الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

GRADUATE DISSERTATION

Presentation with a view of obtaining an academic master's degree in the specialty

« electronic government »

Cybersecurity Governance in Algerian Institutions as a mechanism for managing information security risks

Case of: General Inspectorate of finances

Prepared by:

-REZGUI Abdeldjebar

-TAIBOUNI Ilyas

supervised by:

Dr. DERRAR Hacene

2025/2026

ABSTRACT

In the context of accelerating digital transformation within Algerian public institutions, information systems governance has become a strategic necessity rather than a technical option. The General Inspectorate of Finance (IGF), given the sensitive nature of the financial data it handles, represents a critical case for examining how cybersecurity governance is structured and implemented in the public sector.

Despite the adoption of certain security policies and procedures, field observations reveal persistent gaps in their implementation, a lack of formally defined roles and responsibilities, and the absence of a comprehensive and systematic approach to information security risk management. This reflects a significant disconnect between the theoretical principles of cybersecurity governance and their operational reality within the institution.

To address this problem, the study adopts an interpretivist epistemological stance and an inductive qualitative approach based on Action Research methodology. Data were collected through semi-structured interviews with four key stakeholders occupying strategic positions within IGF, and analyzed using NVivo software to identify recurring themes, patterns, and insights. The analysis reveals six interconnected findings: the absence of a formal cybersecurity governance framework, ambiguity in roles and responsibilities, a predominantly reactive rather than proactive security posture, weak institutional coordination, limited security awareness among staff, and the human factor emerging as the primary and most critical vulnerability within the institution.

The study concludes that effective cybersecurity governance is not solely a technical matter, but a strategic and organizational imperative. It recommends the adoption of ISO/IEC 27001 as a reference framework for establishing a formal Information Security Management System (ISMS), the deployment of a RACI matrix to formalize roles and accountability, and the integration of FMECA and EBIOS risk methodologies to shift the institution from a reactive to a proactive risk management posture. These measures are essential for ensuring the confidentiality, integrity, and availability of IGF's critical information assets within a sustainable digital transformation strategy.

Keywords: Cybersecurity Governance, Information Security Risk Management, ISO/IEC 27001, FMECA, EBIOS, Digital Transformation, General Inspectorate of Finance, Action Research, NVivo .

Résumé

Dans le contexte de l'accélération de la transformation numérique au sein des institutions publiques algériennes, la gouvernance des systèmes d'information est devenue une nécessité stratégique plutôt qu'une option technique. L'Inspection Générale des Finances (IGF), compte tenu de la nature sensible des données financières qu'elle traite, représente un cas critique pour examiner comment la gouvernance de la cybersécurité est structurée et mise en œuvre dans le secteur public.

Malgré l'adoption de certaines politiques et procédures de sécurité, les observations de terrain révèlent des lacunes persistantes dans leur mise en œuvre, un manque de rôles et de responsabilités formellement définis, ainsi que l'absence d'une approche globale et systématique de la gestion des risques liés à la sécurité de l'information. Cela reflète un écart significatif entre les principes théoriques de la gouvernance de la cybersécurité et leur réalité opérationnelle au sein de l'institution. Pour répondre à cette problématique, l'étude adopte une posture épistémologique interprétiviste et une approche qualitative inductive basée sur la méthodologie de la recherche-action. Les données ont été collectées au moyen d'entretiens semi-structurés avec quatre parties prenantes clés occupant des postes stratégiques au sein de l'IGF, et analysées à l'aide du logiciel NVivo afin d'identifier les thèmes récurrents, les tendances et les insights significatifs.

L'analyse révèle six résultats interdépendants : l'absence d'un cadre formel de gouvernance de la cybersécurité, l'ambiguïté des rôles et des responsabilités, une posture de sécurité majoritairement réactive plutôt que proactive, une faible coordination institutionnelle, une sensibilisation limitée du personnel à la sécurité, et le facteur humain qui émerge comme la vulnérabilité principale et la plus critique au sein de l'institution.

L'étude conclut que la gouvernance efficace de la cybersécurité n'est pas uniquement une question technique, mais un impératif stratégique et organisationnel. Elle recommande l'adoption de la norme ISO/IEC 27001 comme cadre de référence pour l'établissement d'un Système de Management de la Sécurité de l'Information (SMSI) formel, le déploiement d'une matrice RACI pour formaliser les rôles et les responsabilités, ainsi que l'intégration des méthodologies de gestion des risques FMECA et EBIOS afin de faire évoluer l'institution d'une posture réactive vers une gestion proactive des risques. Ces mesures sont essentielles pour garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels critiques de l'IGF dans le cadre d'une stratégie de transformation numérique durable.

Mots-clés : Gouvernance de la Cybersécurité, Gestion des Risques de Sécurité de l'Information, ISO/IEC 27001, FMECA, EBIOS, Transformation Numérique, Inspection Générale des Finances, Recherche-Action, NVivo .

الملخص

في سياق التسارع الملحوظ للتحول الرقمي داخل المؤسسات العمومية الجزائرية، باتت حوكمة نظم المعلومات ضرورة استراتيجية لا خياراً تقنياً. وتُمثّل المفتشية العامة للمالية، نظراً للطابع الحساس للبيانات المالية التي تتولى معالجتها، نموذجاً بالغ الأهمية لدراسة كيفية هيكلة حوكمة الأمن السيبراني وتطبيقها الفعلي في القطاع العام.

على الرغم من اعتماد جملة من السياسات والإجراءات الأمنية، تكشف الملاحظات الميدانية عن ثغرات متواصلة في تطبيقها، وغياب لأدوار ومسؤوليات محددة بصورة رسمية، فضلاً عن انعدام منهج شامل ومنظّم لإدارة مخاطر أمن المعلومات. ويعكس ذلك فجوة واسعة بين المبادئ النظرية لحوكمة الأمن السيبراني وواقعها التشغيلي داخل المؤسسة.

للإجابة عن هذه الإشكالية، تبنّت الدراسة موقفاً ابستيمولوجياً تفسيرياً ومنهجاً نوعياً استقرائياً قائماً على البحث الإجرائي. وقد جُمعت البيانات عبر مقابلات شبه منظمة مع أربعة مسؤولين رئيسيين يشغلون مناصب استراتيجية داخل المفتشية العامة للمالية، ثم خُضعت للتحليل باستخدام برنامج NVivo بهدف استخلاص الأنماط المتكررة والمحاور الدلالية المهمة.

كشف التحليل عن ستة نتائج متشابكة ومترابطة، وهي: غياب إطار رسمي لحوكمة الأمن السيبراني، وضبابية في توزيع الأدوار والمسؤوليات، وسيادة نهج أمني تفاعلي بدلاً من النهج الاستباقي، وضعف في التنسيق المؤسسي، ومحدودية الوعي الأمني لدى الموظفين، وبروز العامل البشري باعتباره الحلقة الأضعف والأكثر عرضة للخطر داخل المؤسسة.

خلصت الدراسة إلى أن الحوكمة الفعّالة للأمن السيبراني ليست مسألة تقنية بحتة، بل ضرورة استراتيجية وتنظيمية. وتوصي الدراسة باعتماد معيار ISO/IEC 27001 إطاراً مرجعياً لإرساء نظام إدارة أمن المعلومات (ISMS) بصورة رسمية، وتطبيق مصفوفة RACI لتحديد الأدوار والمساءلة، وإدراج منهجيتَي FMECA و EBIOSلإدارة المخاطر، وذلك بهدف تحويل المؤسسة من نهج تفاعلي إلى نهج استباقي في التعامل مع المخاطر. وتُعدّ هذه الإجراءات ضرورية لضمان سرية وسلامة وتوافر الأصول المعلوماتية الحساسة للمفتشية العامة للمالية في إطار استراتيجية تحول رقمي مستدام.

الكلمات المفتاحية :حوكمة الأمن السيبراني، إدارة مخاطر أمن المعلومات، ISO/IEC 27001، FMECA، EBIOS، التحول الرقمي، المفتشية العامة للمالية، البحث الإجرائي، .NVivo

.

Acknowledgements

بسم الله الرحمان الرحيم

I would like to begin by expressing my gratitude and appreciation to Allah, the Almighty, who allowed me to walk this long path and granted me the strength and patience to spend this stage of my life in pursuit of knowledge until this humble work could be completed.

Most importantly, I would like to express my sincere gratitude to my supervisor, Dr. Hacene Derrar, and to my second supervisor at the General Inspectorate of Finance, Director Nabil Meziane, for all the assistance and support they provided throughout the completion of this work.

Dr. Hacene Derrar, thank you for your guidance and your valuable remarks and observations on this thesis.

Mr. Nabil Meziane, I would also like to express my deep appreciation for your constant support and, above all, for your insightful remarks, especially regarding the professional field.

Thank you both for accompanying me through every step with patience and kindness.

To the two people who gave me life, my beloved parents:

To my father, the man who raised me to value knowledge, who did everything he could for me since my earliest days, and who contributed greatly to shaping the person I am today.

And to my mother, the woman who encouraged me to continue this journey and instilled in me determination, perseverance, and love.

Thank you, Mom and Dad. This achievement would never have been possible without you. This work belongs to you before it belongs to me.

To my brothers, Abdelbassit and Abdessamad, thank you for always being by my side.

I would also like to thank all my family for every kind word and every encouragement I received from them.

To all my friends: Ilyas, the second Ilies, Akram, Abdeljalel, issam and all my classmates with whom I spent the most beautiful two years of my life, thank you all.

And special thanks to my dear colleagues, Asma and Rahma, with whom I shared the joy of this achievement.

And finally, Alhamdulillah for everything ***Thank you all****.*

Abd el Djebar

بسم الله الرحمان الرحيم

Praise be to Allah, who blessed us with the completion of this work, guided us along the paths of knowledge, and granted us patience and strength to finish this humble effort.
I dedicate the fruit of this work with gratitude and deep loyalty to the greatest blessing in my life, the constant source of sincere prayer and the sun which enlightens my path through hardship; my parents who were always my first support and planted in me the love of knowledge and ambition. May Allah preserve them as a treasure and support. I offer them this work with gratitude and deep loyalty for everything they have done.

To my one and only brother and support Ahmed, and to my dearest sisters who are the peace and comfort I always return to, and the motivation that never fades.
To my partner in this journey, my colleague in hard work and dedication, Rezgui Abdeljabbar you are the best a ademic partner and a wonderful pair in overcoming difficulties.
Finally, I would like to express my deepest gratitude to my supervisor, Professor Hacene Derrar, whose advice and guidance had a great and lasting impact on the outcome of this work. I also thank the training supervisor, Mr. Meziani Nabil, for his valuable field support and direction.
To my lifelong friends, with whom I shared countless late nights and the challenges of student life that felt like an entire lifetime: Abdeldjebar, Jalal, Akram, Ilyas, and Issam and to everyone with whom I built unforgettable memories in the university corridors and the residence halls, with all their laughter, pressures, and dreams both big and small. Thank you for giving these two years a deeper and more beautiful meaning.
To my dear female colleagues who were like sisters to me we shared the same seats of knowledge, the bitterness of exhaustion, and the sweetness of achievement together.
Finally, to everyone who helped and supported me in completing this thesis, whether near or far, through actions or words, or even a kind word that lifted my spirits during moments of fatigue and weakness to all of you, I offer my sincerest thanks, appreciation, and loyalty.

Ilyas

Table of content

List of tables

List of figures

List of abbreviations

CIA: Confidentiality, Integrity, Availability

CIS: Center for Internet Security

CNC: Computer Numerical Control

COBIT: Control Objectives for Information and Related Technologies

DoS: Denial of Service

FMECA: Failure Mode, Effects, and Criticality Analysis

GDPR: General Data Protection Regulation

IEC: International Electrotechnical Commission

IGF: General Inspectorate of Finance

IS: Information System

ISO: International Organization for Standardization

IT: Information Technology

NIST: National Institute of Standards and Technology

PCI-DSS: Payment Card Industry Data Security Standard

PII: Personally Identifiable Information

RACI: Responsible, Accountable, Consulted, Informed

RBN: Rule-Based Bayesian Network

SOC-2: Service Organization Control 2

TOGAF: The Open Group Architecture Framework

ZDS: Zero-Subjectivity Closed-Loop Dempster–Shafer

General Introduction

In light of the great transformations witnessed by the contemporary global economy, which has become increasingly based on digital innovation, information systems governance has become one of the main pillars that organizations cannot do without, as information systems are no longer just technical operational tools, but have become a focus in formulating the strategic directions of the organization and enhancing its breathing capacity and achieving its long-term goals.

Cyber as one of the highlights This is due to the heavy reliance on digital systems and information networks, where this topic is of particular importance in Algeria, which has been witnessing technological development in many sectors during these recent years, but despite the facilities provided by this development and the improvement of efficiency and transparency, there is a noticeable increase in the volume of cyber threats that may result in significant financial losses, leakage of sensitive data and damage to the reputation of institutions.

In this context, information security risk management emerges as the main pillar within the framework of information systems governance, has a fundamental role in identifying threats and assessing the level of risks and also the development of mechanisms for prevention.

From this perspective, this study comes to highlight the reality of information security risk management within the General Inspectorate of finance as a model for the study, this institution acquires special importance given the nature of the sensitive information it deals with, and despite the adoption by the General Inspectorate of Finance of a set of security policies and procedures aimed at protecting its information systems, however, field observations and preliminary indicators suggest the existence of some gaps associated with the implementation phase, in addition to the limited adoption of a comprehensive and systematic approach to Cyber Risk Management in accordance with modern international standards and practices.

Hence the importance of this study, which seeks to analyze the reality of risk management within this body, identify strengths and shortcomings, and propose ways to improve them in a way that supports the effectiveness of information systems governance and enhances the organization's immunity in the face of increasing cyber threats.

Chapter I

Context and problematic

1. Context of the study

Information Systems (IS) governance has become an important strategic driver for organizations aiming to combine their digital transformation with their objectives, It focuses not only on technical management but also on value creation, risk management, and the identification of requirements.

This dissertation specifically focuses on the field of risk management, which is a fundamental pillar of information systems governance, cybersecurity is an important issue for individuals, organizations, and governments in Algeria and around the world. Cyberattacks can have serious consequences, including financial loss, theft of sensitive information, damage to reputation, and disruption of essential services.

Governments may also have policies in place to help protect against cyber threats and to respond to incidents when they do occur. Algeria is currently not among the countries that prioritize cyber security sufficiently Although it's a fundamental pillar in combating cybercrime at the national level, particularly in the context of the increasing technological advancements across all economic, cultural, social, and security sectors. Cybercrime is viewed as one of the adverse effects of advanced technology, posing a genuine challenge threatening the lives of individuals, communities, and national security. That significant national efforts are being made to achieve cybersecurity in the fight against cybercrime by establishing specialized structures for combating cybercrime in Algeria. Additionally, it emphasizes the necessity of international cooperation and governmental coordination to exchange information and develop joint strategies to address transnational cybercrimes, thereby contributing to a comprehensive cybersecurity framework that safeguards individuals, institutions, and nations.

However, without a robust IS governance framework the projects remain vulnerable to internal and external threats. The proactive consideration of information security risks becomes a key success in digitalization.

In today's world managing information systems is vital for organizations to succeed and last. This literature review examines the relationship between IS governance, risk management, and information security risk management in the context of sustainable digital transformation. As organizations use technologies they need to balance trying new things with reducing risks. The review begins with core concepts of IS governance, showing how frameworks like COBIT align technology with organizational goals across various sectors, it then explores the development of information security risk management,

highlighting sector-specific challenges and success factors. The chapter also reviews risk

management methods, with a focus on applying Failure Mode, Effects, and Criticality

Analysis (FMECA) to information security. Finally, by combining global and local research, this chapter proposes a conceptual framework linking theory and practice It shows how governance can ensure the security of information systems and the management of risks.

