objectivity, internal audit teams can also perform them if they operate independently from senior management [53]

2. Cybersecurity Auditing According to International Standards

- **NIST Definition of Cybersecurity Auditing**

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology (NIST), provides a comprehensive set of standards to help organizations improve their cybersecurity posture. It serves as a voluntary tool that enables organizations to identify cybersecurity risks, develop response plans, and implement effective risk management strategies[54].

NIST's framework is designed to address cybersecurity risks across critical infrastructure sectors, including those not covered by specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

Cybersecurity auditing under the NIST framework ensures that organizations apply effective security controls according to established standards, enhancing their ability to detect, prevent, and mitigate cyber threats effectively.

[52] Six Benefits of a Cybersecurity Audit (and 6 Steps to Perform One)." *ISACA Journal*. Published on January 16, 2024.
[53] https://www.strongdm.com/blog/cybersecurity-audit
[54] NIST Cybersecurity Framework (https://www.nist.gov/cyberframework)

- **ISO Definition of Cybersecurity Auditing**

The International Organization for Standardization (ISO) defines cybersecurity auditing as a structured and standardized approach to assessing and managing cybersecurity within organizations. The ISO/IEC 27001 standard offers a framework for Information Security Management Systems (ISMS), covering all types of security risks [55].

Cybersecurity audits under ISO standards involve a systematic evaluation of an organization's security policies, procedures, and controls to ensure data protection and compliance with industry best practices.

- **Cybersecurity auditing in national and local legislations**

Cybersecurity auditing is an **essential component** of **national security strategies**, as outlined in Algeria's **National Information Security Reference Framework (RNSI)**. The **latest edition (2020)** identifies **20 key security domains**, including[56]:

- Physical security
- Internet of Things (IoT) security
- Security monitoring and logging
- Incident response management
- Business continuity management
- Human resource security
- Social media security
- Secure software development lifecycle (SDLC)
- IT security requirements for projects
- Third-party security management
- Asset management
- Personal data protection
- Access control management
- Mobile device security
- Network security
- Information system security
- Operational security
- Critical information systems security
- Cloud security
- Encryption

[55] ISO/IEC 27001 Information Security Management Standard
[56] Algerian National Information Security Reference Framework (RNSI, 2020)

Cybersecurity auditing within this framework involves **systematic evaluations** of these **domains**, focusing on **identifying vulnerabilities, assessing risks, and recommending security improvements** to enhance the resilience of **public institutions**.

The **first edition of RNSI (2016)** covered only **seven security domains**, highlighting the **evolution and expansion of cybersecurity governance** over time. These updates reflect **regulatory authorities' commitment** to **enhancing cybersecurity** through the **implementation of international best practices and standards**.

- **Cybersecurity auditing as a regulatory oversight process**

Cybersecurity auditing, as implemented by Supreme Audit Institutions (SAIs) in the public sector, is a comprehensive oversight process. It can be integrated into various types of audits, such as:

- Compliance audits
- Financial audits
- Performance audits

Cybersecurity audits may be conducted as part of an information system audit or as a standalone cybersecurity audit mission[57].

These oversight processes enable SAIs to:

- Assess the effectiveness of cybersecurity measures
- Ensure compliance with cybersecurity laws and regulations
- Evaluate risk management and governance frameworks

Cybersecurity audits follow various standardized methodologies, including:

- Risk-based auditing approaches
- Strategic audit planning
- Continuous security monitoring frameworks

These generally accepted audit standards provide a structured methodology for government auditors, reinforcing independence, transparency, accountability, and audit quality .

Cybersecurity auditing is an indispensable tool for protecting digital infrastructures from evolving cyber threats. By integrating international standards (NIST, ISO) with national cybersecurity regulations, cybersecurity

[57] IDI, 2015, op. cit.

audits enhance risk mitigation strategies and strengthen organizational resilience[58].

By adopting robust cybersecurity audit frameworks, Supreme Audit Institutions can ensure that governmental and public sector organizations effectively safeguard sensitive data, comply with regulations, and maintain public trust in the digital economy.

3. The importance of cybersecurity auditing

With the rapid pace of digital transformation, cybersecurity has become a fundamental pillar in the protection strategies of public institutions. These transformations play a crucial role in enhancing cybersecurity within Supreme Audit Institutions (SAIs) and contribute to achieving several key strategic objectives, including[59]:

- **Identifying vulnerabilities:** Cybersecurity auditing helps identify weak points in information systems, network infrastructure, and security protocols. Through a comprehensive assessment of existing security measures, auditing uncovers potential entry points for cyberattacks, allowing organizations to prioritize and address vulnerabilities quickly.
- **Protecting sensitive information**: Cybersecurity auditing ensures that sensitive data is encrypted and accessible only to authorized personnel, with strict security measures to prevent unauthorized modifications, destruction, or disclosure[60].
- **Ensuring regulatory compliance**: Compliance with industry regulations and data protection laws is essential for institutions to maintain trust and avoid legal consequences. Cybersecurity auditing ensures that organizations meet the necessary compliance requirements and adhere to relevant data protection standards, reducing risks of penalties or reputational damage.
- **Enhancing security posture**: Cybersecurity auditing strengthens security frameworks by identifying security gaps and updating security policies, reducing the risk of cyberattacks.
- **Building trust with stakeholders**: In the face of growing concerns over data security, cybersecurity audits reassure institutions and service beneficiaries, demonstrating a serious commitment to cybersecurity measures.

[58] Swinton, B. & Hedges, M. (2019). "Cybersecurity Governance: A Strategic Framework for Managing Cyber Risk."

[59] Six Benefits of a Cybersecurity Audit, Previously Cited

[60] https://agileblue.com/what-is-a-cybersecurity-audit-why-is-it-important

- **Ensuring business continuity**: By protecting critical systems and sensitive data, cybersecurity audits mitigate the risk of disruptions caused by cyber incidents, ensuring the continuity of government operations.

Cybersecurity Auditing in Public Institutions

According to a study conducted by the United Nations Joint Inspection Unit (JIU) as part of its 2020 program, cybersecurity is not only crucial for private enterprises but also for government institutions. The study highlights that digital transformation and the adoption of ICT solutions have increased the complexity and scope of cyber threats facing public institutions[61].

The study further states:

- New and emerging risks require greater attention, particularly global threats affecting public sector operations.
- Emerging risks arise from the adoption of new technologies, which accelerate digital transformation but also introduce new security vulnerabilities.
- The United Nations Joint Inspection Unit plays a role in analyzing cybersecurity policies and best practices across UN organizations, focusing on IT governance, internet security management, and cloud computing adoption.

Cybersecurity auditing is a **critical tool** for **any government institution** seeking to **protect its digital resources** in an era of increasing cyber threats. By **enhancing security frameworks**, ensuring **compliance with international standards**, and **strengthening trust in digital systems**, cybersecurity audits contribute to building a **secure and resilient public sector** that **effectively serves the public interest**.

4. Challenges faced by supreme audit institutions in cybersecurity auditing

Cybersecurity is a fundamental component of protecting critical infrastructure in the digital age. Supreme Audit Institutions (SAIs) play a crucial role in ensuring the effectiveness of cybersecurity strategies. However, these institutions face significant challenges in conducting cybersecurity audits effectively.

[61] United Nations Joint Inspection Unit. (2020). *Cybersecurity Policies and Best Practices in UN Organizations.*

First: Technical challenges

Technological Complexity

- **Understanding advanced systems:** Modern systems and advanced digital environments require an in-depth understanding of technical and technological structures (NIST, 2018).
- **Rapid evolution of cyber threats:** Cyberattacks are constantly evolving, making it difficult for auditors to keep up with these changes effectively. Cyber threats frequently emerge through new attack vectors and techniques, necessitating that IT security analysts stay up to date with the latest threats and vulnerabilities to effectively protect digital assets.

Lack of skills and knowledge

A shortage of skills and expertise is one of the most prominent challenges in cybersecurity. Auditors and IT security analysts must continually update their knowledge and skills to keep pace with the rapid developments in this ever-changing field. Analysts must have a deep understanding of cybersecurity principles, best practices, various attack methods, malware analysis, and security frameworks such as **NIST** and **ISO/IEC 27001**, in addition to secure coding practices (ISO/IEC 27001:2013). Staying informed about the latest trends and emerging threats in the cybersecurity landscape is critical to ensuring effective protection of systems and networks[62].

Second: organizational challenges

The voluntary nature of the regulatory framework

- **Inability to enforce compliance:** SAIs often lack the authority to enforce the adoption of cybersecurity standards and procedures, which hinders the effective implementation of cybersecurity measures (INTOSAI WGITA, 2016).

Legislative barriers

- **Laws restricting data collection:** Regulations such as the Paperwork Reduction Act limit the ability of SAIs to collect comprehensive and effective data, reducing the efficiency of cybersecurity audits (United Nations JIU, 2020).

Third: Resource-related challenges

The gap between large and small organizations

- **Resource Disparities:** Large corporations typically have sufficient resources to address cybersecurity concerns, whereas smaller organizations

[62] https://www.cybersecurityconsultingops.com/

struggle with limited resources, making them more vulnerable to cyberattacks due to weaker protective measures.

Resource allocation

- **Competing priorities:** Often, cybersecurity competes with other priorities such as physical security and disaster response, which reduces the focus on cybersecurity. In many institutions, cybersecurity budgets remain limited compared to the increasing need for protection against evolving threats .

Fourth: priority-related challenges

The false perception of being unaffected

- **Misconceptions:** Some small organizations believe they are not potential targets for cyberattacks, leading to a lack of interest in adopting robust cybersecurity measures.

Competing priorities

- **Divided efforts:** Allocating resources among various competing priorities can impact the effectiveness of cybersecurity audits.

SAIs face significant challenges in the field of cybersecurity auditing. By understanding these challenges and working to develop effective strategies to overcome them, institutions can enhance the protection of critical infrastructure and ensure the security of information and digital systems more effectively.

II. Cybersecurity audit methodology

Information security is a critical challenge in today's digital era, requiring continuous adaptation of security strategies and the adoption of advanced and reliable audit methodologies. Cybersecurity audits are based on robust frameworks aligned with internationally accepted government audit and regulatory process standards. These frameworks provide a structured approach for evaluating security, identifying vulnerabilities, and making recommendations to enhance security and protect information.

One of the most prominent models in this field is the Information Security Program Audit Guide issued by the Government Accountability Office (GAO). This guide serves as a comprehensive reference, offering precise and innovative instructions for security audit procedures. Through this guide, analysts and auditors can leverage advanced tools and techniques to assess security and analyze threats in a comprehensive and effective manner.