2. Research question

In light of the rapid digital transformation experienced by the General Inspectorate of Finance, information systems have become a central component in the management of various operational, administrative, and control activities. This has led to increased complexity and a rise in cyber-related threats. Despite the adoption of a set of security policies and measures by this institution, practical observations reveal persistent shortcomings in their implementation, as well as a lack of a comprehensive and systematic approach to information security risk management.

This situation reflects a gap between the theoretical framework of cybersecurity governance and its actual implementation within the General Inspectorate of Finance, where risks are often handled in a traditional or fragmented manner, without effective integration with modern governance mechanisms. This deficiency negatively impacts the effectiveness of risk control and the institution's ability to ensure the continuity of its control functions efficiently and effectively in a constantly evolving digital environment.

Accordingly, there is a need to examine the extent to which cybersecurity governance contributes to improving information security risk management within the General Inspectorate of Finance.

Based on the previous context, the following research problem is raised: To what extent does cybersecurity governance contribute to improving information security risk management within the General Inspectorate of Finance?

Secondary questions:

- What are the main information security risks affecting the information systems of the General Inspectorate of Finance?

- To what extent are cybersecurity governance practices formally structured and implemented within IGF?

- How can the adoption of international standards (ISO/IEC 27001, FMECA, EBIOS) enhance information security risk management within IGF's governance framework?

3. Objective of the study

The principle objective of this project is to analyze and know the management of risks within IT governance frameworks, using the project used by the general inspectorate of finance within the ministry of finance as a starting point for this study. The study will focus on identifying the key risk factors and the dimensions of IT governance in the digital projects, the study will focus on the following sub objectives:

- To identify the information security risks that could affect the information system of general Inspectorate of Finance.

- To provide a detailed analysis of risk management in general Inspectorate of Finance IT governance based on qualitative data from real stakeholders.

-Align IT governance practices with the cybersecurity ensuring that the management of risks supports the institutions goals.

4. Justification for the choice of the topic:

We chose the topic of this research based on our specialization in e-government, where we are interested in governance and security, which are essential in projects and the digital transformation of modern organizations. All these fields have importance in aligning information systems with the objectives of the organization.

Moreover, we noticed that in Algeria, few studies have addressed how to govern these risks and reduce them within institutions. Based on this, this research provides a contribution in a field that has not received sufficient attention, which aims to understand the management of information systems security in the organization, especially in light of the emergence of many new projects in Algeria, all related to digitalization, where new risks appear with these projects.

5. Epistemological stance

5.1. Epistemological Positioning

In exploring existing approaches to risk management in information security, we identified a gap in the literature concerning the relationship between risk management and information systems governance. Few studies address how stakeholders perceive and interpret information-related risks in complex and evolving environments such as the General Inspectorate of Finance (IGF) project. To understand this complexity, we have adopted an interpretivist epistemological posture that captures the human, organizational, and technological dynamics. Understanding phenomena requires an in-depth understanding of the practices and action logics of those involved in information security risk management.

This epistemological stance directly informs our choice of a qualitative research methodology that emphasizes active collaboration with stakeholders.

5.2. Research Approach

The methodology of this study is inductive, emphasizing observation and the analysis of empirical information. Our approach proceeds from specific observations toward broader generalization. It seeks to develop deep learning from data collected in the field, which then evolves organically. This methodology yields broader conclusions derived from observations. Consequently, the focus of the research lies in interpreting and exploring the data in order to develop the conceptual framework.

6. Relevance of the Study:

The selection of this topic is the result of extensive and careful reading, which will guide us in making informed decisions from both theoretical and managerial perspectives.

Theoretical:

This study aims to fill the gap in the current literature by identifying the risks related to information security and its impact on cybersecurity. although many studies have been conducted, few studies have taken into account the relationship between risk management and

cybersecurity, and this research will address a new area. Which provides a deeper understanding of the impact of risk management on cybersecurity governance

Managerial

From a practical point of view, these results of this study will provide concrete recommendations for improving and developing risk management practices, as they will help to develop effective strategies for identifying and evaluating cyber risks within their governance frameworks, where the organization will be able to develop its security policy and control procedures, which contributes to enhancing the level of cyber protection, reducing the likelihood of attacks and enhancing the effectiveness of security governance The long-term cyber.

7. Study framework (location):

Internship location:

The general inspectorate of finance, as a body duly authorized to control and verify the financial and accounting management of public organizations, regardless of their legal status, and sometimes even, under certain conditions, private organizations, is positioned in the collective likely to lend its assistance to magistrates wishing to be enlightened on the technical aspects of facts submitted to their assessment.

The legal basis for the quality of legal assistant recognized at the IGF, is declined in the stipulations of article 04 of Executive Decree n ° 08-272 of 06/09/2008, fixing the attributions of the IGF, which provides that the interventions of the latter may relate to "audit, studies, investigations or expert assessments of an economic, financial and accounting nature", as well as it is expressly identified in the provisions of article 07 of Ordinance n ° 96-22 of the 07/09/1996, modified and completed (defined by Executive Decree n° 97-256 of 07/114/1997), which confers on the institution the prerogatives of the judicial police to search and establish on verbal minutes, the offenses relating to the legislation of the exchanges.

MISSION and VALUES

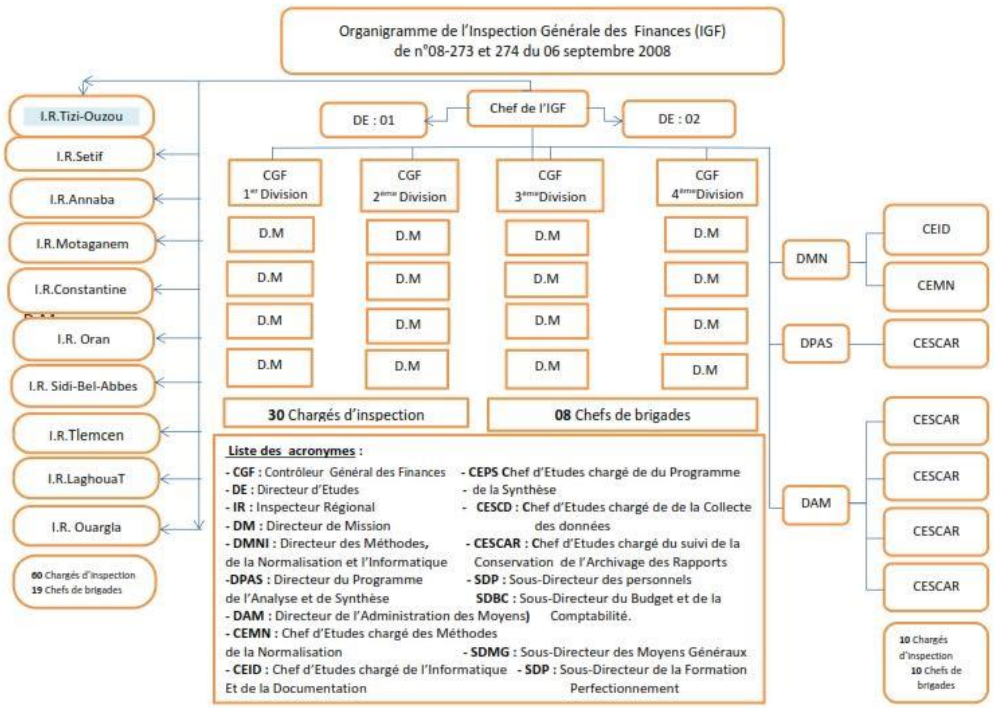
In practice, the interventions related to investigations and expert assessments are carried out according to the following modalities:

Regarding investigations: apart from the administrative investigations that it can carry out at the request of the authorized authorities, the IGF can be involved in a judicial investigation either on direct requisition from the security services, in application of Article 49 of the Code of criminal procedure (CPP) dealing with investigations in case of flagrancy, or on requisition from the judicial authority to technically assist the first during an information, or to communicate reports drawn up on the occasion of missions knowing that said reports may constitute evidence in accordance with the stipulations of Article 214 of the aforementioned code.

Regarding judicial expertise: Whether it is a civil case (Article 125 of the CPCA) or a criminal case (Article 143 of the CPP), and given its status as a specialized control body with operational agents who are sworn officials, the IGF may be required to give its opinions on the technical aspects of facts brought to the appreciation of a judge.

These opinions recorded in so-called expert reports can form the basis for the judge's decision, as the latter may also not take them into account if he considers that he cannot base his intimate conviction on them (Article 144 of the CPP).

Figure 1 : Organigram of the General Inspectorate of Finance.



Source: Document provided by the General Inspectorate of Finance (IGF).

Chapter II

Literature review and Conceptual framework

Section 1 : Literature review

In today's knowledge-driven economy, information systems (IS) have become foundational to the functioning and strategic competitiveness of modern organizations. An information system is defined as an organized socio-technical system designed to collect, process, store, and disseminate information in support of organizational decision-making and control (Pearson, 2022). As organizations increasingly rely on digital infrastructures, the governance of these systems has emerged as a critical strategic concern, particularly in the context of escalating cybersecurity threats. This literature review examines the existing body of knowledge on cybersecurity governance, information security risk management, and related frameworks, with the aim of identifying the theoretical foundations and research gaps that underpin the present study.

1.1. Cyber Governance

Studies indicate that cyber governance is concerned with the decision-making process within the cyber environment to ensure transparency and accountability in the digital sphere. It has emerged as one of the most critical issues in international relations in recent years. International organizations have sought solutions for cyber governance challenges, starting with the ratification of the Council of Europe's "Cyber Crime Convention." Furthermore, global standardization has been adopted, such as the ISO/IEC 38500:2015 standard, which describes corporate governance as a subset of IT governance. Despite these standards, there remains a lack of a framework linking cyber governance and cybersecurity as two distinct topics (Albalasa, Modjtahedib, & Abdic, 2022)

1.2. Management and Governance

Management strategies involve gathering resources and performing tasks according to the organizational structure and goals. The main considerations of this definition can be divided into four dimensions (Albalasa, Modjtahedib, & Abdic, 2022). First, management encompasses various activities and actions such as scheduling, decision-making, and assessment, and represents the most important process for an organization. Second, in order for management to function, resources are needed by combining tangible and intangible resources including money, materials, labor, and knowledge, organizational goals are achieved. Third, management makes a deliberate effort to achieve its goals, with

organizational management and human resource management representing the two key variables in this regard. Fourth, the establishment and functioning of the organization provide management with the opportunity to operate effectively. Together, these dimensions illustrate that governance and management are complementary but distinct: while management concerns the execution of tasks and the allocation of resources, governance provides the overarching framework of accountability, direction, and control within which management operate.

1.3. Cybersecurity Governance Principles

Governing, managing, and maintaining cybersecurity arrangements represent a challenge for business managers, security managers, and auditors alike. To demonstrate the business value of cybersecurity and to balance the risks associated with attacks or breaches, a set of guiding principles should be applied (Melaku, 2023) . An effective cybersecurity governance framework should be flexible and dynamic, adapting to current threats and evolving technological landscapes. It should adopt a risk-based approach, ensuring that security investments are allocated according to the actual risk exposure of the organization. Organizations should also evaluate their IT systems against recognized standards and regulations, including NIST 800-53, SOC-2, and ISO/IEC 27001, as compliance with such frameworks ensures the protection of the confidentiality, integrity, and availability of information assets. A holistic approach is equally essential, addressing people, skills, technology, processes, and governance in an integrated manner . Furthermore, cybersecurity governance frameworks should maintain a clear distinction between governance which involves directing, controlling, and monitoring security programs and management which concerns the operational implementation of security measures. Governance frameworks must also be periodically reviewed and tailored to the specific needs, resources, and risk appetite of the organization. Building a culture of cybersecurity through continuous employee education and awareness programs is indispensable, as is ensuring end-to-end governance that treats information and related technologies as organizational assets. Finally, given the borderless nature of cyberspace, collaboration and cooperation between governments, public and private sectors at both national and international levels is essential to combat cyber threats effectively (Melaku, 2023)

1.4. Three Pillars of Cybersecurity

A complete security plan relies on the collaboration of three fundamental elements (StartechGcc, n.d.) . The first pillar is Process, which is critical to effectively implementing cybersecurity strategy and architecture. It focuses on developing frameworks and procedures that prevent cyberattacks through effective management systems, policies, security audits, and gap analysis. Organisations must understand their systems and identify the data that needs to be protected, focusing on identifying vulnerable data and systems and determining processes to help secure the network (Davies, n.d.) The second pillar is Technology, which represents the most common aspect of developing and maintaining the security of digital systems and infrastructures. Cybersecurity professionals must use the latest technologies to design secure systems and processes that effectively protect the network (Davies, n.d.) . The third pillar is People, as individuals who use data and systems within an organization must adhere to key data protection principles such as setting strong passwords, avoiding suspicious external links and email attachments, and making regular backup copies of data (Mohammed, 2023). These three pillars are interdependent: a weakness in any one dimension can undermine the effectiveness of the other two, which is why a holistic approach to cybersecurity governance must address all three simultaneously.

1.5. Cybersecurity Goals

According to (Alhalima, n.d.) the objective of cybersecurity is to guard information from being stolen, compromised, or attacked. Cybersecurity is measured by at least one of three goals: protecting the confidentiality of information, preserving the integrity of data, and promoting the availability of information for authorized users. These three goals form the Confidentiality, Integrity, and Availability (CIA) Triad, which constitutes the foundational model of all information security programs. The CIA Triad is a security model designed to guide policies for information security within organizations, and is sometimes referred to as the AIC Triad to avoid confusion with the Central Intelligence Agency (Alhalima, n.d.)

Confidentiality refers to the efforts of an organization to ensure that data is kept secret or private, by controlling access to prevent the unauthorized sharing of information whether intentional or accidental. Any unauthorized access to sensitive data such as personally identifiable information (PII), trade secrets, or national security secrets constitutes a breach of confidentiality (Ryan, 2023). Integrity involves ensuring that data is trustworthy, accurate,

and free from tampering, whether accidental or malicious. The integrity of data is maintained only when it is authentic and reliable, and a method commonly used to verify integrity is non-repudiation, which ensures that the origin and receipt of data cannot be denied (Nweke, 2017). Availability, finally, refers to ensuring that data and systems are both accessible and operational for authorized users when needed. Availability can be compromised through attacks such as Denial of Service (DoS), and is mitigated through redundant systems, data backups, and load balancing mechanisms (Understanding the CIA triad in cybersecurity, 2024)

1.6. FMECA in Information Security Risk Management

The application of Failure Mode, Effects, and Criticality Analysis (FMECA) in cybersecurity has expanded in recent years, particularly in the context of industrial systems and smart manufacturing environments. As manufacturing technologies become increasingly interconnected, researchers have explored methods to adapt traditional reliability analysis techniques to assess cyber risks in industrial control systems (Zhang, 2023) highlights that the cybersecurity of computer numerical control (CNC) machine tools has become a major concern due to the growing dependence on smart manufacturing and industrial networks, noting that dedicated risk assessment methods specifically designed for CNC systems remain limited and that domain-specific threat probability databases are still lacking.

More broadly, FMECA has been widely applied in engineering and industrial risk assessment as a structured methodology for identifying failure modes and evaluating their criticality (Stamatis, 2003). Its adaptation to information security contexts has gained increasing attention in recent years, with researchers exploring its application across industrial control systems, healthcare information environments, and critical infrastructure protection. However, its application in the context of public financial institutions in developing countries remains largely unexplored, representing a key methodological contribution of the present study. By integrating FMECA with the CIA Triad framework and ISO/IEC 27005 risk management guidelines, this research seeks to operationalize risk assessment in a manner that is both methodologically rigorous and contextually adapted to the governance challenges specific to IGF.

To address the limitations identified in the existing literature, (Zhang, 2023) proposes a risk quantification framework that integrates FMECA with a Rule-Based Bayesian Network

(RBN), supported by the Zero-Subjectivity Closed-Loop Dempster–Shafer (ZDS) theory. In this framework, experts evaluate FMECA parameters for a set of cyber threats, after which the ZDS theory is used to fuse expert opinions and reduce subjectivity in the assessment process. The aggregated results are then employed to drive a Bayesian network that performs hierarchical probabilistic modelling of cybersecurity risks. The study demonstrates that the use of ZDS significantly improves the robustness of evidence aggregation in cyber risk assessment, and identifies Denial-of-Service (DoS) attacks targeting network communications as representing the highest level of risk within CNC systems. Overall, this work demonstrates how integrating FMECA with probabilistic reasoning techniques can improve the identification and quantification of cybersecurity risks in complex environments, thereby supporting the development of more effective security strategies.

1.7. Cybersecurity Governance in the Algerian Context

Algeria's digital transformation agenda has accelerated significantly in recent years, with major public institutions undertaking large-scale digitalization projects across administrative, financial, and social sectors. However, academic research on cybersecurity governance within the Algerian public sector remains scarce relative to the scale of this transformation. (Mekimah & Zerdoudi, 2022) examined the implementation of Information Security Management Systems (ISMS) in an Algerian industrial context, highlighting significant gaps between policy adoption and practical implementation, and noting that international standards such as ISO/IEC 27001 are referenced but rarely operationalized in a systematic manner. Similarly, (Soumiya & Eddine, 2022), identified the predominance of informal and underdeveloped governance practices across Algerian public institutions, attributing these deficiencies to a lack of binding regulatory frameworks, limited technical expertise, and insufficient institutional pressure to adopt recognized international standards. These findings suggest that while awareness of cybersecurity governance is growing within the Algerian public sector, systematic and formalized governance frameworks remain largely absent a structural gap that the present study seeks to examine in greater depth through the empirical case of the General Inspectorate of Finance (IGF).

1.8. Research Gap

The review of existing literature reveals several important observations that define the theoretical and empirical contribution of this study. First, while cybersecurity governance

frameworks such as COBIT 2019, ISO/IEC 27001, and the NIST Cybersecurity Framework have been extensively studied in Western and private sector contexts, their application within Algerian public financial institutions remains largely unexamined. The specificity of the public sector characterized by bureaucratic constraints, limited resources, and heightened accountability requirements calls for dedicated empirical investigation that existing literature has yet to provide.

Second, existing studies on information security risk management in developing countries tend to focus predominantly on technical solutions, with limited attention devoted to the organizational, cultural, and human dimensions of governance. Yet as the present study demonstrates, it is precisely these dimensions role ambiguity, informal coordination, and limited security awareness that constitute the most critical vulnerabilities in the institutional context under study.

Third, the integration of qualitative methodologies such as Action Research and computer-assisted qualitative data analysis via NVivo in studying cybersecurity governance within public institutions remains rare in the existing literature, particularly in the North African and Algerian context. Most available studies rely on quantitative surveys or purely descriptive approaches, leaving a significant methodological gap in terms of in-depth, interpretive understanding of governance practices from the perspective of institutional actors.

This study therefore seeks to fill these gaps by providing a rigorous qualitative analysis of cybersecurity governance practices at IGF, examining how governance mechanisms contribute or fail to contribute to improving information security risk management, and proposing evidence-based recommendations grounded in internationally recognized standards and frameworks.

Section 2 : Conceptual framework

2.1. Information system:

An Information System (IS) is an organized network of interrelated components that collaboratively produce, distribute, and process information. It functions as a formal, socio-technical organizational system aimed at collecting, processing, storing, and disseminating information. From a socio-technical standpoint, an information system consists of four key

components: tasks, people, structure (or roles), and technology (Kroenke, 2015)
Within an organization, the system can be categorized into three subsystems: the decision system, the information system, and the operating system, each providing essential services to the others

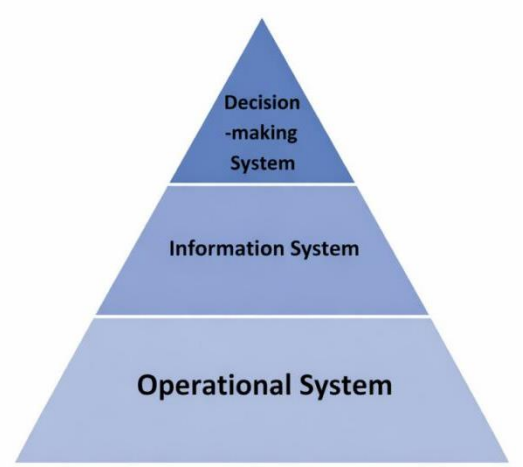
2.1.1. Decision-Making System

The Decision-Making System occupies the highest level of the organizational hierarchy, representing the strategic leadership and defining the overall goals while guiding all operations. This system includes the executive team and key decision-makers responsible for developing strategic plans, making major decisions, and allocating the resources necessary to achieve the organization's objectives. By providing clear direction and effective control, the Decision-Making System ensures the organization remains committed to its vision and capable of adapting to both internal and external changes.

2.1.2. Operational System

The Operational System encompasses all daily operational activities and processes within the organization, covering functional departments such as production, sales, marketing, finance, and human resources. This system is responsible for executing the organization's core functions and delivering products or services to customers. It relies on information provided by the Information System to carry out day-to-day operations, including order processing, service delivery, customer communication, and transaction management. The Operational System plays a key role in translating strategic objectives into tangible results, thereby directly contributing to the organization's success.

Figure 2: *Information system pyramid*



Source: developed by us

2.2. Information System Governance:

Governance refers to a group of organizations that make decisions aimed at managing a specific area of activity. This governance encompasses an integrated system and dynamic processes, including governance procedures, management activities, and more. The term governance is used to describe an organization's ability to organize and manage its internal operations in a way that prevents conflicts of interest, while maintaining a clear distinction between stakeholders such as shareholders and other actors (COBIT 2019 Framework, released by ISACA).

2.2.1. **IT Governance**:

No universal definition of the term "IT Governance" exists. A review of the literature has shown that defining this term is challenging due to its multidisciplinary nature; therefore, different researchers have proposed various definitions.

According to (Joseph & L), IT governance encompasses a set of processes, mechanisms, and best practices that ensure informed decision-making regarding information technology within an organization. It involves stakeholder participation, risk management, transparency, and the alignment of business and technological objectives. By adopting a robust IT governance

approach, organizations can improve their agility, performance, and capacity to address the challenges associated with digital transformation

According to (ITGI, 2006), the responsibility for IT governance lies with the executive management and the board of directors. It encompasses leadership, organizational structure, and processes that ensure IT effectively supports the organization's goals and strategies.

IT governance also covers organizational processes, accountability mechanisms, leadership activities, and structures established within the organization to ensure that IT activities remain aligned with the overall objectives and strategy of the firm. This includes the responsibility of executive management and the board of directors to manage and oversee IT, with the implementation of structures and processes that enable IT to effectively support the business goals.

2.2.2. The 5 domains of IT governance

To support the effective governance of information systems, the COBIT framework identifies five key strategic areas that constitute the main domains of IS governance

Figure 3 The Pillars of IT Governance.

Source: martin gibbs

a-**Strategic-IT alignment**

refers to the degree of congruence between information technology functions and business functions in supporting the overall objectives of the organization (Sabherwal R. S., 2019). It also involves the ability of IT leaders and business leaders to work in a unified strategic direction (Sabherwal & Chan, 2001). From a capability-based perspective, Strategic-IT alignment is considered the utilization of IT to enhance performance through social and structural integration within the organization (Preston & Karahanna, 2009)

b- Value Delivery

Every enterprise will have a governance objective aimed at creating value. Value creation refers to realizing benefits at an optimal resource cost while optimizing risk management. The goals cascade is important because it allows for the prioritization of implementation, improvement, and assurance of enterprise IT governance based on the enterprise's (strategic) objectives and the associated risks (cobit 5)

c- Risk Management

Risk IT is a set of proven, real-world practices that helps enterprises achieve their goals, seize opportunities and seek greater return with less risk. It works at the intersection of business and IT and allows enterprises to manage and even capitalize on risk in the pursuit of their objectives.

It extends COBIT, the globally recognized IT governance framework, and saves time, cost and effort by providing enterprises with a way to focus effectively on IT-related business risk.

d-Resource Management

Aims to ensure the availability of necessary IT capabilities and resources including human, technological, and financial to support the implementation of IT strategies. It also includes employee training and competency development to maintain a high level of skill and proficiency among IT teams.

e-Performance Measurement

Establishes monitoring frameworks to assess the effectiveness of IT, ensuring continuous

improvement. Without measurable KPIs, the other domains cannot achieve their intended outcomes.

2.2.3. The Importance of IT Governance:

According to (Al-Kassar, 2019). It contributes in particular to raising the level of operational performance within these organization, as it works on:

1. Maintain high-quality information that supports business decisions.
2. Generate and create value for the organization through the best use of information technology.
3. Apply strategic goals and gain business benefits through early and effective use of IT.
4. Keep the risks associated with information technologies within a reasonable level.
5. Dealing with the increase in the amount of information in terms of the way institutions choose the correct and reliable information associated with their work, which in turn will contribute to making effective and efficient decisions, and the way this information is managed.

2.2.4. Risk Management as a Core Governance Domain:

Specialized authors define in their writings risk management as being “the process of identifying the vulnerabilities and threats from the framework of an organization as well as designing procedures in order to minimize the impact of them on IT resources”. The risk on organization level cannot be eliminated; it will exist all the time; the management of the organization is responsible with minimizing it to an acceptable level. Risk management should be a continuous process which begins by assessing the level of exposure of the organization and identifying the main incident risks. Once identified, risks have to be minimized using control procedure and finally residual risk should be adjusted at acceptable level.

2.3. Information security and risk management

2.3.1. Fundamentals of information security:

In today’s digital era, the concepts of information security have become a major matter of global interest and importance where Information security encompasses the safeguarding of

data against unauthorized access, misuse, exposure, alteration, or obliteration. It entails the systematic adoption of strategic policies, procedural controls, and technological safeguards to uphold the confidentiality, integrity, and availability (CIA triad) of critical assets.

Information security encompasses a set of preventive and corrective measures, both technical and organizational, designed to ensure the integrity, confidentiality, and availability of data, hardware, and software, as well as the protection of individuals involved in their management (Baggia, 2025)

2.3.2. The importance of Information security:

The importance of information security is based on several key aspects (Mekimah & Zerdoudi, 2022) .

•**National and economic security**: Accuracy and relevance of information are relevant to military and economic spheres.

•**Risk management**: Nations have to apply robust security measures to anticipate and avoid threats caused by interactions with other players.

•**Securing electronic environments**: Establishing a secure electronic environment is critical to the private sector as well as the public sector.

•**Expansion of digital technologies**: Growing use of electronic applications calls for implementation of robust security measures.

•**Protection of critical infrastructure**: Safeguarding information networks to provide business continuity is essential.

•**Technological progress and cybercrime**: Technology continues to grow and expand as a discipline of information technology, and new opportunities are being created, but also more exposure to cybercrime.

2.3.3. Brief History of Information Security and Cybersecurity (Cisco)

The first iteration of the internet emerged in the 1960s as an intranet. This intranet was called ARPANET. According to the History Computer website, ARPANET is an acronym for “Advanced Research Projects Agency Network”. An intranet is a system of files and data that

the United States Department of Defense primarily utilizes. ARPANET was only accessible to people working within the network infrastructure utilizing the TCP/IP protocol suite.

ARPANET was the precursor to the internet, but researchers quickly realized the potential for unauthorized access and data theft. One of the first examples of security threats was a virus called “Creeper.” Rebecca Bales of History Computer writes, “Creeper was written in 1971 by BBN computer programmer Bob Thomas”. As threats emerged, so did prevention methods.

The term “Cybersecurity” was coined by William Gibson in 1983 in his novel entitled Neuromancer. Three years later (in 1986), the U.S. passed “The Computer Fraud and Abuse Act.” Digital criminal activity was new and unregulated, and protocols were necessary to mitigate these threats. Justice.gov states, “As technology and criminal behavior continue to evolve, however, it also remains important that the CFAA be applied consistently by attorneys for the government and that the public better understand how the Department applies the law”.

In the 1990s, the rise and expansion of the internet also expanded its vulnerabilities. In 1995, the first Secure Sockets Layer (SSL) Protocol was developed. According to an article published by the SSL support team, “SSL/TLS uses certificates to establish an encrypted link between a server and a client. This allows sensitive information like credit card details to be transmitted securely over the internet”. Ultimately, implementing the usage of encryption offered secure online transactions and communications for businesses.

Cyberattacks became more sophisticated in the early 2000s and 21st century. Estonia experienced a cyberattack, highlighting the need for national-level cybersecurity. On April 26th, two nights of riots and looting erupted after a USSR monument called the “Bronze Soldier” was scheduled to be relocated. This cyberattack evolved from false claims, anger-triggering spam bots, and inciting riots to exacerbate network functions.

According to an article written by Damien McGuinness of BBC News, “Cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news”. In 2010, Stuxnet was another dangerous example of cyber warfare.

Joshua Alvarez of Stanford University writes, “Stuxnet was the name given to a highly complex digital malware that targeted and physically damaged Iran’s clandestine nuclear program from 2007 until its cover was blown in 2010 by computer security researchers”. This software controlled physical infrastructure. Although the Bush administration created this malware,

President Obama released this malware while simultaneously demanding Iran open itself up to nuclear negotiations. This negatively impacted Iran's nuclear program.

The growing use of IOT devices has introduced new vulnerabilities. Businesses and consumers aim to mitigate security breaches by implementing tools such as Multi-Factor Authentication (MFA), increased use of blockchain, quantum-resistant encryption, AI-driven security systems, and digital tools that utilize system configurations and protocols.

Many of these tools can be found in the form of System Information Event Management software (SIEMs), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or AI-based IDS systems. Many businesses have begun implementing Zero Trust Architecture, which focuses on continuous verification instead of a perimeter defense. As the threat persists and expands, so do the tools and protocols used to secure systems and data integrity.

❖ **The difference between information security and cybersecurity**

Table 1: The difference between information security and cybersecurity

Aspect Cybersecurity	**Information Security (InfoSec)**	**Cybersecurity**
Definition	Protects all forms of information digital, physical, and verbal from unauthorized access, alteration, disclosure, and destruction.	Focuses on protecting digital systems, networks, and data from cyber threats such as hacking, malware, and phishing.
Scope	Broader scope including all information assets, covering both digital and non-digital formats.	A specialized subset of InfoSec that deals exclusively with digital assets and online environments.
Threat Landscape	Encompasses a wide range of risks: insider threats, physical theft, human errors, and cyber incidents.	Concentrates on cyber-specific threats like cyberattacks, data breaches, malware infections, and phishing scams.