Cybersecurity audits rely on Generally Accepted Government Auditing Standards (GAGAS) and regulatory operational frameworks, which ensure accountability

and enhance government operations and services. The International Standards of Supreme Audit Institutions (ISSAI) provide a framework for conducting high-quality audits with efficiency, integrity, objectivity, and independence, thereby supporting continuous improvement and ensuring the highest standards of quality and accountability in auditing processes.

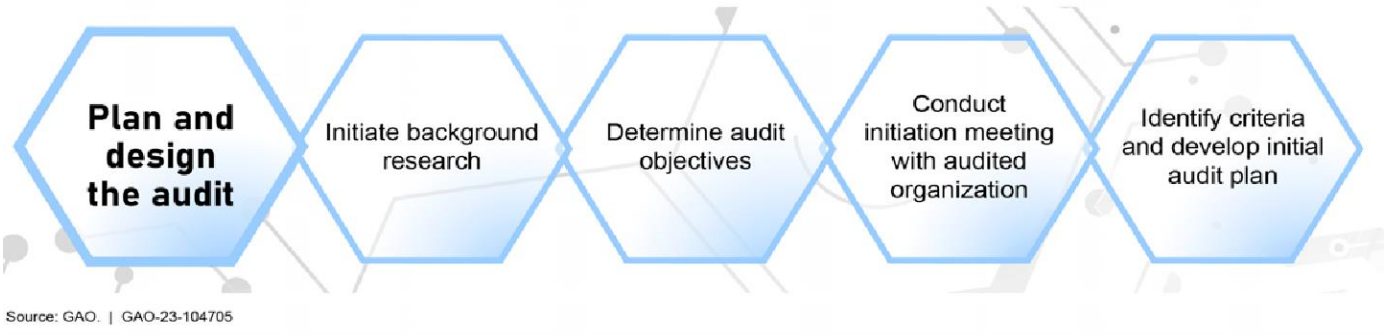
Audit fieldwork requirements under government auditing and review standards establish a general approach for auditors to plan and conduct audits. These requirements ensure that sufficient and appropriate audit evidence is obtained to provide reasonable assurance regarding audit findings and conclusions based on audit objectives[63].

❖ Planning the cybersecurity audit

Planning is an essential part of every audit. Proper planning helps address audit objectives, design methodologies to collect sufficient evidence, reduce audit risk to an acceptable level, and provide a reasonable basis for findings and conclusions. During the planning phase, it is crucial to conduct preliminary research, define audit objectives, hold an initial meeting with the audited organization, establish audit criteria, and develop a preliminary audit plan [64].

Supreme Audit Institutions (SAIs) may adopt risk-based audit planning for reviewing information systems, following international standards such as ISSAI 5310 and NIST Cybersecurity Framework. This approach ensures that cybersecurity audits prioritize high-risk areas, optimize resource allocation, and enhance the effectiveness of security governance within organizations [65].

Figure 02: Cybersecurity Audit Planning and Design



Reference: *Cybersecurity Program Audit Guide, U.S. Government Accountability Office (2023), p. 13.*

[63] GAO's Cybersecurity Program Audit Guide (CPAG), p 11
[64] INTOSAI Guide 5100, Guidelines on Information Systems Auditing, p. 09
[65] How Effective Is Your Cybersecurity Audit?, Matej Drašček, ISACA Journal, June 2022

The **planning phase** includes three key steps that auditors must carefully consider[66]:

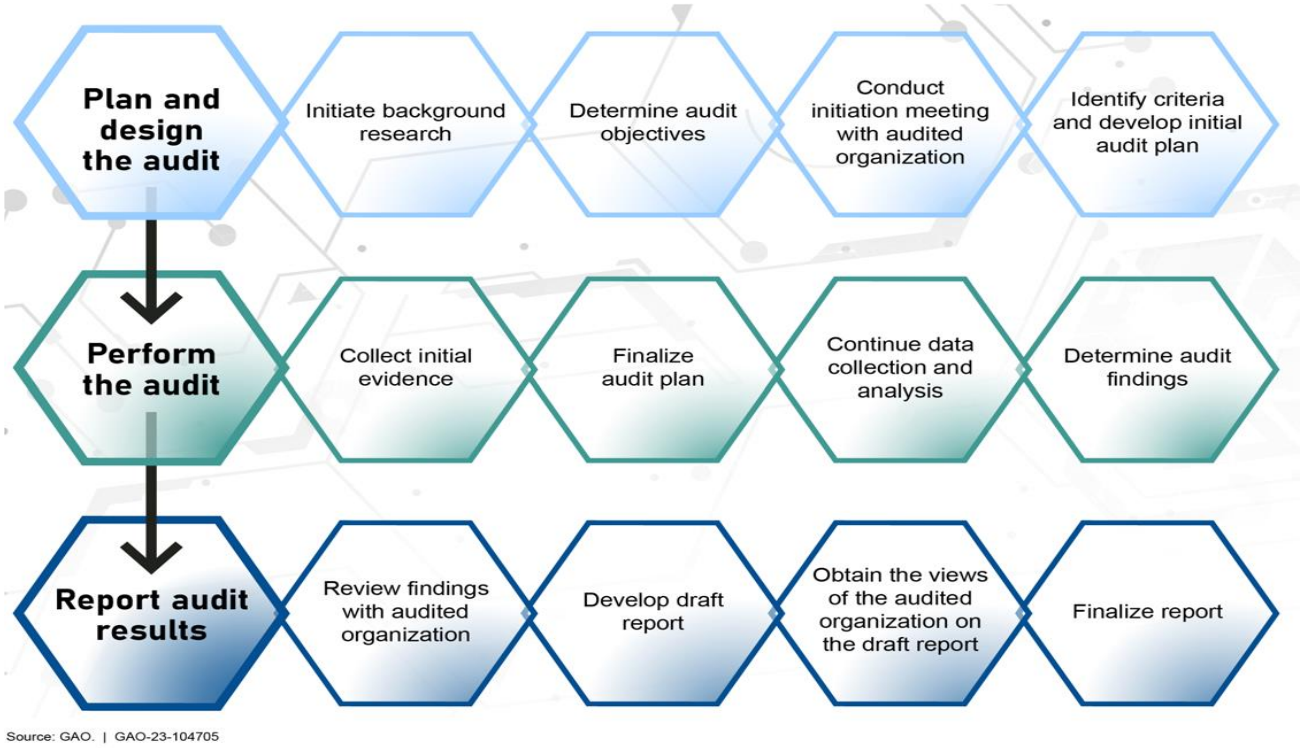
1. **Developing Strategic Plans and Understanding Stakeholder Expectations:**
    - The auditor must analyze industry trends in cybersecurity risk management, identify and clarify emerging cybersecurity risks for senior management, and participate in forward-looking discussions on cybersecurity threats and risks with management, the board, or the audit committee to understand their expectations.
    - However, this step is often overlooked by auditors despite its importance.
2. **Conducting an Initial Risk Assessment:**
    - This step guides the cybersecurity audit mission. It involves identifying the most valuable digital assets of the organization (referred to as "crown jewels") and assessing the level of protection they require based on their importance to the organization.
    - The auditor must evaluate the vulnerabilities of these key digital assets and the potential impact in the event of theft or compromise.
    - This process should be carried out in collaboration with first and second lines of cybersecurity risk management, including the IT team and the Chief Information Officer (CIO) or an equivalent role.
3. **Defining Audit Standards:**
    - This step establishes the criteria on which auditors will base their work. If the organization follows international standards for mapping and measuring cybersecurity risk management processes, auditors should refer to frameworks such as:
        - ISO/IEC 27001 for information security management.
        - COBIT® for IT governance and control.
        - National Institute of Standards and Technology (NIST) cybersecurity standards.
        - CIS Critical Security Controls (Top 20 Cyber Threats).
        - Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool.
        - COSO's Cybersecurity Risk Management Framework.
        - Custom-developed organizational standards.

[66] How Effective Is Your Cybersecurity Audit?,**Author:** Matej Drašček, *ISACA Journal*. Published on June 2022

- These standards are recommended as they have been refined over multiple iterations by professional associations and industry experts, ensuring their relevance and effectiveness.

The three main phases of a cybersecurity audit—planning, execution, and reporting—are illustrated in Figure 2. While each phase and its associated activities are discussed sequentially, many activities may overlap during the audit process.

Figure 03: Key audit phases



Reference: *Cybersecurity Program Audit Guide, U.S. Government Accountability Office (2023), p. 12.*

Planning is a critical component of every audit process. Proper planning helps in:

- Defining **audit objectives**.
- Developing a **methodology to gather necessary evidence**.
- **Minimizing audit risks** to an acceptable level.
- Providing a **reasonable basis for conclusions and findings** based on the audit objectives.

Key Steps in the Planning Phase

a) Conducting Preliminary Research

Before engaging with the audited entity, gaining a thorough understanding of the organization is crucial for effective planning. Relevant information can be obtained by:

- Reviewing previous audit reports and findings.
- Analyzing publicly available information, such as:
  - The organization's website.
  - Regulatory filings.
  - Policy documents.
  - Industry publications and news articles.
- Examining prior recommendations and related reports to assess the effectiveness of past cybersecurity improvements.

By thoroughly analyzing historical data and regulatory contexts, auditors can enhance the accuracy and effectiveness of cybersecurity evaluations and ensure compliance with best practices and industry standards[67].

b) Defining audit objectives

Defining audit objectives is a critical step in the cybersecurity audit process. The first priority is to clearly identify the subject of the audit. What does cybersecurity mean within the organization?
According to ISACA, cybersecurity is defined as:
"The protection of information assets by addressing threats to information processed, stored, and transported by interconnected information systems."

Cybersecurity auditing encompasses:

- Control frameworks
- Governance and risk management practices
- Compliance risks at the enterprise level

In some cases, the audit scope may extend to third-party vendors linked through contractual agreements.[68]

[67] GAO's Cybersecurity Program Audit Guide (CPAG),, Previously cited , p 13.

c) Documenting cybersecurity audit objectives

Clearly documenting cybersecurity audit objectives is **crucial** to ensuring a structured and effective audit. **Audit objectives function as key questions** that auditors seek to answer using available evidence and applicable standards. These objectives, **scope, and methodology** may be adjusted during the audit process as necessary.

Key objectives of cybersecurity audits include[69]:

- Assessing compliance with national cybersecurity regulations and other applicable legislation.
- Evaluating the effectiveness of cybersecurity controls within a broader systems assessment.
- Enhancing security measures related to data protection, system reliability, and risk mitigation.
- Identifying and analyzing potential cybersecurity risks associated with control implementation.
- Reviewing policies and procedures related to system development and security operations.

A report by the European Union Agency for Cybersecurity (ENISA) highlights extensive efforts in developing and implementing cybersecurity performance audits across EU institutions. These audits assess a range of risks, such as:

- Threats to EU citizens' rights due to the misuse of personal data.
- Disruptions in the provision of essential public services.
- Risks leading to significant consequences for public security, economic stability, and national well-being.
- Implications for cybersecurity within the broader EU framework.