Key Principles	Emphasizes the core principles of confidentiality, integrity, and availability (CIA).	Uses digital security controls such as firewalls, encryption, intrusion detection, and endpoint security measures.
Examples	Securing physical documents, implementing access control policies, and protecting verbal communications	Deploying antivirus software, managing network firewalls, and using encryption protocols for data transmitted over the internet.

Source: Developed by us based on theorical framework

2.3.4. The core criteria of information security (The CIA triad)

According to (Death, 2023) Information security relies on three pillars known as the CIA Triad: Confidentiality, Integrity, and Availability, the preservation of which is defined in ISO/IEC 27000.

A-Confidentiality

Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

For example, those who work with an organization's finances should be able to access the spreadsheets, bank accounts, and other information related to the flow of money. However, the vast majority of other employees and perhaps even certain executives may not be granted access. To ensure these policies are followed, stringent restrictions have to be in place to limit who can see what.

b-Integrity

Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.

For example, if your company provides information about senior managers on your website, this information needs to have integrity. If it is inaccurate, those visiting the website for

information may feel your organization is not trustworthy. Someone with a vested interest in damaging the reputation of your organization may try to hack your website and alter the descriptions, photographs, or titles of the executives to hurt their reputation or that of the company as a whole.

A method for verifying integrity is non-repudiation, which refers to when something cannot be repudiated or denied. For example, if employees in your company use digital signatures when sending emails, the fact that the email came from them cannot be denied. Also, the recipient cannot deny that they received the email from the sender.

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.

c-availability

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.

2.4. Information security risk management:

2.4.1. Risk:

ISO 27001 defines risk as the "effect of uncertainty on objectives." This broad definition encompasses not only negative impacts like data breaches but also potential missed opportunities. The standard provides a systematic approach to risk management.

Risk is generally characterized by two fundamental components:

Probability of occurrence: the likelihood that a specific threat will materialize.

Severity of consequences: the extent of damage the event could cause if it occurs.

For example, the unauthorized disclosure of personal data to third parties could significantly harm an organization’s reputation and compromise its legal compliance.

In our conceptual framework, we adopt the standard formulation of risk as:

Risk = Threat × Vulnerability × Impact

Threat: a potential source of harm targeting organizational assets.

Vulnerability: a weakness or flaw in the system that can be exploited.

Impact: the negative effect on organizational functions or objectives.

2.4.2. **Risk management principles**:

from ISO31000 we can extract eight principles of risk management to apply to our organizations:

1. Risk management should be integrated into the organization's governance structure and activities, including strategic planning and decision-making processes.
2. The approach to risk management should be structured and comprehensive to ensure consistency and reliability in managing risks while covering all aspects of risk management, from governance to reporting.
3. The risk management model should be customized to fit the organization's internal and external needs while aligning with its strategy, objectives, and risk appetite.
4. Risk management leaders should involve various stakeholders to consider diverse perspectives and expertise and promote active participation in the risk management process to enhance understanding and commitment.
5. Risk management should be a dynamic process responsive to change, ensuring that risks are continuously identified, assessed, and managed as the risk landscape evolves.
6. Risk-based decisions should be based on the best available information, including empirical data, experience, stakeholder feedback, and expert judgment.
7. Risk management leaders should recognize the influence of human behavior, implicit bias, and cultural factors on all aspects of risk management.
8. Risk management practices should continually improve through learning and experience to respond to emerging risks and evolving business environments.

2.4.3. Types of information security risks:

a. Technical Risk (SentinelOne, n.d.)

Data security risks threaten the integrity and confidentiality of organizational data, whether stored on-premises or in the cloud. These risks include data breaches, accidental exposure, and

data loss. To protect data, organizations need to implement encryption, data access control, and regular backups to ensure data availability and prevent unauthorized access.

b. Human-Centric Risks

(Proofpoint, 2025)Voice of the CISO report found that three in four (74%) chief information security officers (CISOs) said human error was their top cybersecurity risk. This reveals significant growth from last year's 60% of CISOs expressing this sentiment. The study also found a key gap between CISOs and the boardroom. Board members were less likely (63%) to point to human error than CISOs, which shows that CISOs should focus on educating leadership as well as employees. Several of the top causes for data loss events in the survey were related directly to employees. The top response (42%) was negligent insider/employee carelessness, such as an employee misusing data. Other reasons included a malicious or criminal insider (36%), stolen employee credentials (33%) and lost or stolen devices (28%).

c. Organizational & Compliance Risks (Stapleton, 2025)

Compliance risk means the exposure of an organization to legal penalties, financial and material losses, and reputational damage if it fails to comply with applicable industry standards, regulations, laws, and internal policies. Managing compliance risk is not just a legal obligation; it is a strategy for the sustainability and success of an organization, whether it is a public or private organization, a profit or non-profit organization, or state or federal government departments.

Compliance risk spans external regulations and laws, as well as internal policies and procedures, including data protection, environmental laws, industry-specific regulations, and financial reporting. For example, organizations operating in the healthcare industry must comply with the Health Insurance Portability and Accountability Act (HIPAA), and organizations that manage credit card data must comply with the Payment Card Industry Data Security Standard (PCI DSS). Other notable industry standards include FDA, IEEE, API, AML, and regulations such as GDPR, SOX, and SOC.

d. Physical & Environmental Risks

Physical threats are device loss, improper access, and disasters. Lost laptops or drowned data

Centres (ISO, 2019) lead to disruptions. Mitigation includes encryption, biometric controls for access, and geo-redundant backup.

e. Emerging Risks

New risks are revealed by emerging technologies. Cloud misconfiguration, estimated to be responsible for 99% of cloud breaches until 2025 (Gartner, 2021), expose sensitive data. AI created deepfakes, like the $25M CEO scam (Yeung & Magramo, 2023) enable high-profile frauds. IoT

vulnerabilities, found in 57% of all devices (HP Wolf, 2024) provide entry points.

Minimizing risks is by AI-detection technology and cloud security posture management (CSPM).

2.4.4. Risk calculation (MetricStream, n.d.)

Here's a step-by-step example of calculating a risk score:

- **Identify the Risk:** Potential data breach in a financial institution.
- **Assess the Likelihood:** Based on historical data, assess the likelihood as high (e.g., 0.8 on a scale of 0 to 1).
- **Assess the Impact:** Estimate the potential impact as severe (e.g., financial loss of $1 million).
- **Calculate the Risk Score:** Use the formula: Risk Score = Likelihood × Impact. In this case, Risk Score = 0.8 × $1 million = $800,000.
- **Evaluate and Prioritize:** Compare this risk score against others to determine priority.

Visual Aids or Charts to Illustrate the Process:

- A probability-impact matrix showing the plotted position of the data breach risk
- A flowchart detailing the steps in the risk scoring process

2.4.5. The process of risk management((Thomas, n.d.)

The risk management process is a framework for the actions that need to be taken to keep an organization safe from threats beyond their risk appetite. It consists of five key steps that form a continuous cycle:

Step 1: Identify the Risk

Identify and list every potential risk that could affect your organization, including internal and external factors. This foundational step ensures no significant threat is overlooked.

The initial first step in the risk management process is to identify the risks that the business is exposed to in its operating environment. Risks can arise in many areas:

- Legal risks (e.g., lawsuits or regulatory penalties)
- Environmental risks (e.g., natural disasters or climate change impacts)
- Market risks (e.g., market fluctuations or increased competition)
- Regulatory risks etc. (e.g., new laws or compliance requirements)
- Operational risks (e.g., internal process failures or system outages)
- Strategic risks (e.g., poor business decisions or industry disruptions)
- Reputational risks (e.g., negative publicity or loss of customer trust)

It is important to identify as many of these risk factors as possible. In a manual environment, these risks are noted down manually. If the organization has risk management solutions in place, all this information can be directly inserted into the system. The advantage of this approach is that these risks are now visible to every stakeholder in the organization with access to the system.

The advantage of this approach is that these risks are now visible to every stakeholder in the organization with access to the system. Instead of this vital information being locked away in a report which must be requested via email, anyone who wants to see which risks have been identified can access the information in the risk management system.

Step2: Analyze the Risk

Examine each identified risk in detail to understand its nature, scope, and potential impact. Determine how and where the risk could affect the organization, and assess factors like causes, dependencies, and potential consequences.

Once a risk has been identified it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the organization.

To determine the severity and seriousness of the risk it is necessary to see how many operational functions the risk affects.

There are risks that can bring the whole business to a standstill if actualized, while there are risks that will only be minor inconveniences in the analysis.

Key considerations during risk analysis include:

- What is the likelihood of this risk occurring?
- What would be the impact if it does occur?
- Which business processes or departments would be affected?
- What are the root causes or contributing factors?
- What controls or mitigations are currently in place, and how effective are they?

In a manual risk management environment, this analysis is done at a slower pace than when a risk management solution is implemented. Using this system to map risks to different documents, policies, procedures, and business processes means you will already have a risk management framework to help you evaluate risks the effects of each risk.

Step 3: Evaluate the Risk or Risk Assessment

Assess each analyzed risk to determine its priority level. This step, (often called risk assessment) involves assigning a likelihood and impact level to each risk and then combining these to prioritize risks from highest to lowest concern.

Risks need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on their severity. For example, a risk that may cause some inconvenience is rated ‘low’, while risks that can result in catastrophic loss are rated the highest.

Ranking risks allows the organization to gain a holistic view of the risk exposure of the whole organization. The business may be vulnerable to several low-level risks, but it may not require upper management intervention. On the other hand, just one of the highest-rated risks is enough to require immediate intervention.

There are two types of risk assessments:

Qualitative Risk Assessment

Many risk assessments are inherently qualitative. This is because, while we can derive metrics from the risks, most risks are not quantifiable. For instance, the risk of climate change that many businesses are now focusing on cannot be quantified as a whole; only different aspects of it can be quantified.

For this reason, there needs to be a way to perform qualitative risk assessments while still ensuring objectivity and standardization in the assessments across business units.

Quantitative Risk Assessment

Finance-related risks are best assessed through quantitative risk assessments. Such risk assessments are common in the financial sector because the sector primarily deals in numbers. This includes money, metrics, interest rates, or any other data points critical for risk assessments.

Quantitative risk assessments are easier to automate than qualitative risk assessments and are generally considered more objective. Go in more depth on this topic in our article, "Bringing Quantitative Risk Analysis to Enterprise Risk Management".

Step 4: Treat the Risk

Decide on and implement the appropriate risk response for each significant risk. In this step, you develop action plans to mitigate risks, avoid them, transfer them (e.g., through insurance), or accept them if they fall within your risk appetite.

Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs. In a manual environment, this entails contacting every stakeholder and then setting up meetings so everyone can talk and discuss the issues.

The problem is that the discussion is broken into many different email threads, across different documents and spreadsheets, and many different phone calls.

In a risk management solution, all relevant stakeholders can be sent notifications from within the system. Discussion regarding the risk and its possible solution can take place within the system.

Upper management can also keep a close eye on the solutions being suggested and the progress being made within the system. Instead of everyone contacting each other to get updates, everyone can get updates directly from within the risk management solution.

Step 5: Monitor and Review the Risk

Continuously track identified risks and review the effectiveness of your risk management measures. This final step ensures that risk levels remain within acceptable ranges and that any changes in circumstances are accounted for promptly.

Not all risks can be eliminated, and it is inevitable that some risks will always be present. Market risks and environmental risks are just two examples of risks that always need to be monitored.

Under manual systems, monitoring happens through diligent employees. These professionals must ensure they keep a close watch on all risk factors. In a digital environment, the risk management system monitors the entire risk management framework of the organization, immediately alerting teams to any risk changes with less room for human error.

2.4.6. ISO 2700 Family: Core Standards & Sustainability Links

The ISO 27000 series provide globally recognized frameworks for Information Security Management Systems (ISMS).

However, in order to conduct a unified effort to protect information, the International Organization for Standardization (ISO) recommends the ISO/IEC 27001 standard, published in 2005. While ISO/IEC 27001 is now considered the reference framework for any stakeholder involved in developing an information system security policy, many misunderstandings still remain regarding its adoption.

2.4.6.1. ISO 2700 Family

The ISO 27000 series provide globally recognized frameworks for Information Security Management Systems (ISMS). These standards are critical for aligning information security

with sustainability goals like energy efficiency, compliance, and ethical governance.

Key ISO 27000 Standards

Table 2 : shows ISO 2700 Family

Standard	**Purpose**
ISO/IEC27001	Requirements for establishing, implementing, and maintaining an ISMS.
ISO/IEC27002	Guidelines for selecting security controls (encryption, access control).
ISO/IEC 27005	Risk management framework for ISMS.
ISO/IEC 27009	Sector-specific adaptations of ISO 27001 (healthcare, energy sectors)
ISO/IEC 27013	Guidance on integrating ISO 27001 with ISO 20000 (IT service management).
ISO/IEC 27014	Governance of information security
ISO/IEC 27032	Guidelines for cybersecurity in cyberspace.

Source:Developed by us

2.4.6.2. PCI-DSS (Payment Card Industry Data Security Standard):

According to (Khan, 2022) The PCI-DSS standard is a widely acceptable set of guidelines that provide procedures and policies on optimizing the security of cash, debit, and credit card transactions to protect cardholders against misuse of their personal information . This standard focuses on encryption, access control, and regular network monitoring to prevent data breaches during transactions. In addition, it provides comprehensive frameworks, tools, support resources, and measurements to ensure that the information of cardholders is safe. PCI-DSS is mandatory for organizations such as financial institutions, service providers, as well as merchants that process, store, or transmit credit card data. Failure to comply with the standards leads to severe penalties in the form of legal action.

2.4.6.3. GDPR (General Data Protection Regulation):

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. (GDPR, n.d.)

The GDPR has a significant effect all around the globe as its broad territorial application and being taken as golden standards to regulate similar issues in different jurisdictions (Cedric Ryngaert, 2020)

2.4.6.4. Control Objectives for Information and Related Technologies (COBIT) :

COBIT is a cybersecurity framework that was developed by the Information Systems Audit and Control Association (ISACA) for governing and managing organisational IT environments. It provides a set of principles, practices, and processes for effective IT governance and management, including cybersecurity (Reuben-Owoh & Haig., 2025) COBIT defines the design factors that should be considered by each enterprise to build a best-fit governance system focusing on the context, objectives and needs of the enterprise (Bilgin Metin, 2024) . COBIT defines the components to build and sustain a governance system as follows: processes, policies and procedures; organizational structures; information flows; skills; infrastructure; and culture and behaviors (ISACA, 2019)

2.4.6.5. CIS Critical Security Controls (Khan, 2022) :

The framework is essential because it focuses on the small number of actions that can be worked upon to prevent or reduce cybersecurity risk. The Center for Internet Security CIS Critical Security Controls are guidelines that are prioritized to properly position an organization against cyber-attacks and form an in-depth defense of specific and actionable best practices to mitigate the attacks. The SANA Institute initially developed the framework . However, it is currently managed by the Center for Internet Security and produced by technology experts to create a globally accepted security best practice.