In this regard, the report published by the European Union Agency for Cybersecurity (ENISA) on cybersecurity in EU institutions highlights the extensive efforts undertaken to prepare and implement performance audits focused on cybersecurity.
These audits assess a variety of risks, including:

- Threats to the rights of European citizens due to misuse of personal data.

[69] ISACA, *Information Systems Auditing: Tools and Techniques, Creating Audit Programs*, USA, 2016

- The inability of institutions to fully or partially deliver essential public services.
- Risks that could lead to severe consequences for public security, well-being, and the economy of member states.
- Potential impacts on cybersecurity within the European Union.

When designing their audits, these institutions rely on various methodologies, such as:

- Evaluating strategic documents or specific cybersecurity policies.
- Analyzing processes to assess compliance with international standards such as COBIT.
- Assessing the effectiveness of existing IT management systems.

The audits have also examined issues that could negatively affect infrastructure or public services.

d) Defining the scope and boundaries of the audit

The scope represents the boundaries of the audit and is directly linked to the audit objectives. It defines the subject that auditors will evaluate, such as a specific program or aspect of a program, the necessary documents or records, the time period under review, and the locations to be included.

In cybersecurity auditing, scope determination involves identifying the computer systems, functions, and processes to be assessed. It may also include defining the policies and procedures to be reviewed. For instance, the scope might cover:

- An entire organization or a specific part of it, a network, or a narrowly targeted application or technology (e.g., wireless systems, cloud computing, blockchain, artificial intelligence) or location (such as systems or applications managed by third parties).
- All security controls or a limited subset of controls within a category, such as configuration management.

The scope of a cybersecurity audit is often more restrictive compared to general IT audits due to its complexity and technical details. Therefore, it is advisable to break down the overall scope into manageable audit processes, either annually or as part of a multi-year plan, with assessments grouped by relevant domains and methodologies.[70]

[70] ISACA. *Transforming Cybersecurity Using COBIT 5.* USA, 2013. Available at: www.isaca.org/knowledgecenter/research/researchdeliverables/pages/transforming-cybersecurity-using-cobit-5.aspx.

The first step in conducting an IT audit involves defining the scope for reviewing information systems. This includes identifying systems, applications, and processes to be audited. Clearly defining audit objectives ensures that only relevant systems and environments are tested, preventing scope creep, which can lead to inefficiencies, delays, resource strain, and reduced audit effectiveness.[71]

Supreme audit institutions (SAIs) may focus on specific business units or applications or aim to evaluate the effectiveness of an entire cybersecurity program.

Audit scope in international cybersecurity reports:

The report issued by the Joint Inspection Unit (JIU) on cybersecurity in UN system organizations highlights the extensive efforts made to define audit scope with precision.

- The review included all relevant UN entities, such as the Secretariat, departments, offices, specialized agencies, programs, and organizations.
- Special attention was given to the role of the JIU in providing cybersecurity services, ensuring that priorities were accurately set and efforts properly directed.
- The institutional and legal framework governing the audit scope was clearly established, allowing for focused efforts on critical cybersecurity issues.
- Additionally, excluded aspects of the audit scope were explicitly outlined and reviewed, demonstrating the rigorous approach and thorough analysis presented in the report.

This structured approach underscores the importance of scope definition and its impact on the quality of cybersecurity analysis and audit outcomes.

e) Conducting a preliminary meeting with audited entities

The audit team should conduct an initial meeting with the audited entity to communicate the objectives, preliminary scope, methodology, and expected timelines. During this meeting, the team should request relevant documents from the organization. Based on the audit objectives, the following general information may be required[72]:

[71] Denise Owens, Managing Data Privacy and Information Security With IT Audits, *ISACA Journal*. Published on 23 May 2023

[72] GAO's Cybersecurity Program Audit Guide (CPAG), Previously cited ,p 14 ,

Key information to be requested

- **Missions and operational processes:**
  Obtain documents detailing how operational processes contribute to organizational objectives and how dependent they are on IT infrastructure.
    - Examples of supporting evidence:
        - Standard Operating Procedures (SOPs)
        - Process flowcharts
        - Operational workflow diagrams
- IT Governance, management, and responsibilities:
  Obtain documentation on organizational structures, particularly the roles and responsibilities of teams in charge of cybersecurity and incident response.
- **Budget and funding:**
  Request financial reports related to IT and cybersecurity expenditures.
- **Personnel and locations**:
  Obtain details on the size and structure of IT and cybersecurity teams, including:
    - Employees
    - Contractors
    - Operational sites
- **Network and system architecture:**
  Gather network diagrams and system architecture blueprints relevant to the audit, including:
    - Security and privacy controls implemented.
- Recent Incidents and Previous Audits:
  Obtain records of significant IT incidents and findings from past audits, including:
    - Cybersecurity breaches
    - Security-related events

Post-Audit Evaluation

At the conclusion of the audit, the team should assess whether the preliminary meeting and subsequent procedures effectively supported the audit objectives. The feedback and documents collected contribute valuable insights to improving audit methodologies and security frameworks.

f) Audit Framework and Context

Once the audit objectives have been defined, the planning and scoping process must establish all cybersecurity-related areas to be covered. In other words, what are the audit boundaries? This may include[73]:

- A specific country
- A geographical region
- A department
- A functional area
- A particular aspect of cybersecurity

The scope determination should be based on a risk assessment.
Cybersecurity audit scopes are typically more specific than general IT audits due to the high level of complexity and technical details involved. For annual or multi-year audits, it is recommended to divide the overall scope into manageable reviews, classified by subject area and methodology used.[74]

In the context of defining the audit methodology

The European Union Internal Security Report on Cybersecurity Audits within EU institutions highlights the significant efforts made to conduct performance audits focused on cybersecurity.
Most Supreme Audit Institutions (SAIs) have conducted performance audits related to cybersecurity, while:

- Poland and Hungary conducted compliance audits on cybersecurity.
- The European Court of Auditors (ECA) conducted policy analyses on cybersecurity strategies.

The topics covered in cybersecurity audits varied significantly across Supreme Audit Institutions (SAIs):

- Some SAIs focused on public interest areas, such as maritime defense systems and water management systems.
- The Irish and Hungarian SAIs conducted broader audits on:
    - National cybersecurity strategy implementation
    - Personal data protection
    - Security of national data assets

[73] Ian Cooke, Previously cited ,P03 .

[74] *Transforming Cybersecurity*, ISACA USA, 2013- https://www.isaca.org ›

- Estonian and Lithuanian SAIs emphasized the strategic importance of national data assets for national security and their protection from external cyber threats.
- The Danish SAI conducted an audit on ransomware resilience across four public institutions.
- SAIs in the Netherlands, Poland, and Portugal assessed the effectiveness of IT systems used for border control.

These audits also examined issues that could negatively impact public infrastructure or services. The European Union's internal security framework was a key focus in several of these audits.

❖ Engaging external experts

Given resource constraints, Supreme Audit Institutions (SAIs) may engage external experts, such as IT consultants and contractors, to conduct information systems audits. These institutions ensure that external experts are well-trained and knowledgeable in professional conduct guidelines and applicable audit standards.

Their work must be closely monitored through formal contracts or service level agreements (SLAs), ensuring active participation from SAI staff in planning, reviewing, reporting, and follow-up phases. Additionally, SAIs must ensure that their internal teams possess the necessary skills and expertise to verify compliance with agreed-upon standards[75].

Auditors may also leverage work conducted by internal auditors, other auditors, or external experts, if deemed appropriate or necessary, in alignment with SAI mandates and applicable legislation[76].
However, auditors must establish a sufficient basis for relying on external work, ensuring that:

- The external experts are competent and independent
- The quality of the work performed meets the required standards

Ultimately, the Supreme Audit Institution (SAI) remains solely responsible for any audit opinion or report issued, and engaging external experts does not diminish this responsibility.

❖ Conducting the audit

[75] INTOSAI GOV 9140: Use of Experts in Audit and Assurance Engagements
[76] https://www.iaasb.org/consultations-projects/using-work-expert

The execution of an audit process is not only about comprehensively gathering audit evidence but also about ensuring the accuracy and reliability of that evidence. During the audit cycle, evidence must be systematically collected across the four key domains defined within the cybersecurity framework. These domains include various processes such as identity and access management, data protection, cloud and software security, and third-party and workforce management, among others.[77]

For a cybersecurity audit to be **effective**, auditors must collect **sufficient and appropriate evidence** to make well-informed decisions.

The International Standards on Auditing (ISA) establish a set of procedures for evidence gathering (ISA 500), including inquiries, observations, analytical procedures, and re-performance. However, some of these methods alone may not be reliable enough to ensure a comprehensive cybersecurity audit.
For instance, if the audit team only gathers evidence through interviews with first and second-line security personnel, it may be efficient but less effective than re-performing some of the processes carried out by system administrators. Typically, adequate audit evidence is collected through a combination of methods to ensure the quality of evidence in accordance with audit standards.[78]

Key stages of audit execution (as per the U.S. Government Accountability Office - GAO)[79]

1. Collecting Preliminary Evidence
2. Finalizing the Audit Plan
3. Continuing Data Collection and Analysis
4. Determining Audit Findings

1. Collecting Preliminary Evidence

Audit evidence can be categorized into three main types:

- **Physical Evidence:**

[77] [77] E.E. El-Masry, K.A. Hansen,Factors affecting auditors' utilization of evidential cues. Taxonomy and future research directions Managerial Audit. J., 23 (1) (2008), pp. 26-50,
[78] Sergeja Slapničar, Effectiveness of cybersecurity audit, International Journal of Accounting Information Systems, Volume 44, March 2022, P 5
[79] GAO's Cybersecurity Program Audit Guide (CPAG), Previously cited , P 27.

- Collected through direct observation, site visits, or inspection of assets, operations, and people.
- Documented using summarized notes, photographs, videos, diagrams, maps, or physical samples.
- Auditors must verify whether **prior authorization** is needed to capture images, especially within **restricted premises**.

- **Documentary Evidence:**
  - Includes existing records such as:
    - Policies and procedures
    - Previous audit reports
    - System security plans
    - Business continuity and disaster recovery plans
    - Risk assessments and impact evaluations
    - Security control assessments
    - Incident reports and response plans
    - System configuration and patch management records
    - Data inventories and external agreements

- **Testimonial Evidence:**
  - Gathered via inquiries, interviews, focus groups, public forums, or surveys.
  - Assessed for relevance, accuracy, and reliability to ensure sufficient and appropriate evidence.