2.4.6.6. The Open Group Architecture Framework (TOGAF):

TOGAF (The Open Group Architecture Framework) is an enterprise architecture framework used to design, plan, implement, and manage information technology architectures throughout the organization. TOGAF is designed to provide systematic structural guidance in the development of enterprise architectures, with the primary goal of improving organizational efficiency and effectiveness through better IT integration and management (Hidayat, Indrajit, & Dazki, 2024) . The TOGAF is a framework for Enterprise Architecture. It may be used freely by any organization wishing to develop an Enterprise Architecture for use within that organization (The Open Group Standard)

2.4.7. The Impact of Digital Transformation on Risk Management

Digital transformation significantly impacts risk management by introducing new categories of risks, such as cybersecurity and data privacy threats, which compel organizations to evolve their traditional risk management practices into more dynamic and technology-driven frameworks. (Alnawaiseh & Al-Mahasneh, 2024) examine Digital transformation has redefined the concept of risk management in organizations of all walks of life. As more and more companies make use of digital technologies in their line of businesses, the face of risk has also completely changed, therefore forcing firms to reconsider their means of identifying, assessing, and mitigating various forms of risks. If one were to look back, then traditionally, risk management had its focus on operational, financial, and compliance-related risks. However, with the advent of the digital age, a whole new dimension of risks has surfaced that includes cybersecurity threats, data privacy concerns, and technological disruptions, among others. This evolution has brought a need for organizations to reshape their conventional risk management framework to not only mitigate these digital risks but also ensure business continuity in an ever-connected and data-driven world.

2.4.8. Cybersecurity governance process categories

The term “cybersecurity governance process categories” is used here to mean “processes that support the planning, implementation and maintenance of cybersecurity, which interact with standard business processes, but which comprise a series of factors rather than activities”.

Five governance process categories are recognized human, external, financial, technological, and organisational (Bilgin Metin, 2024)

Table 3: Cybersecurity governance process categories descriptions.

Process Category	**Description**
External	External process factors relate to the outside regulations, industry standards and best practices that affect the decisions of an organisation regarding cybersecurity adoption. In terms of implementation critical success factors (CSFs), they are about ensuring robust cybersecurity not only within the company but also in the 3rd parties that the organisation is associated with in order to ensure all round comprehensive protection.
Financial	Financial resources are a key determinant in a company's ability to invest in cybersecurity measures. The financial adoption factors and implementation CSFs that fall under this category relate to an organisation's financial capacity to (1) implement cybersecurity measures and (2) sustain the implemented measures successfully.
Human	This process category concerns the human factors that play a critical role in the successful adoption and integration of cybersecurity measures. For instance, without adequate security awareness among employees, phishing attempts or social engineering attacks may succeed from the threat point of view. Similarly, without the necessary awareness of employees, any technical cybersecurity measure that is implemented may fail to be effective from the security control point of view.
Organisational	This process category concerns factors related to aspects like business continuity, company reputation, customer needs, and cybersecurity governance. The organisational process category is particularly wide and multi-faceted and impacts right across business functions.

Technological	This involves the technology related issues that impact decision-making relating to cybersecurity adoption and implementation. It thus encompasses the technology aspects of decisions regarding the acquisition and deployment of cybersecurity tools and systems, and their on-going maintenance. It also encompasses cybersecurity assessment of the wider company IT portfolio.

Source: Developed by us

Chapter III

METHODOLOGICAL FRAMEWORK

In this chapter, we outline the methodological background applied to our study, having been selected specifically to be aligned with the kind of research that we are carrying out. We need this methodological foundation for the purpose of addressing rigorously our research question, which studies information security threat.

1. Presentation of the Research Methodology: Action Research (Nicodemus & Swabey, 2015)

In the context of our study, we chose procedural research as a research method, as this method is especially suitable for discovering and improving risk management practices related to information security at the General Inspectorate of Finance. Action research is an approach for investigating questions and finding solutions to problems that people confront in their everyday lives. Although most frequently associated with educational research, action research is practiced within a number of diverse disciplines. Action research serves as an umbrella term for several approaches that have emerged from different research traditions, and researchers and educators have differing perspectives about what it is, what it is for, and who can do it.

Steps of Implementation

The action research process will be structured in three cycles to embrace a comprehensive and iterative approach:

Diagnostic Phase: Represents the first step of diagnosing the current risk management practices and cybersecurity governance at the General Inspectorate of finance through in-depth interviews with key stakeholders, this stage aims to identify the prevailing problems and gaps, as well as areas for improvement

Co-Design Phase: Based on the findings of the diagnostic phase, the next step will be co-designing solutions with internal stakeholders. This phase will be focused on developing implementable and sustainable strategies and tools that overcome the challenges, ensuring the solutions are contextualized and compatible with information security requirements.

Evaluation Stage: The last step is to evaluate the Applied Solutions in order to measure their effectiveness in reducing risks and improving information security. This phase will also include collecting stakeholder feedback to evaluate and improve solutions based on their practical

impact and applicability. This methodology is particularly suitable for our research studying the integration of information security risk management and cybersecurity governance.

We justify our choice of a qualitative approach based on procedural research for the following reasons:

- Through our review of the literature, we noticed that qualitative approaches are widely used in research dealing with the intersection of Information Systems, risk management

- action research is particularly suitable for improving practices and performance within organizational contexts. In our study, we seek to identify ways to enhance information security risk management and cybersecurity governance

- action research is based on several qualitative methods of data collection, such as observation, analysis of documents, interviews. These tools will allow us to collect in-depth data on current practices, perceptions, and needs, with the aim of designing effective and sustainable interventions.

2. Data Collection Method

Data collection is a systematic process aimed at collecting and obtaining information about the variables of interest, with the aim of providing answers to research questions, testing hypotheses, evaluating results. This process is an essential element in all academic disciplines. Although the procedures used may vary from one area to another, the emphasis on accuracy, clarity and ethical integrity in data collection is crucial in all areas. The ultimate goal of data collection is to produce high-quality evidence that allows for reliable analysis and supports the drawing of sound and convincing conclusions. Regardless of whether the research is based on qualitative data, the accuracy of the data collection process is an essential element in ensuring the validity and reliability of the research as a whole. The selection of appropriate data collection techniques, their adaptation or development from scratch, as well as the development of clear protocols for their application, significantly reduce the likelihood of mistakes and enhance the reliability of the results.

The Central Position of Data Gathering in Research

Data collection is a fundamental process in the implementation of any research study, and it is a very complex process that requires careful planning, methodological consistency, patience and unwavering commitment to ensure its success. This process begins by determining the type of data to be collected in accordance with the research requirements.

2.1. Observation (Kumar, 2023)

Observation method is “a data collection method in which a person (usually trained) observes subjects of phenomena and records information about characteristics of the phenomena”. Science begins with observation and also uses observation for final validation of findings. Observation is used quite often in social sciences and is supplemented by interviews and study of records. Observation is considered as a classic method of scientific inquiry. Observation involves the investigation watching the subjects or research situation. Observation method of collecting the data is one of the oldest and this technique is used by both the scientists and social scientists. The term observation sounds to be simple and gives an impression that the collection of data through this method is easy. But it is not true in scientific investigation. There is also a criticism that this method is unreliable but by doing it more scientifically, limitations could be overcome. This method of data collection is one of the oldest methods and it can be treated as scientific only when the criteria such as objectivity, free from bias, reliability and systematization is followed. So we can say that observe means “to watch attentively in a scientific manner”. In an observational study, the current status of phenomenon is determined not by asking but by observing

2.2. Interviews

Research interviews are one of the most important sources of informational information. They allow for the collection and examination of diverse factors, including the perception, attitudes, feelings, and opinions of the interviewee. There are 3 types for Research Interview Structured Interview, Unstructured Interview and Semi-Structured Interview and we have selected the latter

Semi-structured Interview: Also known as an "in-depth" or "qualitative" interview, this type of format often includes open-ended questions. It also allows room for the inclusion of

additional questions in case the respondent brings up unexpected issues. In order to carry out this kind of interview, the interviewer employs a guide to questions that are prepared in advance, grouped under themes and in a logical order. The interviewer, nonetheless, ought not to follow the guide rigidly or even to the wording. Rather, the respondents are given the opportunity to respond in their own words and in an order that feels natural to them. The researcher directs the conversation back to the general aim when needed and asks follow-up questions at proper and natural intervals.

3. Data collection tools

Data collection tools are the instruments and techniques used to gather the necessary information for a research study. These tools are essential to ensure that the data collected is accurate, consistent, and relevant to the research objectives.

3.1. Interview guide

As part of our research aimed at studying information security risk management and cybersecurity governance in the framework of digital transformation, we chose semi-structured interviews for two reasons. Firstly, because it is a method that allows collecting rich and diverse information without being overly constrained by preconceived results. Secondly, the use of an interview guide helps to prevent the dialogue from deviating from the research goal, while at the same time allowing to explore new issues that may arise during the discussion.

a. Interview guide

The interview guide has been prepared to ensure the depth and organization of the search. It is addressed to experts and stakeholders in the field of information systems governance, digital security.

b. Justification for Sample Selection

The sample consisted of four individuals occupying strategic positions. They were selected due to their direct involvement in information systems management, data processing, and decision-making support. As such, they represent key stakeholders essential for understanding how information security risks are managed.

Data saturation will be assessed after the analysis of the interviews to ensure that the collected data are sufficient to draw meaningful conclusions and reflect recurring patterns within the scope of the study.

Table 4: The interviewees

Interviewee	Position	Date & Location	Duration
Interviewee 01	Director of Information Systems	IGF	2:15 min
Interviewee 02	Director of Statistical Information	IGF	40 min
Interviewee 03	Head of Study	IGF	1:10 min
Interviewee 04	Computer Science Engineer	IGF	30 min

Source: Developed by us

4. Data treatment

In this study, qualitative data extracted from semi-structured interviews will be analyzed using NVivo , a software specialized in qualitative research. It will assist in coding and categorizing the interview content, enabling the identification of key themes, recurring patterns, and significant insights related to cybersecurity governance and risk management.

4.1. Nvivo

Nvivo is a powerful qualitative data analysis program that allows researchers to analyze and organize large data such as interview transcripts and is characterized by other characteristics such as coding, classification and visualization of textual data, which makes it an effective tool to extract valuable information from qualitative research in this study, NVivo was used to analyze the data extracted from interviews and aggregated data. This program has helped to

systematically examine the answers, identify general topics and trends associated with information security risks and procedures for their management. It also made it possible to extract the identified risk factors, understand their effects, and ensure an accurate understanding of the challenges associated with cybersecurity risk management.

Chapter IV

Results Analysis and discussion

This chapter presents the analysis and discussion of the results obtained through qualitative interviews with key stakeholders within the General Inspectorate of Finance (IGF) as the institution under study. This research aims to explore how cybersecurity governance contributes as an effective mechanism in the management of information security within public institutions, and more specifically, seeks to study the role of cybersecurity governance in enhancing information security risk management, improving decision-making, and ensuring compliance with relevant legal standards and regulations, all within the overall framework of IT governance.

Section 1: Results analysis

1.Diagnostic of governance cybersecurity Practices at IGF:

This section provides an overview of the current information systems infrastructure within the organization under study, and its compatibility with approved information security practices. This diagnosis focuses on identifying the strengths and weaknesses of cybersecurity governance, the level of integration of technological tools with the objectives of information protection, as well as the degree of awareness of various actors of the concepts of cybersecurity and risk management. Such an analysis also contributes to building a clear understanding of the corporate context, laying the foundation for conducting an information security risk analysis in the subsequent stages.

Figure 4 : Word cloud of the general overview of the Thematic area

Source: developed by us using Nvivo

The word cloud produced by the NVivo program represents a visual representation of the most frequently present vocabulary in the contents of the study interviews, where the size of each word is directly proportional to its iterative weight in the analyzed body. Reading this cloud reveals a coherent semantic system that can be illustrated as follows:

At the level of dominant concepts, the Terms "government" and "cybersecurity" are at the forefront of the visual landscape with their striking size, which embodies the dual centrality of these two concepts in the consciousness and speech of the respondents. Their close proximity indicates that the researchers do not separate cybersecurity as a technical practice and governance as an organizational and institutional framework, but rather recognize the complementary relationship between them as a causal and structural relationship.

At the level of the semantic field of responsibility and management, the vocabulary of "responsibilities" "management" and "roles" of medium to large sizes clearly stands out, reflecting that the issue of the distribution of roles and the determination of responsibilities is a central concern in the statements of the respondents. This heavy presence is read in light of the reality on the ground, which revealed a functional ambiguity and weakness in determining the powers of each party in the security system.

As for the field of risk assessment, the vocabulary of "risks" "assessment" and "incidents" are prominently present, in a clear indication that the issue of monitoring and assessing risks and dealing with security incidents represents the most urgent functional axis in the speech of the respondents. Perhaps what is remarkable here is the simultaneous presence of the "assessment" vocabulary along with the "incidents" vocabulary, which suggests that the researchers associate the assessment with the event after the fact and not with preemption before it happened, which reinforces the result of the dominance of the interactive approach.

With regard to the field of regulatory frameworks and policies, the presence of the vocabulary of "framework" "policies" "official" and "standards" albeit in smaller sizes indicates that the researchers are aware of the importance of official frameworks and international normative references, but their relative small size in the cloud suggests that these concepts remained more present at the level of wishful thinking and suggestion than in actual practical reality.

Finally, at the level of the human dimension, the terms "employees" and "awareness" are present in the middle layer of the cloud, which confirms that the human factor forms an independent semantic link in the perceptions of the researchers, closely related to the concept

of security awareness as an indispensable protective pillar in any effective cyber governance system.

To sum up, this semantic cloud embodies a coherent cognitive structure that reveals a real field awareness of the requirements of cyber governance, as opposed to a clear applied gap between theoretical perception and actual corporate practice.

1.1 Synergies Between cybersecurity governance and management of information security:

One of the particularly important aspects emerging from the interviews is the recognition of synergies between cybersecurity governance and the effective management of information security. This is reinforced by the Information Security Manager at IGF, who states: "Cybersecurity governance and information security management go hand in hand." This statement establishes a fundamental link between both dimensions.

This perspective is also reflected in the approach of the Head of Studies, who acknowledges that "a specialized cybersecurity authority is currently being established." This indicates the necessity of implementing cybersecurity governance.

1.1.1 The human and cultural dimension of information security:

The results of the interviews revealed that the human factor represents the weakest link in the information security system, as respondents unanimously agreed that the lack of cybersecurity awareness among employees turns them from organizational assets into exploitable vulnerabilities without their awareness. An uninformed employee who opens a suspicious link or uses a weak password in fact poses a greater threat than any external technical attack, as they penetrate the security system from within.

The respondents also indicated that this cultural weakness is not limited to the technical level of employees, but extends to middle and managerial levels, which in many cases lack sufficient awareness of the implications of cyberattacks on the organization as a whole. Hence, the necessity of building a genuine organizational security culture becomes evident one that goes beyond occasional training sessions to establish a continuous and sustainable awareness that becomes an integral part of every employee’s professional identity, regardless of their position or educational level.

1.1.2 Data sovereignty as a component of information security

A specific aspect emerging from the interviews concerns data sovereignty. During the internship, the Information Security Manager emphasized that "ensuring that data remains within Algeria" is essential, noting that "storing sensitive information abroad is illegal". In this context, the organization has recently established a data center within IGF, reflecting a clear orientation toward strengthening data sovereignty and ensuring local data hosting in compliance with national legal requirements for the protection of sensitive information.

The results of the interviews conducted in this study reveal that the examined institutions are facing an imperative need to build an integrated information security strategy that goes beyond fragmented, reactive responses toward a comprehensive and systematic vision. Respondents unanimously agreed that the true starting point of such a strategy lies in establishing a formal governance framework based on recognized international standards, as no security effort can generate real impact in the absence of this reference framework, which provides coherence and institutional legitimacy to the security system.

1.1.3Towards an Information Security Strategy

This strategy is built on three interrelated and complementary dimensions. At the organizational level, it requires the precise definition of roles and responsibilities, as well as the clear identification of accountability at each stage of the security process, moving away from temporary assignments and ad hoc coordination through administrative correspondence, which most respondents described as the prevailing practice within their institutions.

At the operational level, it necessitates the adoption of a periodic and structured methodology for risk assessment, classification, and proactive mitigation, rather than waiting for security incidents to occur and then attempting to contain their impact.

At the human and cultural level, an integrated strategy requires serious investment in continuous awareness and training programs for all employees across different hierarchical levels, as no technical or organizational framework can be effective without the development of a strong institutional security culture that transforms every employee into a first line of defense rather than a potential vulnerability.

What unifies these three dimensions is the principle of continuity and periodic evaluation, ensuring that the strategy remains dynamic and adaptive in the face of an ever-evolving cyber threat landscape. This was emphasized by the Information Systems Manager, who highlighted the importance of key performance indicators (KPIs) and the RACI matrix as tools to ensure both effectiveness and accountability.

1.2. Governance and information security:

1.2.1. Regulatory and Normative Framework

An important element of information security governance at IGF lies in its anchoring within a strong regulatory and normative framework. The Information Security Manager emphasizes that: “At IGF, information security governance relies heavily on compliance with national laws such as the Personal Data Protection Law 18-07, and international standards such as ISO 27001 and ISO 27005 are used as sources of inspiration to guide auditing practices.” This dual reference to national legislation and international standards demonstrates the organization’s commitment to embedding governance practices within a structured and recognized framework, while considering international standards as a source of inspiration for improving and developing governance mechanisms.

The statement further adds that: “The governance framework is reinforced by presidential decrees and internal audit cycles to ensure that all IT processes comply with these regulations.” This reference to presidential decrees and internal audit cycles reveals the existence of formal mechanisms for monitoring and verifying compliance, which are essential for ensuring effective governance.

1.2.2. Access Control and Data Protection

Access control policies and the protection of sensitive data emerge as fundamental pillars of the security governance framework within the organization. In this context, the Chief Information Security Officer (CISO) explicitly stated: ″We ensure that access to our systems is strictly controlled and that sensitive data is fully protected. Internal traffic is also highly regulated, ensuring that only authorized personnel can access key applications and essential files.″

The adoption of this "restrictive approach" to access management reflects an acute awareness of cybersecurity risks and underscores a commitment to ensuring data confidentiality and integrity. Furthermore, this emphasis on data protection aligns with the organization's regulatory compliance strategy, particularly regarding the implementation of the requirements of Law 18-07 related to the protection of individuals in the processing of personal data, thereby establishing a sound legal and technical standing for the institution.

1.2.3. Organizational Constraints and Governance Challenges

Despite the presence of certain structural elements, the analysis reveals notable organizational constraints. The Information Security Manager notes that "the IT department's structure is highly technical in nature, as the IT Manager simultaneously assumes the roles of systems administrator and network engineer, which may limit the strategic orientation." This overlap of responsibilities reflects a dominance of the technical dimension over a broader governance perspective, which can affect the effectiveness of governance at the institutional level.
He further adds that "some staff members still confine themselves to their traditional roles without extending toward integrated governance responsibilities." This situation highlights a rigid functional compartmentalization that limits the adoption of a comprehensive and interconnected governance approach, particularly in the context of the increasing complexity of information security.

In the same context, one of the interviewees confirms that "there is still ambiguity in the coordination mechanisms between developers, users, and administrative bodies," while emphasizing the need for "clear organizational procedures to structure the digital transformation process." These findings reflect the necessity of redefining roles and clarifying processes in order to ensure better coordination and more effective support for digital transformation initiatives within the institution.

1.2.4. Digital Foundations and Structured Data

Another essential aspect of governance emerging from the interviews concerns the importance of structured data as the foundation of any digital initiative. The Information Systems Manager states that: "Digitalization represents the fundamental basis of any information system project. We cannot talk about artificial intelligence, dashboards, or data-driven decision-making without the availability of reliable and well-structured data." This statement emphasizes that

data quality and reliability are essential prerequisites for developing advanced applications and supporting decision-making processes.

This perspective highlights the importance of effective data governance as a key component of the overall governance of information systems.

1.2.5. Towards Integrated Governance

The reading of the interview results leads to a fundamental conclusion that the studied institutions are experiencing a state of governance vacuum, which casts a shadow over all aspects of the cybersecurity framework. This makes the establishment of an integrated governance system not merely a strategic choice, but an existential necessity imposed by the escalating nature of digital threats.

The respondents' accounts reveal that the absence of a formal framework does not only imply a lack of documents and policies, but rather reflects the absence of a shared vision that unifies the efforts of institutional actors and transforms security work from a fragmented individual activity into an interconnected system with clear objectives and effective control mechanisms.

The integrated governance envisioned by this study must be grounded in the firm belief that cybersecurity is not purely a technical matter delegated to the IT department alone, but rather a shared institutional responsibility extending from top management to the lowest operational levels. This was emphasized by the Information Systems Manager, who stated that true governance means strategic alignment between security objectives and the overall objectives of the institution.

Accordingly, building such governance requires, first, overcoming the pattern of temporary assignments and role ambiguity described by most respondents as a dominant feature of their institutional reality. This can be achieved by establishing clear and formalized structures that precisely define who decides, who executes, who monitors, and who is accountable, similar to what tools such as the RACI matrix enable.

Second, this governance must be framed within an international normative reference such as ISO/IEC 27001, which several respondents identified as the most suitable model to ensure the comprehensiveness of the security framework and its continuous assessment and improvement.

Third, governance must integrate the human dimension at its core rather than treating it as a peripheral element, as no regulatory framework regardless of how robust it may be can be effective without embedding a strong organizational security culture.

1.3. Information Security Risk Management

The analysis of the interviews reveals an approach to information security risk management that combines both formal and informal elements, with clear challenges observed in the systematic implementation of risk treatment processes. This section explores the different dimensions of this risk management as they emerged from the collected testimonies.

1.3.1. Risk Identification and Categorization

The interviews reveal a clear awareness within the institution of the various categories of potential risks that may affect its information systems. The Information Systems Engineer (DSI) explains that: “We face several types of risks, including unauthorized access attempts to Wi-Fi networks, surveillance systems, and administrative applications such as accounting.” This statement highlights a strong focus on unauthorized access risks, which are considered one of the main threats to information security.

The testimonies also point to additional risk categories, including: “configuration errors and lack of security updates, which are major concerns,” as well as “intrusion attempts, poor management of regular updates, and the possibility of espionage through interconnected systems.” This diversity of identified risks reflects a relatively comprehensive approach to threat identification.

The Information Systems Engineer add another dimension by mentioning a specific risk: “The use of uncontrolled USB devices is considered one of the major threats within the institution.”

1.3.2. Methodological Framework for Risk Management

The Information Systems Manager explains that the institution adopts a structured methodological framework for risk management, stating: “We implement a formal risk management process inspired by ISO 27005, which includes risk identification, assessment, treatment, and regular monitoring.” This reference to ISO 27005 reflects an effort to frame risk management practices within a recognized international standard, ensuring a systematic and standardized approach.

He further adds that: “The assessment of risk severity is also carried out in accordance with compliance requirements from national legislation and international standards,” highlighting the integration of regulatory and legal dimensions into the process of risk evaluation and prioritization. This approach reflects an increasing awareness of compliance as a key factor in determining risk treatment priorities.

1.3.3. Implementation Challenges and Organizational Limitations

Despite the existence of a structured methodological framework, the interviews reveal significant challenges in the practical implementation of risk management processes. The Information Systems Manager explains that: “The implementation of risk management procedures still faces several difficulties, including weak commitment from some departments, the presence of unawareness-based behaviours among users, as well as a lack of training programs in cybersecurity.” This statement highlights three main obstacles: limited engagement from certain units, insecure user behaviours, and insufficient cybersecurity training and capacity building.

He further adds that: “The application of risk treatment is still not consistent across all units, which creates vulnerabilities that must be addressed.” This lack of uniform implementation of risk management practices across departments represents a key weakness that affects the overall effectiveness of the institution’s security framework.

One of the interviewees points to an additional organizational issue, stating: “Poor implementation is a real threat, as there is no dedicated cybersecurity unit, and responsibility is assigned to the general IT department, which increases exposure to risks.” The absence of a specialized cybersecurity team, with reliance on the general IT function, is seen as a factor that increases vulnerability and reduces the level of risk control within the organization.

1.3.4. Human and Cultural Dimension of Risks

The testimonies of the four interviewees consistently and convergently reveal that the human factor occupies a central position within the cybersecurity risk landscape, with some even considering it the primary and most critical source of threats within the institution. The Information Systems Engineer emphasized that humans represent a major source of risk, whether through opening suspicious links or using weak passwords, noting that even with strong security systems in place, a simple human error can create a vulnerability that is difficult to mitigate.

In the same context, the Head of Studies described the level of cybersecurity awareness among employees as significantly low, highlighting a substantial knowledge gap in dealing with digital threats and stating that this situation elevates “human risks” to critical levels within the institution.

The Information Systems Manager added a more nuanced cultural dimension, indicating that the level of security awareness varies according to job position, age, and experience. This

implies that human vulnerability is not a uniform phenomenon but rather a differentiated one that requires tailored training approaches.

Furthermore, the Head of Statistics introduced a social dimension by linking awareness levels to educational background, observing that employees with university-level education generally demonstrate higher awareness, whereas middle-level staff often do not fully grasp the severity of cybersecurity breaches and their consequences.

Taken together, these testimonies clearly illustrate that human and cultural risks are not peripheral elements of the cybersecurity framework but rather lie at its core. Any security strategy that overlooks this dimension and relies solely on technical solutions is inherently limited, regardless of how advanced or sophisticated it may be.

1.3.5. Integration of Risk Management into the Global Strategy

No comprehensive security strategy is complete unless risk management is embedded at its core rather than treated as a peripheral component. This is the most prominent lesson consistently highlighted in the interviewees' accounts. The analysis of the interviews reveals that the studied institutions suffer from a clear disconnect between daily security practices and the logic of systematic risk management, as periodic assessments are largely absent and risks are typically handled in a reactive, ad hoc manner after incidents occur rather than being anticipated in advance.

The Information Systems Manager precisely summarizes this situation by noting that the absence of a formal framework leads to methodological weaknesses in incident response and to a lack of clear prioritization of security issues. In contrast, he emphasizes that effective governance is one that transforms risk management from an isolated technical activity into an integrated managerial process aligned with the institution's strategic objectives, relying on tools such as the RACI matrix and key performance indicators (KPIs) as mechanisms to ensure accountability and structured decision-making.

The Head of Studies further stresses that integrating risk management into the overall strategy requires a clear and structured methodology for identifying, assessing, and treating risks, referring to ISO/IEC 27001 as the most appropriate standard for achieving such integration.

Similarly, the Information Systems Engineer adds that the shift from a reactive approach to a proactive one can only be achieved when risk management becomes an integral part of the institutional planning cycle, ensuring that cybersecurity risks are considered at the moment of strategic decision-making rather than addressed after their consequences emerge.

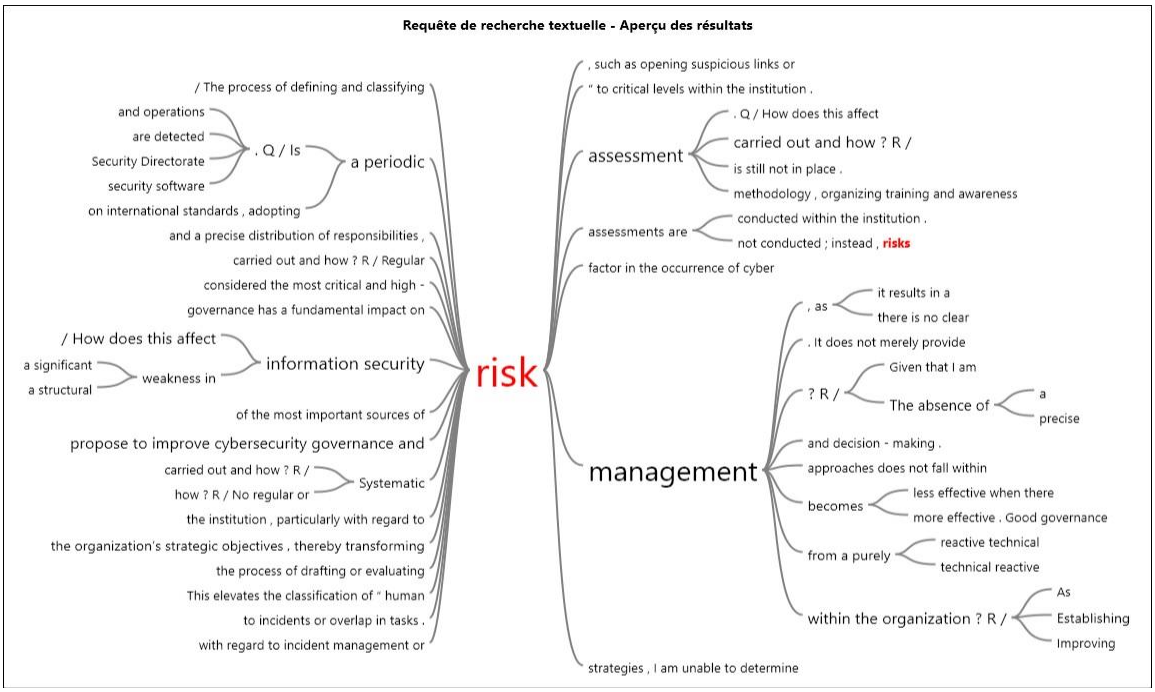
In conclusion, these converging testimonies indicate that embedding risk management within a comprehensive strategy is not merely a technical procedure or administrative document, but rather an institutional philosophy grounded in anticipation, continuous learning, and clear accountability. This philosophy is essential for enabling the studied institutions to move beyond their current state of vulnerability toward a more mature and effective security model.

2. Information Security Risk Management Process

2.1. Identification

The identification phase focused on exploring existing information security risks within the institution, with particular emphasis on the application layer. This phase constituted a fundamental step in establishing a basis for a systematic risk analysis and in highlighting vulnerabilities previously identified by stakeholders. All risks related to the application layer were carefully examined and addressed.

Figure 5 :Mind map of information security risks



Source: developed by us using Nvivo

The results are displayed in the form of a mind map branching out from the central keyword into multiple contexts. The text excerpts reveal that the document addresses fundamental issues related to the absence of a clear methodology for risk assessment within organizations, the weak distribution of responsibilities, and the impact of these factors on the effectiveness of security decision-making. It also highlights recommendations advocating for improved cybersecurity governance and the development of more sustainable methodological frameworks, suggesting that the document is most likely a critical study or evaluative research identifying gaps and proposing solutions within a specific organizational environment.

Table 5 : Identified Security Risks by Application and Function

Application	**Layer**	**Role**	**Security Risks**
Aruba Controller	Network layer	Wireless access point control	- Unauthorized Wi-Fi access - Improper access configuration - Controller vulnerability exploitation
Active Directory	Identity layer	User and session management	- Privilege escalation attacks - Credential theft - Mismanaged access rights
Kaspersky Controller	Endpoint layer	Antivirus engine management	- Unauthorized console access - Antivirus engine vulnerabilities - Inadequate update management
GTC	Operations layer	Centralized technical operations	- System intrusion - Security device mismanagement
Smart PSS	Physical layer	Video surveillance monitoring	- Unauthorized camera access
DLGC	Storage layer	Data storage management	- Data loss or theft - Poor access governance - Absence of audit trails

DLGC	Finance layer	Billing operations	- Financial data leakage - Record tampering - Fraudulent data exploitation
PCPaie	HR layer	Payroll processing	- Sensitive data theft - Unauthorized HR record modification - Lack of encryption
PCCompta	Accounting layer	Financial accounting	- Unauthorized access to financial records - Insufficient backup procedures

Source: Developed by us

2.2. Risk Categorization Based on the CIA Security Principles

In this table, risks have been categorized into five main groups: Access and Rights Management, Technical and Configuration Risks, Sensitive Data Risks, Connected Systems & Physical Risks, and Human Risks, based on the CIA Triad (Confidentiality, Integrity, and Availability).