2. Evaluating data reliability

The reliability of computerized data and the systems processing them is a critical factor in cybersecurity audits. The evaluation process includes:

- Assessing the importance of the data
- Examining the strength of corroborative evidence
- Identifying risks associated with data integrity and misuse

3. Finalizing the Audit Plan

Before finalizing the audit plan, the team must conduct preliminary data testing to provide reasonable assurance of data availability and reliability.

- Availability is critical—if data cannot be accessed, or if the required data does not exist, the team may need to reassess audit objectives.
- Reliability is essential—if data integrity cannot be verified, the team cannot use it to support audit conclusions and recommendations.

When finalizing the audit plan, the team should review potential changes in:

- Objectives, scope, methodology, time constraints, and resources

4. Continuing data collection & analysis

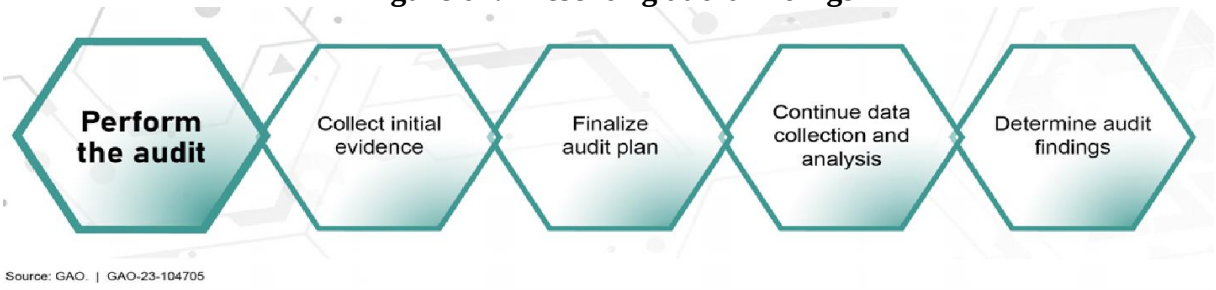
Following the finalization of the audit plan, the team proceeds with data collection and analysis, based on preliminary findings.
Common audit techniques include:

- **Examinations:**
  - Reviewing and analyzing audit subjects, such as security mechanisms, procedures, or documentation.
  - Helps auditors gain a clear understanding of cybersecurity processes.
- **Interviews:**
  - Conducting structured discussions with key personnel to gather firsthand insights into security practices.
  - Helps auditors clarify ambiguities and obtain additional evidence.
- **Testing:**
  - Performing controlled evaluations of security mechanisms, protocols, and configurations to assess:
    - Conformity with cybersecurity policies
    - Effectiveness of security controls
    - Alignment with expected security behaviors

By systematically gathering and analyzing evidence, auditors can validate cybersecurity controls, identify vulnerabilities, and enhance governance mechanisms.

❖ Presenting and reporting audit findings

Figure 04: Presenting audit findings



Source: *Cybersecurity Audit Program Guide, U.S. Government Accountability Office (GAO), (2023), p. 28.*

Cybersecurity audit reports must adhere to the reporting standards of the Supreme Audit Institution (SAI) and evaluate the technologies assessed based on the level of accuracy required by stakeholders.[80]

A **comprehensive audit report** represents the **final step in verifying the effectiveness of cybersecurity governance**. Only through a **detailed review of cybersecurity risk management** can auditors identify **critical control weaknesses** and **prevent providing stakeholders with a false sense of security**.[81]

According to **Standard 2420 of the Institute of Internal Auditors (IIA)** on **Quality of Communications**, audit reports must be[82]:

✓ Accurate
✓ Objective
✓ Constructive
✓ Comprehensive
✓ Timely

A key challenge in **cybersecurity risk management reporting** is the **technical nature of cybersecurity terminology**, which requires **clear and accessible communication** for non-technical stakeholders.

[80] IT Audit Guide for Supreme Audit Institutions (SAIs), 2014, p. 28
[81] https://www2.deloitte.com › Deloitte ›
[82] https://iaonline. theiia.org/blogs/Jim-Pelletier/2020/Pages/3-

At this stage, it is crucial to **evaluate the adequacy of audit evidence**. During evidence analysis, the audit team should assess[83]:

- Documentation of test nature, timing, and extent
- Effectiveness of control mechanisms (e.g., memos detailing procedures, test results, analytical outputs)
- Compensatory controls or alternative mitigating factors
- Criteria, conditions, root causes, and impacts for each evaluation result
- Conclusions and recommendations based on audit findings

If **gaps in audit evidence** exist, the audit team should engage with the **audited entity** to request additional documents or clarifications before finalizing their analysis.

a) Audit findings report

After completing the audit, the audit team must[84]:

1. Review findings with the audited entity
2. Prepare a draft report
3. Obtain feedback from the audited entity
4. Finalize the audit report

b) Reviewing findings with the audited entity

Upon completing the audit work, the audit team should provide the audited entity with a factual statement summarizing the audit findings. The entity has the opportunity to:

- Review, comment, and discuss findings
- Provide supporting documentation that may impact conclusions and recommendations

During this phase, sensitive issues may be addressed, and the draft report may be updated accordingly.[85] The audit team should maintain continuous communication regarding findings requiring immediate corrective actions throughout the audit process.

c) Preparing the draft report

Audit reports should clearly and concisely present findings, including:

- Audit objectives
- Scope and methodology

[83] GAO, CPAG, op. cit., p. 28.
[84] Ibid., p. 28.
[85] Ibid., p. 28.

- Findings, conclusions, and recommendations

Information from the factual statement review must be appropriately integrated into the final report.
To enhance readability and clarity, graphs and tables are recommended.

d) Obtaining feedback on the draft report

Sharing the draft audit report with the audited entity for review and feedback helps ensure the report is:
✓ Fair
✓ Comprehensive
✓ Objective

While **written feedback is preferred**, **verbal feedback** is also accepted.

e) Determining report sensitivity

Cybersecurity audit reports are often **issued in two formats**:

a) **A general (public) report**
b) **A sensitive (restricted) report**

- The sensitive report includes detailed security findings and specific vulnerabilities, but carries a risk of exposure if widely circulated.
- The general report reaches a broader audience, ensuring transparency while excluding sensitive information.

To prevent unauthorized disclosure, draft cybersecurity reports must be submitted for sensitivity review before finalization.
After reviewing sensitivity findings, appropriate revisions are made. Depending on the audit type, the final report may be:

✓ General (public)

✓ Sensitive (restricted)

✓ Both (dual report issuance)

f) Finalizing the audit report

Once the audited entity has had sufficient time to review and provide comments, the audit team proceeds with finalizing the report.
Finalization includes:

- Addressing the entity's feedback
- Including the management response (if applicable)
- Documenting verbal feedback sources (if written feedback is unavailable)

After completing these steps, the audit team can proceed with the report's publication and distribution.

Chapter conclusion

This chapter highlights the significance of evaluating **information systems** and **cybersecurity** as a fundamental pillar in protecting **information infrastructure** and ensuring **business continuity**. The **audit of information systems** involves assessing **technical processes** and **data** to verify their **effectiveness** and **security** in achieving **business objectives**. This process includes reviewing the **development**, **implementation**, and **maintenance** of **IT systems** to ensure they align with **business needs** while maintaining **security**, **privacy**, and **cost efficiency**.

Cybersecurity plays a crucial role in safeguarding **information assets** from increasing **cyber threats**. It requires a combination of **technologies** and **best practices** designed to protect **information** from **unauthorized access** and ensure **institutional stability** and **security**. The implementation of **cybersecurity governance** and **maturity steps** helps establish a **robust framework** for **data protection** and enhances **operational effectiveness** within institutions.

Cybersecurity auditing aims to assess an organization's **preparedness** to address **cyber challenges** by evaluating the **availability** and **effectiveness** of **security measures** and ensuring **compliance** with **legal** and **security standards**. The **audit methodology** is based on **comprehensive risk assessment** and the application of **international auditing standards**, ensuring a **thorough** and **effective review** of **information security**.

In this regard, **Supreme Audit Institutions (SAIs)** play a **vital role** in enhancing **oversight** of **information systems** amid **rapid technological advancements** and **digital transformation**. By establishing **specialized units** and adopting **international best practices** and **standards**, these institutions contribute to ensuring **transparency**, **efficiency**, and **cybersecurity**. Strengthening **cooperation** between **stakeholders** and developing **advanced audit tools** and **techniques** further enhances their ability to **protect data** and ensure the **continuity of government operations**.

In conclusion, this chapter underscores the **critical importance** of evaluating **information systems** and **cybersecurity** to safeguard **institutions** from escalating **cyber threats** and achieve their **strategic objectives**. **Close collaboration** between **SAIs**, **government institutions**, and the **private sector** forms the foundation for a **secure** and **sustainable cyber environment**.

Practical and analytical aspects of the audit mission: Evaluating the information systems and cybersecurity of Sonelgaz Distribution Company

Introduction

Electricity and gas are the backbone of many modern technologies and services, often overlooked in their vital role. In many parts of the world, especially in developed countries, it is difficult to imagine life without them, as numerous aspects of daily life fundamentally depend on the continuous availability of electricity and gas. Furthermore, the infrastructure for electricity and gas transmission and distribution constitutes a critical part of the essential infrastructure in most countries worldwide, ensuring sustainable energy supply, industrial operations, and the provision of essential public services【European Union Agency for Cybersecurity.

Sonelgaz is one of the key institutions in Algeria's energy sector, playing a crucial role in the country's economic and social development amid ongoing challenges and advancements. The company has adopted IT-based strategies as part of its recent strategic plans, aiming to enhance service quality at lower costs while reducing production and distribution time.

Given the significance of energy transmission and distribution infrastructure, safeguarding the institutions responsible for these services against cyber threats is of paramount importance, particularly with the rising number of cyber threats and sophisticated attacks. According to a **2021 study**, **83% of critical infrastructure organizations** experienced breaches in operational technology over the previous 36 months[86].

As a result of such incidents, electricity and gas companies worldwide have been required to comply with cybersecurity controls and standards issued by international regulatory bodies. Organizations such as the **European Union Agency for Cybersecurity (ENISA)**, **ISACA**, the **International Organization for Standardization (ISO 27001)**, and the **U.S. National Institute of Standards and Technology (NIST)** have issued guidelines, methodologies, and approaches to address cybersecurity challenges and enhance preparedness against cyber

[86] Center for Strategic and International Studies (CSIS), Significant Cyber Incidents Since 2006, USA, 2021, https://csis-website-prod. s3.amazonaws.com/s3fs-public/220104_ Significant_Cyber_Events.pdf

threats[87]. In the European Union, ENISA has reviewed the state of cybersecurity awareness among its member states[88].