Each risk is assessed to determine its impact, where an "X" indicates the affected dimension, whether Confidentiality (C), Integrity (I), or Availability (A).

Category	Risk	Confidentiality (C)	Integrity (I)	Availability (A)
Access and Rights Management	Unauthorized access to the wireless network.	X		
	Improper configuration of access controls.	X	X	X
	Elevation of privileges.	X	X	
	Credential theft.	X		
	Inadequate management of access rights.	X	X	
	Incorrect configuration of user permissions.	X	X	
	Ineffective access management.	X	X	X
	Unauthorized access to the management console.	X		
	Unauthorized access to surveillance cameras.	X		
	Unauthorized access to accounting data.	X		
Technical and Configuration Risks	Exploitation of controller security vulnerabilities.	X	X	
	Security vulnerabilities in the antivirus engine.	X	X	
	Inefficient update management.		X	X
	System intrusion.	X	X	X
	Inadequate management of security equipment.	X	X	X
	Lack of encryption.	X		
	Inadequate backup practices.			X
Sensitive Data Risks	Data loss or theft.	X	X	X
	Leakage of financial data.	X		
	Theft of sensitive data	X		
	Unauthorized or fraudulent use of information.	X	X	
	Unauthorized modification of HR data.		X	
	Data tampering.		X	
	Insufficient traceability.	X	X	
Connected Systems &Physical Risks	Cyber espionage through connected systems.	X		
	Interception of video streams.	X		
Human Risks	Fraudulent manipulation.	X	X	

Table 6 : identified the CIA security principles

Source: Developed by us

Based on the risk matrix findings, it is evident that the organization faces a complex security landscape requiring immediate response and rigorous governance. The results highlight that risks such as system intrusions and access misconfigurations pose a comprehensive threat, impacting all three pillars of security (Confidentiality, Integrity, and Availability) simultaneously, which could lead to operational paralysis and a loss of institutional credibility. Furthermore, there is a high concentration of risk surrounding "Confidentiality," a critical factor when handling financial and accounting data, where any unauthorized access to these information assets could result in severe legal and administrative consequences. Additionally, the lack of traceability mechanisms and encryption represents a fundamental vulnerability that weakens the ability to detect tampering or ensure data integrity, underscoring the urgent need to transition from ad-hoc security measures to a comprehensive organizational framework that proactively addresses these technical and administrative gaps.

2.3. Risk RACI Matrix: Information Security Management

Table 7 : Identified RACI matrix

Activities / Tasks	Information Systems Manager (DSI)	Cybersecurity Officer	IT Team / IT Engineer	Employees
Identification of information assets	A	R	C	I
Risk identification	A	R	C	I

Risk analysis using FMECA	A	R	C	I
Risk assessment and classification	A	R	C	I
Development of risk treatment plan	A	R	C	I
Implementation of security measures (Firewall, Antivirus, etc.)	A	C	R	I
Access rights and permissions management	A	R	R	C
System and network monitoring	A	R	R	I
Backup management	A	C	R	I
Security incident response	A	R	R	I
Security awareness and training	A	R	C	R
Security audits and periodic reviews	A	R	C	I

Source: Developed by us

The RACI matrix provides a clear and structured overview of the distribution of responsibilities related to information security risk management within the organization. It helps formalize governance by assigning each activity to the appropriate stakeholders according to their roles and level of involvement.

Overall, the Information Systems Manager (DSI) holds the *Accountable (A)* role for all activities, which reflects their strategic responsibility and final decision-making authority

regarding information security governance. This ensures centralized oversight and alignment with organizational objectives.

The Cybersecurity Officer plays a central operational role, mainly acting as *Responsible (R)* for most risk management activities, including risk identification, analysis, classification, and incident response. This highlights their key position in implementing security policies and ensuring technical risk mitigation.

The IT Team / IT Engineer is primarily involved in the *Responsible (R)* role for technical execution tasks such as implementing security controls, managing backups, system monitoring, and supporting access management. They ensure the operational continuity and technical enforcement of security measures.

Finally, the Employees are mostly assigned the *Informed (I)* role, with limited *Responsible (R)* participation in security awareness and training activities. This reflects their role in complying with security policies and contributing to the human aspect of cybersecurity, particularly in reducing risks related to human error.

In conclusion, this RACI matrix enhances clarity in roles, reduces ambiguity in responsibilities, and strengthens coordination between technical, managerial, and operational actors. It also supports better governance of information security by ensuring that each risk management activity is properly assigned, monitored, and executed.

2.4. the analysis of Verbatim matrix

This section is based on the analysis of qualitative data collected through semi-structured interviews conducted with a group of officials within the General Inspectorate of Finance.

The Verbatim matrix is presented in Appendix No. 2.

Axe 1: Regulatory framework

These statements reveal a mixed and transitional state of cybersecurity policy across the surveyed organizations. While most institutions currently lack any formal or approved cybersecurity framework, some are in the process of establishing dedicated cybersecurity authorities under presidential decrees that will clearly define their mandates and operational structures. In contrast, at least one organization already has an official framework in place, governed by an Information Systems Security Policy designed to protect digital assets, though evaluating its clarity and effectiveness remains challenging without specialized technical expertise. Overall, the landscape reflects an early stage of institutional maturity in cybersecurity

governance, with efforts underway to move toward more structured and formally recognized frameworks.

Axe 2: Distribution of responsibilities

Within the IGF institution, cybersecurity roles and responsibilities remain unclear or are assigned in an informal manner. Where they do exist, the separation of duties is not well defined, particularly in incident management and risk assessment, leading to task overlap and slower response times. Incident coordination also relies mainly on informal direct communication with IT departments rather than structured systems and procedures. This overall lack of formal governance creates structural weaknesses that significantly affect the effectiveness of information security risk management within the institution.

Axe 3: Coordination and communication

I observed that internal communication regarding cybersecurity incidents and risks within the organization remains largely informal and reactive. The organization relies mainly on direct contact with the IT Directorate or official administrative correspondence as its primary coordination mechanism, rather than structured and proactive communication systems. In some cases, external reporting to specialized bodies affiliated with the Ministry of National Defense is required when risks arise. The organization has only shown a more structured approach in certain aspects, using official correspondence addressed to different departments to ensure proper documentation and institutional organization.

Axe 4: Proactive approach

Based on what I gathered from the surveyed organizations, risk management is predominantly reactive rather than proactive. Most institutions address cybersecurity risks only after incidents occur, without implementing regular assessments, preventive measures, or structured early detection mechanisms. Where limited preventive actions exist such as system updates and security software they are insufficient to constitute a comprehensive risk management strategy.

Axe 5: Training and awareness

The study shows that poor security awareness among employees represents a key and recurring vulnerability, with the human factor being the weakest link due to practices such as using weak passwords and mishandling sensitive data or suspicious links. Awareness levels also vary depending on education, position, and experience, with employees who have a university background or work in information systems demonstrating higher awareness than others. This weakness is mainly attributed to the absence of continuous training and awareness programs, making the strengthening of the human factor a strategic priority in cybersecurity.

Axe 6: Information security risk management

These statements collectively affirm that cybersecurity governance represents a fundamental strategic pillar in risk management, transforming the handling of threats from a mere reactive technical response into a systematic and continuous managerial process, grounded in international standards such as ISO/IEC 27001 and clear mechanisms for defining roles and responsibilities. However, the human factor remains a weak link in this framework, given a moderate to low level of security awareness that calls for ongoing training and awareness programs. Effective governance also contributes to enhanced monitoring through key performance indicators and improved incident response capabilities, although developing such a framework often requires specialized technical and legal expertise that exceeds internal organizational capacity.

2.5. Word Frequency Analysis Query

Table 8 : Word Frequency Query

Word	Frequency	Percentage
governance	62	3.03%
organization	48	1.63%
cybersecurity	38	3.10%
security	39	2.90%
management	33	2.31%
responsibilities	30	2.39%
assess	27	2.08%
effective	27	1.04%

Source : Extracted from nvivo

The word frequency analysis of the study reveals that cybersecurity and governance are the two most dominant terms, appearing at the highest weighted percentages of 3.10% and 3.03%

respectively, which confirms that these two concepts form the central axis of the research. This is closely followed by terms related to risk management such as risks, management, assess, and incidents, reflecting the study's strong focus on evaluating and responding to security threats. The notable presence of words like responsibilities, roles, and define points to a recurring concern around the lack of clarity in task distribution within the surveyed institutions. Meanwhile, the relatively low frequency of the word proactive appearing only 8 times compared to terms associated with reactive behavior, aligns with the study's finding that most organizations respond to incidents after they occur rather than anticipating them. Finally, the presence of awareness and employees among the key terms underscores the human dimension as a persistent vulnerability throughout the study. Overall, the word frequency data is fully consistent with the six analytical axes of the research, reinforcing the conclusion that cybersecurity governance, risk management, and role definition are the three pillars around which the entire study revolves.

2.6. Word Frequency Analysis and Sources Grouped by Word Similarity

Table 9: Sources grouped by word similarity

Source A	Source B	Correlation Coefficient
Information Systems Manager	Study Director	0.812
Information Systems Manager	IT Engineer	0.811
IT Engineer	Study Director	0.756
Head of Statistics	Information Systems Manager	0.752
Head of Statistics	Study Director	0.740
Head of Statistics	IT Engineer	0.712

Source : Extracted from nvivo

All correlation coefficients are high, exceeding 0.71, indicating a strong and consistent alignment in the discourse used among all respondents. The highest correlation is recorded between the Information Systems Manager and the Study Director (0.812), suggesting that these two actors share the most similar concepts and terminology, likely due to their close professional roles and direct involvement with technical and cybersecurity systems.

In contrast, the lowest correlation is observed between the Head of Statistics and the IT Engineer (0.712), which can be explained by the difference in their specializations and job functions, although the correlation remains generally high. It is also noteworthy that the Head of Statistics shows the lowest correlation values with all other respondents, indicating a more distinct discourse compared to the others, which is expected given the administrative and statistical nature of the role, which is relatively distant from the technical domain.

Second section: Discussion

1.Absence of a Formal Cybersecurity Governance Framework

The findings of the field study, based on qualitative data analyzed using nvivo, reveal a near-total absence of a formal framework governing cybersecurity practices within the General Directorate of Informatics and Statistics (IGF). Three out of four interviewees confirmed that no officially approved cybersecurity policy exists, highlighting a structural weakness in cybersecurity governance.

This finding aligns with (Albalasa, Modjtahedib, & Abdic, 2022), who emphasizes that effective management requires a clear organizational structure to guide resources toward strategic objectives. It is also consistent with (Soumiya & Eddine, 2022), who identified the predominance of informal and underdeveloped governance practices in the Algerian public sector.

This absence cannot be attributed solely to a lack of awareness; rather, it reflects deeper institutional factors, including the absence of a binding regulatory framework, limited pressure to adopt international standards such as ISO/IEC 27001, and a shortage of specialized resources. Consequently, this situation leads to unclear strategic direction, weak oversight mechanisms, and reduced compliance with international best practices.

2.Ambiguity in Roles and Responsibilities

The analysis highlights a clear gap between the theoretical recognition of the importance of role distribution and its practical implementation. The head of the study reported the absence of formally defined cybersecurity roles, while the IT director indicated that responsibilities are assigned temporarily and on an ad hoc basis.

This situation contradicts (Albalasa, Modjtahedib, & Abdic, 2022) ,who considers clear role allocation a fundamental pillar of effective management, and diverges from the holistic approach advocated by (Melaku, 2023), which calls for the integrated consideration of people, skills, technologies, and processes.

This issue can be explained by the lack of formal job descriptions related to cybersecurity and the absence of its integration into the organizational structure. As a result, accountability is weakened, responsibilities overlap, and the likelihood of unmanaged security gaps increases.

3.Lack of Structured Information Security Risk Management

nvivo analysis revealed the absence of any formal or periodic risk assessment process. Risks are addressed only after incidents occur, reflecting a reactive rather than a proactive approach.

This contradicts (Melaku, 2023), who advocates for a risk-based approach to cybersecurity management, and diverges from the model proposed by (Zhang, 2023), which integrates FMECA with Bayesian networks to reduce subjectivity in cyber risk assessment.

This deficiency exposes all three dimensions of the CIA Triad confidentiality, integrity, and availability to simultaneous risk, as highlighted in cybersecurity literature (Alhalima; Understanding the CIA Triad, 2024).

From an analytical perspective, this gap is linked to a lack of expertise in risk analysis, the absence of standardized tools and methodologies, and the failure to prioritize risk management at the strategic level. Its implications include inefficient resource allocation, an inability to anticipate threats, and increased system vulnerability.

4.Reactive Rather than Proactive Security Approach

All technical interviewees confirmed that the institution adopts a reactive approach to cybersecurity, responding to threats only after incidents occur, without implementing proactive measures such as security audits or vulnerability assessments.

This approach contradicts (Davies, n.d.), who highlights the importance of proactive mechanisms in cybersecurity, and diverges from (Melaku, 2023), who emphasizes the need to shift toward a preventive, risk-based model.

This tendency can be attributed to an organizational culture focused on short-term problem-solving rather than long-term strategic planning, as well as to limited technical and human resources. The consequences include higher incident costs, delayed response times, and negative impacts on business continuity.

5.Informal Coordination and Weak Institutional Governance

The findings indicate that coordination within IGF is informal and situational, lacking structured mechanisms for communication and collaboration among stakeholders.
This contradicts the principle of collaboration emphasized by (Melaku, 2023), which considers cybersecurity a multi-level domain requiring coordinated efforts across internal and external actors. Meanwhile, the Director of Statistics stressed that cybersecurity governance should provide a structured framework aligning security with institutional strategic objectives.
This situation reflects a broader governance issue, particularly the confusion between governance and management, as highlighted by (Melaku, 2023), where governance relates to strategic direction and oversight, while management concerns operational execution.

The absence of formal coordination leads to slower incident response, poor information sharing, and reduced effectiveness of security decisions.

6. Human Factor and Security Awareness

All respondents agreed that the human factor represents the weakest link in the institution's cybersecurity posture, with low security awareness identified as a primary source of risk.
This finding aligns with (Mohammed, 2023), who emphasizes the importance of user adherence to basic data protection practices, and with (Melaku, 2023), who advocates for building a comprehensive cybersecurity culture through continuous training and awareness.
The Director of Statistics added an important dimension by noting that security awareness varies according to educational level, which calls for tailored training programs adapted to different user profiles.
This issue is mainly due to the absence of structured training programs and the lack of integration of awareness initiatives into internal policies. Its consequences include increased vulnerability to social engineering attacks, data breaches, and weak compliance with security procedures.

7. Synthesis of Findings

Overall, the findings reveal a consistent organizational pattern in which theoretical awareness of cybersecurity and governance exists, but practical implementation remains limited. This observation aligns with (Leroy, Zolotaryova & Semenov, 2023), who identified similar discrepancies in stakeholder perceptions within institutional contexts.