These regulations aim to establish a minimum set of fundamental cybersecurity requirements, based on best practices and standards, to mitigate cyber risks to organizations' informational and technological assets from both internal and external threats. Ensuring the protection of these assets necessitates focusing on key security objectives, which include:

- **Confidentiality**: Ensuring that sensitive data is accessed only by authorized individuals.
- **Integrity**: Protecting data from unauthorized modifications and ensuring its accuracy.
- **Availability**: Guaranteeing that critical systems remain operational and accessible when needed.
- **Resilience**: Strengthening the ability to recover from cyber incidents and ensuring business continuity[89].

These controls take into account the four fundamental pillars on which **cybersecurity** is based:

- **Strategy**
- **People**
- **Process**
- **Technology**

Securing the **infrastructure and operations** of **gas and electricity distribution companies** is of **critical importance** in the face of **growing cybersecurity threats**. It has become **essential** to **assess** the **preparedness of institutions** in this sector to confront these challenges.
The **cybersecurity audit** conducted by the **Algerian Court of Accounts** as part of the **evaluation of the management of the gas distribution company** is among the **most significant** cybersecurity audits in **Algeria's energy sector**. This study aims to **assess the information system's readiness** to counter **cyber threats**, identify **vulnerabilities and challenges**, and evaluate the **company's**

[87]Volume 1, 2023, ISACA Journal, Case Study: Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator .
[88] European Union Agency for Cybersecurity (ENISA), *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies*, Greece, 29 November 2021, *https://www.enisa.europa.eu/publications/*
[89] https://ega.ee › Essential-Cybersecurity-Controls

strategies in enhancing **security** and **protecting its infrastructure and operations** from various **threats.**

I. Motivations and objectives of the Algerian court of accounts' oversight of Sonelgaz distribution's information system and cybersecurity

The Algerian Court of Accounts is the supreme oversight body responsible for monitoring public funds, with constitutional and legal authority to conduct ex-post audits of the state's finances and local communities. This institution is tasked with promoting good governance of public funds and enhancing transparency in public administration. It also holds administrative and judicial powers that enable it to conduct comprehensive oversight of public financial management.

The motivations and objectives behind the Court of Accounts' audit of Sonelgaz Distribution's information system and cybersecurity are centered on assessing the company's preparedness as a key operator in Algeria's energy sector. The aim is to evaluate its ability to govern its information system and mitigate cyber threats that could potentially disrupt the distribution of electricity and gas to consumers, thereby ensuring the stability and reliability of the country's energy supply.

The Court conducts all types of audits, including compliance audits, financial audits, and performance audits, in accordance with national regulations and international standards for supreme audit institutions (SAIs). It is responsible for overseeing various entities, including those that provide public services such as health, education, and energy.

The mandate granted to supreme audit institutions (SAIs) to conduct IT system audits is established within the ISSAI international standards under the Lima Declaration. The authority of the Court of Accounts to conduct IT and cybersecurity audits stems from its broader mandate to perform financial, compliance, and performance audits, either separately or in combination[90].

[90] *Algeria IT Audit Guide*

Figure 04: Electrification and gas supply to farms before the end of november 2022

The **motivations and objectives** of the Algerian Court of Accounts in auditing the **information system and cybersecurity of Sonelgaz Distribution** are to **assess the company's readiness** as a key operator in the **energy sector** in Algeria. The aim is to evaluate its ability to **govern its information system** and address **cybersecurity threats** that could impact the **distribution of electricity and gas to consumers**, thereby ensuring the **stability and reliability** of energy distribution in the country.

Source: Sonelgaz Algeria.

Additionally, the Court aims to strengthen its capabilities in information system evaluations, in line with Algeria's regulatory framework and government directives. It also seeks to adhere to the guidelines of INTOSAI and its regional affiliate organizations to ensure best practices in cybersecurity oversight.

II. Framework and context of the audit process

As part of information systems audits, particularly in cybersecurity, supreme audit institutions have conducted performance audits on cybersecurity-related topics. Some institutions have focused on compliance audits, while others have analyzed policies. Certain institutions have divided topics according to specific areas, such as evaluating national strategies or policies, analyzing procedures for compliance with the COBIT methodology, and even employing ethical hackers to test cybersecurity system effectiveness.

The topics addressed in these audits have varied significantly. Some institutions focused on critical areas such as cybersecurity in maritime defenses and water management systems, while others tackled broader issues such as the implementation of national cybersecurity strategies, data protection, and the

safeguarding of national data assets. Despite this diversity, all institutions examined issues that could negatively impact infrastructure or public services.

In this context, the evaluation of the information system of **Sonelgaz Distribution Company** was a key focus of the performance audit for the period **2019–2022**. Cybersecurity is one of the most critical aspects of **information systems auditing**, aligning with the broader **audit framework and context**. The audit was conducted by the **specialized working group on IT system auditing** within the Algerian **Court of Accounts**, following **Decision No. 55 of February 17, 2021**, which assigned the team under the supervision of the **Eighth Chamber**, responsible for the energy sector. This initiative was part of **the quality management audit**, included in the annual audit program of the **Eighth Chamber for 2022**, with cybersecurity being one of the core audit themes.

- **Sonelgaz Distribution Company: A Prime Target for Cybersecurity Threats**

As a key electricity distribution operator, Sonelgaz Distribution is a potential target for cyberattacks due to its critical role in delivering electricity across Algeria. The company plays a vital role in supplying electricity to households, businesses, and public institutions, making it a crucial part of the national infrastructure. The company faces major challenges in ensuring the security of its IT systems, protecting them from cyber intrusions that could disrupt electricity distribution or compromise sensitive customer data. Therefore, it is imperative for Sonelgaz to implement effective security measures to mitigate these risks and enhance the protection of its IT resources and networks.

- **Algeria's Commitment to Cybersecurity**

The Algerian government's recognition of cybersecurity's importance reflects the challenges of the digital era and the growing threats to national and international security. Cyber threats pose a significant risk to national security, potentially disrupting state infrastructure and causing severe economic and resource losses. In response, Algeria has implemented a series of policies and measures to strengthen national cybersecurity.

- **Sonelgaz: a leading energy distributor in Algeria**

Sonelgaz Distribution is a leading entity in Algeria's energy sector, providing electricity and gas services to over 11.4 million electricity customers and more than 7.3 million gas customers. In 2022, the company generated approximately

85,754 GWh of electricity, contributing to economic and social development. Sonelgaz's extensive infrastructure, comprising a vast electricity and gas distribution network, ensures reliable service delivery, reinforcing its vital role in Algeria's economic growth.

Additionally, the establishment of ELIT, a subsidiary specializing in IT system management, underscores Sonelgaz's commitment to protecting and securing its IT systems. This initiative enhances the company's capabilities in mitigating cyber risks and ensuring service continuity for consumers.[91]

- **Sonelgaz's Cybersecurity Strategy: Part of the 2035 Strategic Plan**

Sonelgaz's cybersecurity action plan is an integral component of its 2035 Strategic Plan, focusing on raising awareness and empowering its subsidiaries in cybersecurity management. The plan aims to improve the protection of Sonelgaz's equipment, networks, systems, and data, incorporating best security practices available in the industry. All Sonelgaz subsidiaries, under the leadership of Algeria's IT Technology Company (ELIT), collaborate in implementing the strategy.[92]

The cybersecurity strategy's objectives include:

- Establishing an effective cybersecurity response mechanism
- Ensuring continuous availability of IT systems
- Reducing exposure to potential cyber risks

The plan's development is based on analyzing the security needs of Sonelgaz subsidiaries and assessing the physical security of technological infrastructures.

III. Objectives, scope, and methodology

❖ **Objectives:**

The first step for an Information systems auditor is to define the scope of the audit. This step clarifies the concept of cybersecurity within the company's context.

[91] https://www.sonelgaz.dz
[92] Same reference

For the audit of Sonelgaz Distribution's Information Systems, the objective is to conduct a comprehensive assessment of the information system, focusing on aspects related to IT governance.

The evaluation of **Sonelgaz Distribution's Information System and its cybersecurity** requires a precise definition of **audit objectives**. Clearly defining these objectives ensures a **focused approach** that aligns with the **company's requirements and legal regulations**. The objectives serve as key questions that auditors seek to answer based on **evidence and established standards**.

The key objectives of the cybersecurity evaluation at Sonelgaz Distribution are:

1. **Verifying** the existence and alignment of the **cybersecurity policy** with the company's objectives and legal requirements.
2. **Assessing** cybersecurity **monitoring** in accordance with **national standards and information security regulations**.
3. **Enhancing performance oversight** by evaluating **cybersecurity effectiveness** within the broader **IT system evaluation**.
4. **Evaluating data reliability**, system confidentiality, integrity, and availability.
5. **Determining the effectiveness** of **cybersecurity mechanisms** and identifying **potential risks** associated with their implementation.
6. **Assessing risk management** and the ability to **recover information after incidents**.

❖ **Audit Scope:**

Defining the **audit scope** is a crucial step after establishing the **audit objectives**. The planning and **scoping phase** must outline all aspects to be covered under **cybersecurity**. This involves setting **boundaries** for the audit, which may include:

- A **specific country**, **geographical area**, **department**, or **business process** within the company.
- A **particular aspect** of **cybersecurity**.

It is preferable to base the scope on a risk assessment, helping to prioritize key areas that are most critical and most vulnerable to threats.

Sonelgaz Group's strategy focuses on developing "control mechanisms" in **IT systems**, leading to a **major reorganization** of **IT management responsibilities**. **ELIT (Algerian Information Technology Company)** was designated as a **specialized subsidiary responsible for information systems**, receiving full ownership of these systems while each subsidiary focuses on its core activities.

In this context, the audit conducted by the Algerian Court of Accounts primarily examines IT governance within Sonelgaz Distribution. The audit also assesses the **legality and effectiveness of the agreement** outlining the **terms and conditions of services provided by ELIT to Sonelgaz Distribution**.

Cybersecurity audits typically have a **narrower focus** compared to **general IT audits**, due to the **technical complexity** and **specific risks** involved. To enhance efficiency, the **audit scope** is divided into **manageable audit rounds**, each covering **specific areas or processes**. This structured approach allows for a **targeted assessment** and a **balanced distribution of audit efforts**.

The **cybersecurity audit** of Sonelgaz Distribution focuses on **internal cybersecurity arrangements**, particularly **institutional measures** ensuring **effective cybersecurity management**. The evaluation examines the **company's compliance** with **national cybersecurity regulations** and assesses the implementation of **security policies and procedures** in alignment with **national and international cybersecurity standards**.

Additionally, the audit evaluates the **effectiveness of security measures** in protecting **sensitive corporate data** from **potential cyber threats**. The focus includes:

- **Identity and access management**
- **Data encryption**
- **Backup and data recovery mechanisms**
- **Information security awareness programs**

These combined elements establish a **rigorous methodological framework** for evaluating the **quality of Sonelgaz Distribution's Information System and its cybersecurity** from **2019 to 2022**.

❖ Methodology and Audit Tools

The audit was conducted using a **rigorous evaluation methodology** that included several key steps, such as **document collection, analysis, evaluation, and structured interviews** with various stakeholders. Additionally, **coordination meetings** were held with the audit team. The independence and integrity of the evaluation process were ensured through continuous **dialogue with stakeholders**, their participation in the assessment, and the formulation of results.

- **Developing a protocol for information exchange between it auditors and other auditors**

When **IT auditing** is part of a broader audit process, it is essential to ensure that the audit team functions **in an integrated manner** to achieve the overall audit objectives. To facilitate effective integration, **Supreme Audit Institutions (SAIs)** may establish a **protocol** for information exchange between **IT auditors and other auditors**[93].

During the **opening meeting of the audit process**, the **IT audit team** coordinated with the **eighth chamber's audit team**, as well as with an appointed expert, to define the **methodology, work approach, and information exchange process**. All these elements were formally documented in the meeting minutes as part of the **audit documentation process**.

- **Risk-Based Approach**

Once the **audit scope** was defined, the next step was to determine the **audit objective**—in other words, **why is the audit being conducted?** From an audit perspective, it is recommended to follow a **risk-based approach** and set **audit objectives accordingly**.[94]
To enable the **Supreme Audit Institution** to effectively use a **risk assessment framework**, it must gather **relevant information about the entities under audit**. This is often done through **targeted surveys**[95].

In this context, the **audit team** designed **survey questionnaires** based on the **COBIT framework**, each focusing on a **specific COBIT domain**. By analyzing

[93] INTOSAI IT Audit Guidelines, op. cit., p. 13.
[94] Cooke, I., & Raghu, R. V. (2019, March 1). IS Audit Basics: Auditing Cybersecurity. IS Audit Basics. Retrieved from [https://www.isaca.org/]
[95] INTOSAI IT Audit Guidelines, p. 13

the **responses**, conducting **meetings with the company's IT management**, and reviewing **additional clarifying information**, the **scope and level of cybersecurity risks** were determined.

- **Adopting a COBIT-Based Audit Methodology**

The **COBIT** (Control Objectives for Information and Related Technologies) framework is an internationally recognized **IT governance model** that ensures the **optimal use of information technology**. It is widely used to improve business performance through a **balanced framework** that maximizes IT value while **minimizing risks** [96].

COBIT is an **integrated framework**, allowing compatibility with **other recognized standards** such as **CMMI, PRINCE2, ISO 27001, ISO 38500, ITIL, and ISO 9001**. It provides a **comprehensive structure** for **IT governance** and ensures effective **integration of standards, frameworks, and best practices**.

Aware of the importance of these tools, the **audit team formally adopted COBIT** as part of its key objectives for **2022**.

- **Engaging expertise under article 58 of ordinance 95-20 (as amended):**

As part of its mission to develop IT auditing practices, the **audit team sought external expertise** to provide **technical consultation and assistance** to audit structures.

In 2022, the **team leveraged expert consultation**, in accordance with **Article 58 of Ordinance 95-20 (as amended)**. A **contract was signed with an IT expert** for the period **November 11, 2022 – April 11, 2023**. The agreement covered:

- Interpretation and explanation of technical documents
- Execution of technical tests
- Training and coaching of the audit team during consultation and assistance for two pilot audits conducted by the first and eighth chambers

- **Survey and desk review**

A **variety of qualitative and quantitative data sources** were utilized by the **audit team**, which included **judges from the eighth chamber, the audit team,**

[96] ISACA. (2007). COBIT 4.1: IT Governance Framework. Rolling Meadows, IL: ISACA.

and the external expert. This ensured the **accuracy and reliability of the findings**.

The **data sources** included **survey questionnaires and desk reviews**. Information was collected through **surveys sent to the company's IT management**. Key data components analyzed included:

- Company policies and administrative decisions
- Institutional strategies and adopted technologies
- Security policies and operational procedures
- Internal and external reports

A **critical review** of supporting **documents, institutional capabilities, and operational cybersecurity structures** was conducted, taking into account **legal aspects**, including **data mapping and information system architecture**.

- **Audit Standards (COBIT-Based Methodology)**

IT auditors must define measurable, reliable, and audit-relevant evaluation criteria[97].
In this regard, the **audit team relied on COBIT 4.1's IT governance framework** to assess the most critical areas. The **key intervention domains** included:

- Planning and Organization (PO1 to PO10)
- Acquisition and Implementation (AI1 to AI7)
- Delivery and Support (DS1 to DS13)
- Monitoring and Evaluation (ME1 to ME4)

The audit team integrated these elements to establish a **precise methodology** for assessing the **quality of Sonelgaz Distribution's IT system management** from **2019 to 2022**.

Regarding **cybersecurity management**, the evaluation focused on the following key processes and domains:

- **IT Strategic Planning (PO1)** (Comité de Contact des ISC de l'UE, 2020):
- **IT Risk Management (PO9)** (NIST, Cybersecurity Framework, 2020):

[97] INTOSAI. (2019). GUID 5100: Guidance on Audit of Information Systems. Retrieved from https://www.issai.org/wp-content/uploads/2019/09/Guid-5100-Guidance-on-Audit-of-Information-Systems.pdf.

- **Software Application Acquisition and Maintenance (AI2)** (ISO 27001, 2020):
- **IT Infrastructure Acquisition and Maintenance (AI3)** ;
- **Service Level Management (DS1)** ;
- **System Security Assurance (DS5)**.

- **Collaboration with the audited entity**

Given Sonelgaz Distribution's lack of prior experience with performance audits by public accounting bodies, an **introductory meeting** was held on **September 29, 2022**. The meeting:

- Clarified the methodological approach adopted by the audit team.
- Outlined the audit procedures to be followed.
- Presented the COBIT 4.1 framework as the audit methodology.
- Introduced a risk-based audit.

- **International Collaboration**

As part of **knowledge-sharing efforts**, the **Algerian Court of Accounts** established a **partnership** with the **International Voluntary Financial Services Organization (FSVC)**. Eight meetings were conducted during the audit planning phase, during which various methodologies were reviewed, including:

- **NIST's cybersecurity framework**
- **COBIT 4.1's risk assessment methodology**

The alignment of the audit scope and objectives with COBIT 4.1 confirmed its selection as the preferred audit framework.

IV. Stages and implementation of the audit process

The audit was a **performance audit** based on the **INTOSAI standards and principles**, with the **main audit question** being whether **Sonelgaz Distribution** had effectively **managed cybersecurity**. The key stages of the audit implementation included:

1. Collection of preliminary evidence
2. Finalizing the audit plan
3. Continuing data collection and analysis
4. Determining audit findings

The **audit period** covered the years **2019 to 2021**.

The **audit began in October 2022**, and **four expert reports** were submitted to the **Eighth Chamber** between **February and October 2023**, in line with the audit mission schedule for the **"Performance Evaluation of Sonelgaz Distribution"**.
The audit team consisted of:

- **Mission Leader**
- **An assistant**
- **The head of the IT audit team**
- **An IT expert under contract**

The audit team developed the audit plan and requested documents and questionnaires related to IT governance in its four key areas, as previously outlined.

a) Collection of preliminary evidence

The audit team developed an **audit plan** covering all aspects of **Sonelgaz Distribution's IT governance**. As a **first step**, the team requested relevant **documents and questionnaires**. More than **eight interviews** were conducted, and **two applications related to finance and accounting** were tested.

The **COBIT 4.1 framework**, the **Control Objectives for Information and Related Technologies**, and the **ISO/IEC 27001** standard for IT security management systems and security controls (2020) were used**.

- **Classification of Evidence:**

Physical evidence:

- Collected through direct inspection by the audit team, including site visits to various departments and observations of personnel, assets, and processes.
- Recorded in summarized notes, screenshots, diagrams, maps, and physical samples.
- Permissions were obtained from the organization before collecting sensitive evidence, such as screenshots of certain applications.

Documentary evidence:

- Included copies of **policies and procedures, results of previous examinations, screenshots, training records, event logs, access logs, spreadsheets, database excerpts, and organizational performance data**.
- Additional documentary evidence collected:
  - Inventories of major IT systems
  - Relevant audit reports
  - System security plans
  - Disaster recovery and contingency plans
  - Security assessment reports
  - Operational concepts
  - Network diagrams
  - Agreements with external entities
  - System license packages
  - Inventories of specific network devices
  - Lists of active exemptions from security controls

Testimonial Evidence:

- Collected through inquiries, interviews, public forums, and questionnaires.
- Evaluated to ensure sufficiency, relevance, accuracy, and reliability.

Through this structured approach, the audit team was able to gather the necessary evidence to accurately and comprehensively assess the effectiveness of Sonelgaz Distribution's cybersecurity management.

b) Evaluating data reliability

Data reliability is a critical factor in auditing Sonelgaz Distribution's information systems and cybersecurity. The evaluation process consisted of several key stages, taking into account:

- **The significance of the data**
- **The strength of corroborative evidence**
- **The risks associated with data usage**
- **Lessons learned during the evaluation process**

Before implementing the audit plan, the **team conducted sufficient preliminary tests** on **core datasets** to ensure **availability and reliability**.

- **Data availability** is crucial; if **required data is unavailable**, or **does not exist**, the audit team must **reassess its objectives**.
- **Data reliability** is **essential**, as **unreliable data cannot be used to support conclusions and recommendations**.

During the **testing phase**, **30 out of 34 COBIT 4.1 domains** were evaluated, and after gathering enough information and evidence, the **IT expert prepared four partial reports in the form of risk matrices**.

c) Finalizing the Audit Plan

Before **finalizing the audit plan**, the team **reviewed and updated**:

- Audit objectives
- Scope
- Audit procedures
- Timelines
- Resource allocation

These adjustments were based on **findings from the preliminary assessment**.

d) Continued Data Collection and Analysis

After **updating the audit plan**, the audit team proceeded with **data collection and analysis** according to the outlined **audit framework**.

When analyzing **evidence**, particularly for **evaluating controls**, a combination of:

- Examinations
- Interviews
- Tests

was used to ensure **robust findings**.

Verification and evaluation:

In assessing Sonelgaz Distribution's IT system and cybersecurity, verifications included:

• Examinations

- **Reviewing, inspecting, observing, tracking, studying, or analyzing** one or more **evaluation elements** (e.g., specifications, mechanisms, or activities).
- **Aimed at improving auditors' understanding, clarifying ambiguities, and obtaining necessary evidence**.

• Surveys and desk reviews

- Multiple qualitative and quantitative data sources were used, involving eighth chamber judges, the audit team, and the external expert, to ensure data accuracy and reliability.
- Surveys were distributed to Sonelgaz Distribution's IT management.
- Key data components analyzed:
  - Policies and administrative decisions
  - Institutional strategies and adopted technologies
  - Security policies and operational procedures
  - Internal and external reports
- A critical review of regulatory documents, institutional capabilities, and operational cybersecurity practices was conducted, considering legal aspects, data mapping, and IT system architecture.

• Interviews and Meetings

The **audit team conducted interviews** with:

- The Director of Modernization
- The IT Systems Director
- Officials from subsidiary structures
- Representatives from ELIT (Algerian Information Technology Company)
- IT security officials
- Internal audit directors
- Financial and accounting managers
- End users of financial and accounting applications

These interviews provided insights into cybersecurity capabilities, risk management practices, and system vulnerabilities.

• Testing and Simulations

- Specific tests were performed on key components of Sonelgaz Distribution's IT and cybersecurity infrastructure.
- Simulations were conducted to compare the actual system state against expected security behaviors.

V. Audit report results

Four expert reports were submitted to the Eighth Chamber between February and October 2023, in the form of risk matrices. Coordination was maintained with the audit team of the Eighth Chamber throughout all stages of the audit process. The preparation of all audit outputs was carried out through continuous coordination with the Eighth Chamber, as well as with the audited entity, to ensure high-quality audit results. Additionally, the Eighth Chamber's audit team was tasked with collecting sufficient supporting evidence to substantiate the audit findings.

The drafting of the final report falls under the jurisdiction of the reporting Magistrate, who integrates the findings into their report according to its format and subject. The audit case file was also digitized using the **ALFRESCO** application.
After conducting the audit, the audit team undertook the following steps:

- **Reviewing the results with the audited organization**

Upon completing the audit, the team presented a statement of facts to the audited organization, detailing the audit findings through official correspondence and coordination meetings. The IT Directorate reviewed and discussed this statement with the audit team, providing feedback and supporting documents. Any outstanding issues were addressed and, based on this exchange, the draft report was updated accordingly.

- **Drafting the preliminary report**

The audit team presented the draft findings in a **clear and comprehensible manner**. This draft included the **audit objectives, scope, methodology, results, and conclusions**. The information provided by the audited organization, based on the statement of facts, was appropriately integrated into the report. Additionally, **graphs and tables** were utilized to enhance the report's clarity and readability.

Obtaining the audited organization’s feedback on the draft report

The draft report, along with the findings, was discussed with the audited organization’s officials for **review and feedback**. This process contributed to **developing a fair, comprehensive, and objective report**. Feedback was provided in writing by the audited entity, and verbal comments were also accepted.

VI. Opinion of the Court of Accounts

Based on the expertise provided by the **Information Systems Audit Team** at the **Court of Accounts**, and in accordance with **approved standards and the adopted audit methodology**, the **Court of Accounts** notes that **Algeria Technology Information Company (ELIT)** has been effective in its role as a **specialized subsidiary responsible for information systems and cybersecurity at Sonelgaz Distribution**. Through the **delegation of ownership of information systems** to this company, it has played a crucial role in securing and managing Sonelgaz's digital infrastructure.

Following the principle of **joint work with the audited entity** and **constructive dialogue with stakeholders**, the **observations and opinions** of the **Information Systems Audit Team** were discussed. These discussions were conducted with **full adherence to the principles of independence and impartiality**. Ultimately, the **audit methodology and key findings** were approved. Some of these findings were **already implemented** by the audited entity during the audit period, in accordance with the principle of **counteractive measures**.

Upon the **completion of the expert review period** with the **Eighth Chamber**, which was responsible for the audit mission, **four partial reports** were submitted in the form of **risk assessment matrices**. These reports included:

- The **objectives** of the audit process,
- The **main audit issue and sub-questions**,
- The **audit methodology and tools used**,
- The **risk classification**,
- The **responses of the audited entity (Sonelgaz Distribution)**,
- The **opinion of the audit team**.

Findings and conclusions

The **first step** for information systems auditors is to **define the audit subject**, which facilitates understanding **cybersecurity in the context of Sonelgaz Distribution**. Defining the audit subject enables auditors to **focus their efforts** and **identify key aspects** to be examined in the assessment of **information security and related technologies**—a crucial factor in ensuring an **effective audit process**.

The key findings of the **field study** can be summarized as follows:

- **Selection of the primary audit focus:** The **Algerian Court of Accounts** selected the **evaluation of Sonelgaz Distribution's information system and cybersecurity** as a **key audit focus** to assess the company's readiness as a **major operator in the Algerian energy sector**.
- **Impact of information and cybersecurity experts:** Findings indicate that **including an expert in information systems and cybersecurity** had a **positive effect** on the **quality of audit results**.
- **Significance of audit standards:** The selection of **appropriate audit standards** was crucial for reviewing the company's **preparedness against cyber threats**.
- **Need for additional ethical hacking specialists:** The findings highlight the **necessity of including additional experts** in **ethical hacking and penetration testing** within the audit team.
- **Precision in defining the audit subject:** One of the **primary focuses** of the study was the **importance of accurately defining the audit subject**.
- **Necessity of coordination between departments:** The results emphasize the **need to strengthen communication and coordination** between **different company departments**.
- **Providing proper training:** Findings suggest that **appropriate training** should be provided to **employees** to enhance their **understanding and capabilities** in **cybersecurity**.
- **Challenges in application management:** The study identified **complexities in managing applications** and the need to **thoroughly evaluate them** to ensure compliance with **cybersecurity and functional requirements**.

- **Data security and privacy protection:** One of the **main challenges** in **information systems auditing**, especially amid **increasing cyber threats**.
- **Managing the complexity of the information system:** Proper management of the **complexity of the information system** is essential to avoid **negative impacts** on company operations, requiring **effective oversight**.

After **completing the audit**, the findings are reviewed with the **audited organization**, followed by the development of a **draft report** and obtaining **feedback** from the organization. The **final report** should present the **objectives, scope, methodology, findings, conclusions, and recommendations** in a **clear and structured manner**, using **graphs and tables** to **enhance readability**. Additionally, **sensitivity reviews** should be conducted to **prevent the disclosure of sensitive information**. The **final reports** are issued **after reviewing the audited entity's feedback** and incorporating any necessary **modifications**.

Conclusion

The modern digital environment demands **continuous efforts** to enhance **information systems and cybersecurity oversight** by **supreme audit institutions (SAIs)**. These institutions must **adapt to evolving technological challenges** and develop **audit strategies** to counter increasing **cyber threats** effectively.

This study highlights the **importance of understanding the fundamental concepts of information systems and cybersecurity auditing**, identifying **key objectives**, and recognizing the significance of **IT auditing**. It also underscores **Algeria's efforts** in strengthening **cyber governance** and developing **cybersecurity strategies**.

Given the **complexity and proliferation of cyber threats**, **IT auditing** is crucial for **protecting IT environments, ensuring regulatory compliance, and mitigating cyber risks**. As the **digital landscape evolves**, a **proactive approach** to **IT auditing** will be essential in addressing future IT challenges.

SAIs play a **pivotal role** in **enhancing information systems oversight** amid **digital transformation**. Through **legislative development, establishment of specialized units, training of personnel, and adoption of best practices and international standards**, these institutions contribute to **ensuring transparency, efficiency, and cybersecurity**.

It is also **essential** to **understand and apply cybersecurity audit methodologies effectively**, with a focus on **challenges facing SAIs**. Auditors must **enhance their IT knowledge** and utilize **technological solutions** to achieve **successful oversight and auditing goals**.

In summary, **securing information systems and ensuring cybersecurity** require **close cooperation** between **supreme audit institutions, government agencies, and the private sector**. **Strengthening information systems oversight and cybersecurity auditing** fosters **transparency, efficiency, and cybersecurity**, leading to a **robust, data-driven government and economic system** that effectively serves the public interest.

- **Findings**

Based on the **main hypothesis and sub-hypotheses**, the study demonstrates that **applying information systems and cybersecurity auditing methods and tools** plays a crucial role in **enhancing the efficiency of financial oversight** and **strengthening the ability of SAIs to address current challenges**. The key findings include:

- **Acceptance of the first sub-hypothesis:** If **SAIs understand and apply the fundamental concepts of information systems and cybersecurity auditing**, they will be **better equipped** to address current challenges effectively.
- **Acceptance of the second sub-hypothesis:** If **SAIs adopt key steps and an effective methodology** in **evaluating information systems and cybersecurity**, it will **enhance audit efficiency** and achieve oversight objectives **more effectively**.
- **Acceptance of the third sub-hypothesis:** If **SAIs improve auditing procedures and policies related to IT and cybersecurity**, a **secure and reliable government system** will be established, aligning with **international standards** and **enhancing national cybersecurity**.
- **Acceptance of the fourth sub-hypothesis:** If **coordination and collaboration among oversight bodies** are **enhanced**, their ability to **combat cyber threats** will be **significantly improved**.

❖ **General findings**

Key findings relevant to the study include:

1. The study highlights the **importance of applying information systems and cybersecurity audit methods and tools** to **enhance the efficiency of financial oversight**.
2. Continuous improvement in **oversight and auditing strategies** plays a crucial role in **addressing growing cyber threats** and **securing IT environments**.
3. SAIs contribute to **developing cyber governance** and ensuring **transparency, efficiency, and cybersecurity**.
4. **Ensuring information systems security** requires **close collaboration** among **SAIs, government agencies, and the private sector**.
5. **Strengthening cooperation and coordination:** Effective **collaboration** between **oversight institutions** enhances their ability to **combat cyber**

threats, facilitating **information exchange and a shared understanding of cybersecurity challenges**.

6. **Ensuring regulatory compliance:** IT auditing helps **guarantee compliance** with **existing regulations and security standards**, improving **cybersecurity** and building a **secure and reliable government system**.
7. **Role of oversight bodies:** SAIs play a **critical role** in **proposing and developing legislation, establishing specialized units, and adopting international best practices and standards**, contributing to **transparency, efficiency, and cybersecurity**.
8. **A proactive approach: Adopting a proactive stance in IT auditing** will be crucial for the **future of IT risk management**, helping organizations **effectively counter increasing cyber threats**.

Through these findings, it is evident that **enhancing information systems oversight and cybersecurity auditing** significantly contributes to **protecting data and ensuring the continuity of government operations in a seamless and reliable manner**, reinforcing **public trust in the government and data-driven economic systems**.

❖ **Recommendations**

Based on the findings, the **key recommendations** are as follows:

1. **Enhance training and continuous development** for auditors and oversight professionals to strengthen their **understanding of emerging technologies and cyber threats**.
2. **Promote collaboration and information sharing** between **oversight institutions** to **enhance their ability to combat cyber threats** effectively.
3. **Strengthen cyber governance** at the **government level** by **establishing and enforcing a strong legislative and regulatory framework**.
4. **Encourage institutions** to **adopt best practices in information security and regulatory compliance**.
5. **Increase awareness of cybersecurity** and emphasize the **importance of preventive measures and modern security technologies** to **protect data and critical infrastructures**.

References list

References in arabic:

1. Dahmash, Naeem & Abu Zar, Afaf Ishaq. *Regulatory Controls and Internal Auditing in IT Environment.* The Fifth Annual International Scientific Conference, Faculty of Administration, Economics, and Management Sciences, Al-Zaytoonah University of Jordan, under the theme *"Knowledge Economy and Economic Development,"* Amman, Jordan, 2005.
2. Musleh, Nasser Abdul Aziz. *The Impact of Computer Use on Internal Control Systems in Banks Operating in the Gaza Strip.* Master's Thesis, Islamic University, Faculty of Commerce, Gaza, 2007.
3. Al-Humairi, Bashir, Al-Qawi, Mohammed, Al-Shammari, Abdelkader. *Use of IT and Data Auditing Using COBIT.* Central Organization for Control and Auditing, Yemen, 2011.
4. Saeed, Howaida Al-Noor. *IT Auditing.* National Audit Office, Sudan, 2011.
5. Ehab Khalifa. *Electronic Power and the Shift in Power Characteristics.* Bibliotheca Alexandrina, Egypt, 2014.
6. Ibrahim Jabal. *Available Control Tools for Supreme Audit Institutions and Ways to Develop Them.* Cairo: Dar Al-Nahda Al-Arabiya, 2015.

Standards and guidelines :

1. INTOSAI Working Group on IT Audit (WGITA) & INTOSAI Development Initiative (IDI), *IT Audit Guide for Supreme Audit Institutions*, translated by the State Audit Bureau of Kuwait, February 2014.
2. INTOSAI Working Group on IT Audit (WGITA) & INTOSAI Development Initiative (IDI), *IT Audit for Supreme Audit Institutions*, 2022.
3. International Organization of Supreme Audit Institutions (INTOSAI), *Guidance 5100: Guidelines for IT Systems Review.*
4. ISSAI 5300 - *IT Audit Guidelines*.
5. *Cybersecurity Audit Guide*, U.S. Government Accountability Office (GAO), 2023.

6. INTOSAI, *ISSAI 100 - Fundamental Principles of Public Sector Auditing – Audit Team Management and Skills*, 2019.

Laws and Executive Decrees:

1. **Law No. 04/09** of August 5, 2009, concerning special rules for preventing and combating crimes related to information and communication technology.
2. **Law No. 18-04** of May 10, 2018, defining the general rules related to postal and electronic communications.
3. **Law No. 18-07** of June 10, 2018, on the protection of natural persons in the processing of personal data.
4. **Law No. 18-05** of May 10, 2018, concerning electronic commerce.
5. **Presidential Decree No. 20-05** of January 20, 2020, establishing a national information systems security framework.
6. **Presidential Decree No. 15-261** of October 18, 2015, defining the composition, organization, and operational procedures of the National Authority for the Prevention of Cybercrime.

Foreign Sources :

1. **Center for Strategic and International Studies (CSIS).** "Significant Cyber Incidents Since 2006." USA, 2021.
2. **Deloitte.** "IT Audit in the Era of Digital Transformation: How to Adapt and Thrive." *Deloitte Insights*, 2021.
3. **PwC.** "Digital Transformation." *PwC*, 2018.
4. **EY, Ajak.** "Navigating the Risk and Regulatory Landscape: Technology and Digital Transformation." *EY Insights*, 2020.
5. **Siponen, M., & Vance, A.** "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations." *MIS Quarterly*, 2010.
6. **ISACA Journal, Volume 1, 2023.** "Case Study: Performing a Cybersecurity Audit of an Electric Power Transmission Systems Operator."
7. **European Union Agency for Cybersecurity (ENISA).** "Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies." Greece, November 29, 2021.

8. **EU Contact Committee of SAIs.** "Audit Compendium: Cybersecurity in the EU and Its Member States - Auditing the Resilience of Information Systems and Critical Digital Infrastructure Against Cyberattacks." December 2020.
9. **ISACA.** "Auditing Cybersecurity." *ISACA Journal*, 2019.
10. **Cooke, I., & Raghu, R. V.** "IS Audit Basics: Auditing Cybersecurity." *IS Audit Basics*, March 1, 2019. Retrieved from https://www.isaca.org/.
11. **Sathyanarayanan, Kishan.** "Disaster Recovery and Business Continuity Preparedness for Cloud-based Start-ups." *ISACA Now Blog*, 2023.
12. **Kim Pham, CIA, Market Advisor.** "Cloud Computing — What IT Auditors Should Really Know." *ISACA Now Blog*, 2022.

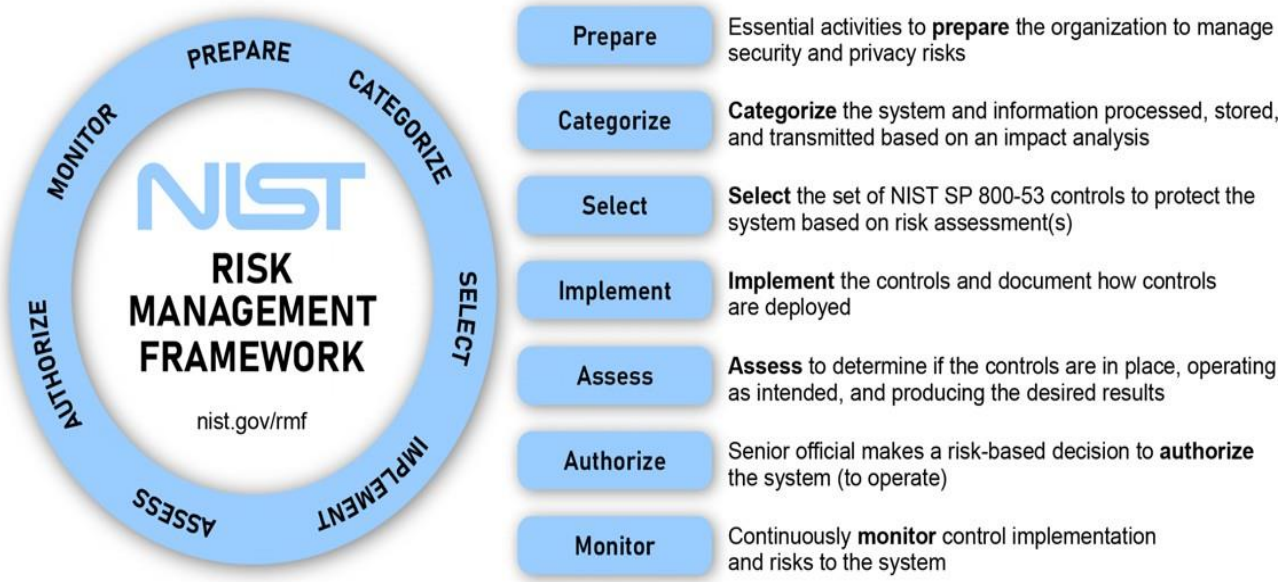
Web Resources:

1. **ENISA (European Union Agency for Cybersecurity).** https://www.enisa.europa.eu/publications/
2. **eGA (e-Governance Academy).** https://ega.ee - *Essential Cybersecurity Controls*
3. **Fibladi.** https://fibladi.com/
4. **Sonelgaz.** https://www.sonelgaz.dz/
5. **National Audit Office of Bahrain.** https://www.nao.gov.bh/category/information-systems-audit
6. **Audit Guru.** https://audit.guru/disaster-recovery-and-business-continuity-in-it-audits/#:~
7. **Atlant Security.** https://atlantsecurity.com/cybersecurity-audits-are-necessary-in-the-due-diligence-of-ma-deals/
8. **Pempal.** https://www.pempal.org - *Auditing IT Governance*
9. **ISACA.** https://www.isaca.org/resources/news-and-trends/industry-news/2023/managing-data-privacy-and-information-security-with-it-audits
10. **UpGuard.** https://www.upguard.com/blog/cyber-hygiene
11. **Deloitte.** https://www2.deloitte.com
12. **Internal Auditor Online (The Institute of Internal Auditors).** https://iaonline.theiia.org/blogs/Jim-Pelletier/2020/Pages/3-
13. **TechTarget.** https://searchsecurity.techtarget.com
14. **Ministère de la Défense Nationale (Algeria).** https://www.mdn.dz/site_principal
15. **Medium.** https://medium.com

16. **strongDM.** https://www.strongdm.com/blog/cybersecurity-audit
17. **Cybersecurity Consulting Ops.** https://www.cybersecurityconsultingops.com/
18. **AgileBlue.** https://agileblue.com/what-is-a-cybersecurity-audit-why-is-it-important

Appendices

Appendix 01: Key elements of the national institute of standards and technology (NIST) risk management framework



Source: *National Institute of Standards and Technology, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2,* SP-800-37 (Gaithersburg, MD: Dec 2018); images: agency logos. | GAO-23-104705

Appendix 02: The ISO 27001 standard family

The **ISO 27001 standard family** is a set of international standards developed to provide a framework for **Information Security Management Systems (ISMS)**. These standards aim to ensure that organizations have effective processes in place to protect their information from security threats while ensuring **confidentiality, integrity, and availability** of data. The family includes multiple standards, among which the most notable are:

- **ISO/IEC 27001**: Defines the requirements for establishing, implementing, maintaining, and continuously improving an ISMS, including the **identification, assessment, and treatment of information security risks**.
- **ISO/IEC 27002**: Provides guidance on security controls based on best practices and offers a **set of security controls** for use within an ISMS.
- **ISO/IEC 27003**: Offers guidance on implementing an ISMS, explaining how to establish and operate an **ISMS based on ISO/IEC 27001**.
- **ISO/IEC 27004**: Focuses on **measuring the effectiveness** of ISMS, including methods for monitoring, analyzing, and improving performance.

- **ISO/IEC 27005**: Provides guidelines for **information security risk management**, complementing ISO/IEC 27001 by offering a **structured risk management approach**.
- **ISO/IEC 27006**: Specifies **requirements for certification bodies** providing audit and certification of ISMS in compliance with ISO/IEC 27001.
- **ISO/IEC 27007**: Provides guidance for conducting **internal audits of an ISMS**.
- **ISO/IEC 27008**: Offers guidelines for ISMS auditors on **assessing the effectiveness of information security controls**.
- **ISO/IEC 27017**: Provides guidelines for **cloud security**, supplementing ISO/IEC 27002 with additional security controls specific to **cloud computing services**.
- **ISO/IEC 27018**: Focuses on the **protection of personal data** in **public cloud** services, offering controls based on ISO/IEC 27002.

These standards **establish a strong foundation** for information security within organizations, aiding compliance with **regulatory and legal requirements** while improving **operational security efficiency**.