Therefore, the core issue within IGF is not a lack of knowledge, but rather structural and institutional barriers, including the absence of a binding regulatory framework, a shortage of specialized human resources, and the weak strategic integration of cybersecurity.

Addressing these challenges requires strong institutional commitment, supported by regulatory reforms, the adoption of international standards, and the implementation of sustainable training and awareness programs. Such measures are essential to position cybersecurity as a strategic pillar within public sector governance.

General conclusion

This dissertation was initiated from a central research problem examining the extent to which cybersecurity governance contributes to improving information security risk management. It was conducted through an in-depth field study within the General Directorate of Informatics and Statistics (IGF) at the Ministry of Finance, with the aim of analyzing how information security risk management is structured and implemented within IT governance frameworks, particularly in the context of sustainability-oriented digital transformation.

To address this problem, the study pursued three interrelated objectives. First, it aimed to identify the key information security risks affecting the institution's information system. Second, it sought to provide a comprehensive analysis of existing risk management practices based on qualitative data collected from institutional stakeholders. Third, it examined the extent to which governance practices are aligned with cybersecurity requirements in order to ensure coherence between risk management processes and the organization's strategic objectives.

The findings, derived from qualitative analysis using nvivo, reveal a fundamental structural gap between the conceptual recognition of cybersecurity governance and its operational implementation. While institutional actors demonstrate a clear awareness of the importance of cybersecurity and governance principles, this awareness remains largely untransformed into formalized structures, policies, and systematic practices.

This gap is manifested through a set of interconnected deficiencies, including the absence of a formal cybersecurity governance framework, the lack of clearly defined roles and responsibilities, and the absence of structured and periodic risk assessment mechanisms. As a result, the institution predominantly adopts a reactive approach to cybersecurity, addressing risks only after incidents occur. In addition, the findings highlight weak institutional coordination and fragmented communication processes, alongside limited security awareness, where the human factor emerges as a critical vulnerability.

From an analytical perspective, these results demonstrate that the challenges faced by IGF are not primarily related to a lack of knowledge or awareness, but rather to structural and institutional constraints. These include the absence of a binding regulatory framework, the shortage of specialized human resources, and the weak strategic integration of cybersecurity within governance systems.

Beyond the empirical findings, this study reinforces the strong interconnection between information security risk management and cybersecurity governance within the broader context of sustainable digital transformation. It shows that risk management should not be considered merely as a technical or operational function, but rather as a strategic governance mechanism that enables organizations to anticipate, prioritize, and mitigate risks in alignment with long-term objectives.

From a practical perspective, strengthening cybersecurity governance in public sector institutions requires the adoption of a comprehensive and integrated approach. This includes the implementation of internationally recognized standards such as ISO/IEC 27001, the formal definition of roles and responsibilities, the establishment of structured coordination mechanisms, and sustained investment in capacity building and cybersecurity awareness programs.

In this regard, the study highlights the necessity of shifting from a reactive security posture to a proactive, risk-based approach. Such a transition is essential not only to enhance the resilience of information systems, but also to ensure business continuity, improve institutional performance, and support sustainable digital transformation.

Ultimately, this dissertation demonstrates that information security risk management, when effectively integrated into a clear and structured governance framework, becomes a key strategic enabler. It strengthens organizational resilience, protects critical information assets, and supports the achievement of broader development and sustainability objectives. As digital transformation continues to reshape public sector institutions, the integration of cybersecurity, governance, and risk management will become increasingly essential for ensuring long-term stability and sustainable growth.

Bibliography

Albalasa, T., Modjtahedib, A., & Abdic, R. (2022). Cybersecurity governance: a scoping review. *International Journal of Professional Business Review, 7*(4).

Alhalima, I. (n.d.). *fundamentals of cyber security: unit - cyber security goals*. Retrieved from University of Mosul: https://uomosul.edu.iq/computerscience/wp-content/uploads/sites/13/2025/05/LECT-1.FUNDAMENTALS-OF-CYBER-SECURITY-Ibrahim-Alhalima.pdf

Al-Kassar, T. (2019). An investigation of capital investment and accounting information: evidence from Jordan. Investment Management and Financial Innovations,. *16*(3), 106-119.

Alnawaiseh, N., & Al-Mahasneh, M. A. (2024). The Impact of Digital Transformation Requirements on Risk Management. *Library Progress International, 44*(3), 18488.

Alonso, c. (n.d.). *Global Suite Solutions. Risk assessment methods: Mehari, Ebios, Octave.* Retrieved from https://www.globalsuitesolutions.com/risk-assessment-methods-mehari-ebios-octave/

Baggia, A. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *13*(1).

Bilgin Metin, F. G. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics, 13*(21), 4226.

Cedric Ryngaert, M. T. (2020). SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW THE GDPR AS GLOBAL DATA PROTECTION REGULATION? (C. U. Press, Ed.) *American Journal of International Law,AJIL Unbound, 114*, 5-9.

Davies, J. (n.d.). *3 Pillars of cybersecurity: process, technology and people*. Retrieved from The Knowledge Academy: https://www.theknowledgeacademy.com/blog/three-pillars-of-cyber-security/

Death, D. (2023). Information Security Handbook: Enhance your proficiency in information security program development 2nd Edition. 370.

Gartner. (2021). *Is the cloud secure?* Retrieved from https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

GDPR. (n.d.). *What is GDPR, the EU's new data protection law?* Retrieved from GDPR: https://gdpr.eu/what-is-gdpr/

Grall, M. (2018). *EBIOS: The risk management toolbox — Generic approach. Club EBIOS & Agence nationale de la sécurité des systèmes d'information (ANSSI).* Retrieved from https://club-ebios.org/site/wp-content/uploads/productions/EBIOS-GenericApproach-2018-09-05-Approved.pdf

Hidayat, R. S., Indrajit, R. E., & Dazki, E. (2024). TOGAF's Approach in Developing an Enterprise Architecture for the Information Technology Security Industry. *Journal La Multiapp, 5*(5), 630-645.

HP Wolf, S. (2024). *HP Wolf Security study reveals platform security gaps that threaten organizations at every stage of the device lifecycle. HP Inc.* Retrieved from https://www.hp.com/us-en/newsroom/press-releases/2024/hp-wolf-security-study-reveals-platform-security-gaps.html

ISACA. (2019). *COBIT for Small and Medium Enterprises.* Retrieved from https://www.isaca.org/resources/news and-trends/ isaca-now-blog/2021/cobits-value-for-small-and-medium enterprises?gad_source=1&gclid=CjwKCAjwvIWzBhAlEiwAHHWgvb0 0ic4YhJzYg4E9tj76ByOJpZBtdkMcDr2TENfls1Zyx6-SxL_DbhoC6EsQAvD_BwE

ISO, 2. (2019). *Security and resilience — Business continuity management systems — Requirements. ISO*. Retrieved from https://www.iso.org/standard/75106.html

ITGI. (2006). Information security governance: Guidance for boards of directors and executive management.

Joseph. (n.d.). *IT governance: An essential pillar of IT service management. Lemon Learning.* Retrieved from https://lemonlearning.com/fr/blog/une-gouvernance-it

Khan, M. M. (2022). Cyber Security Standards. *10*(2).

Kroenke, D. M. (2015). MIS Essentials (4th ed.). Pearson Education.

Kumar, A. (2023). OBSERVATION METHOD. *Library Philosophy and Practice, 13*(6), 1-14.

LAMIEN, S. (2023). Towards a better adoption of information systems security standards in Burkina Faso. International Journal of the Researcher.

Mekimah, S., & Zerdoudi, A. (2022). The evaluation of the information security management system (ISMS) to ISO 27001 standards: Case study of the port company of Skikda-Algeria. Scientific Journal,. *8*(2).

Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy, 3*(3), 327-350.

MetricStream. (n.d.). *Calculate risk scores for better risk management. MetricStream*. Retrieved from https://www.metricstream.com/learn/risk-scores-for-better-risk-mgmt.html

Mohammed, A.-D. (2023). Cybersecurity .

Nicodemus, B., & Swabey, L. (2015). Action research. In C. V. Angelelli and B. J. Baer (Eds.) Researching translation and interpreting. New York: Routledge.

Nweke, L. O. (2017). Using the CIA and AAA Models to Explain Cybersecurity Activities. *PM World Journal, 6*(12).

Pearson. (2022). Management Information Systems: Managing the Digital Firm .

Preston, S., & Karahanna, E. (2009). Antecedents of IS strategic alignment: A nomological network. *Information Systems Research, 20*(2), 159–179.

Proofpoint. (2025). *Global insights into CISO challenges, expectations and priorities. Proofpoint, Inc.* Retrieved from Voice of the CISO: https://www.proofpoint.com/us/resources/white-papers/voice-of-the-ciso-report

Reuben-Owoh, B., & Haig., E. (2025). A Systematic Review of Voluntary Cybersecurity Standards and Frameworks. *International Journal of Information Security, 24*(5).

Ryan, J. (2023). The CIA Triad.

Sabherwal, R. S. (2019). How does strategic alignment affect firm performance? The roles of information technology investment and environmental uncertainty. *MIS Quarterly, 43*(2), 453–474. doi: https://doi.org/10.25300/MISQ/2019/13626

Sabherwal, R., & Chan, Y. (2001). Alignment between business and IS strategies: A study of prospectors, analyzers, and defenders. Information Systems Research. *12*(1), 11–33. doi: https://doi.org/10.1287/isre.12.1.11.9714

SentinelOne. (n.d.). *10 data security risks for 2026*. Retrieved from https://www.sentinelone.com/cybersecurity-101/data-and-ai/data-security-risks/

Soumiya, L., & Eddine, Z. I. (2022). Evaluation of the maturity of information system governance according to the COBIT 4.1 framework: Case of the Ministry of National Education. *The Creativity Journal*.

Stamatis. (2003). Failure mode and effect analysis: FMECA from theory to execution (2nd ed.). ASQ Quality Press.

Stapleton, S. (2025). *What is compliance risk? Definition, types, management, examples. Pathlock*. Retrieved from https://pathlock.com/blog/grc/compliance-risk/

StartechGcc. (n.d.). *Best Three Pillars of Cyber security Digital Peace of Mind*. Retrieved from StartechGcc: https://www.startechgcc.com/three-pillars-of-cyber-security/

The Open Group Standard. (n.d.). *The TOGAF® Standard, Version 9.2*.

Thomas, C. (n.d.). *Five steps of the risk management process. 360Factors.* Retrieved from https://www.360factors.com/blog/five-steps-of-risk-management-process/

Understanding the CIA triad in cybersecurity. (2024). Retrieved from SCRIBD: https://fr.scribd.com/document/796122464/CIA-Triad

Yeung, J., & Magramo, K. (2023). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'*. Retrieved from CNN: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

Zhang. (2023). Quantifying potential cyber-attack risks in CNC Systems under Zero-Subjectivity Closed-Loop Dempster–Shafer theory FMECA and Rule-Based Bayesian Network modelling. Reliability Engineering & System Safety, Elsevier.

Appendix

Appendix I – Interview Guide

Cybersecurity Governance in Algerian Institutions as a mechanism for managing information security risks

Interview Guide

Axis	Question
Representative Questions:	Name Position years in the organization
Regulatory Framework	Are there internal policies or a formal framework within the organization that governs cybersecurity? How do you evaluate the clarity of these policies in terms of implementation?
Distribution of Responsibilities	How are roles and responsibilities defined in the field of cybersecurity? How does this affect information security risk management?
Coordination and Communication	Is there effective communication when security risks or incidents occur?

	How is coordination ensured between different departments regarding cybersecurity?
Proactive Approach	Does the organization rely on a proactive approach to identifying risks, or are they addressed after they occur? How is this done? Are periodic risk assessments conducted, and how are they carried out?
Training and Awareness	Does a lack of awareness contribute to the occurrence of risks? How do you assess the level of security awareness among employees?
Information Security Risk Management	Do you consider that cybersecurity governance has a real impact on managing these risks, and how? What are the main measures you would propose to improve cybersecurity governance and risk management within the organization?

Appendix II – Verbatim matrix

Interviewee	Regulatory framework	Distribution of responsibilities	Coordination and communication	Proactive approach	Training and awareness	Information security risk management
Head of Study	There are currently no formal policies or an approved framework governing cybersecurity within the institution. Therefore, it is not possible to assess the clarity or applicability of such policies, as they do not exist as an established regulatory framework in the first place.	There are no defined roles or responsibilities in the field of cybersecurity within the institution. There is no effective communication system for managing security incidents. However, coordination is handled through a direct communication protocol with the IT Directorate, activated upon detection of suspicious activity to ensure rapid intervention and reduce system damage.	There is no effective communication mechanism in place within the institution for handling security risks or incidents. Coordination in cybersecurity is mainly carried out through a direct communication protocol with the IT Directorate, which is activated whenever suspicious activity is detected, in order to ensure rapid intervention and limit technical damage.	The institution does not adopt a proactive approach to risk management, as risks are mainly addressed after they occur through incident response, without regular assessment or preventive measures. In addition, periodic risk assessments are not conducted and risks are handled in an ad hoc manner, which weakens early detection and increases the likelihood and impact of security incidents.	Poor security awareness significantly increases the occurrence of risks, as the human factor is considered the weakest link and employees may unintentionally become exploitable vulnerabilities. Overall, the level of security awareness among employees is very limited, with major gaps in understanding digital threats and handling sensitive data, making human risk a critical issue within the institution.	Cybersecurity governance plays a fundamental role in risk management by establishing a regulatory framework that aligns security with the organization's strategic objectives, shifting risk management from a reactive technical response to a continuous and structured managerial process. To improve governance and risk management, it is essential to implement a clear framework based on recognized standards such as ISO/IEC 27001 and to clearly define roles and responsibilities within the institution, especially in risk management and decision-making.
Computer Science Engineer	There is currently no official cybersecurity policy in the organization, but a specialized	Cybersecurity roles are generally defined, with the IT department handling technical	There is no clear or effective communication when security risks or incidents occur.	The organization does not follow a structured proactive approach to risk	Poor security awareness significantly increases risks, as the human	Poor security awareness significantly contributes to risks, as human errors such as using weak passwords or

	cybersecurity body is being established. Once created, it will operate under a presidential decree that clearly defines its mandate, ensuring a well-defined and structured framework.	aspects and management responsible for decision-making. However, there is sometimes no clear separation of responsibilities, particularly in incident management and risk assessment. This lack of precision can slow down incident response and create task overlap, which reduces the effectiveness of information security risk management due to unclear accountability at each stage.	Coordination in cybersecurity is mainly done through official correspondence once an incident happens.	management; instead, it mainly relies on reactive responses after incidents occur, with limited preventive measures such as system updates and security software. In addition, there is no systematic or periodic risk assessment in place.	factor is a major vulnerability (e.g., weak passwords or clicking suspicious links), where even small errors can compromise strong security systems. Overall, employee awareness is moderate to weak: those working directly with information systems are more aware, but there is a general need for continuous training and awareness programs.	opening suspicious links can create vulnerabilities even in well-protected systems. Overall, employee awareness is moderate to weak: while staff working directly with information systems show better understanding, there is still a general need for continuous training and awareness programs.
Director of Information Systems	There is currently no official cybersecurity framework or approved policies within the organization. However, a competent authority in this field is being developed in accordance with a presidential decree that defines its establishment and mandate.	Cybersecurity roles are only temporarily assigned, without a formal structure. This absence of an official framework creates a structural weakness in information security risk management, leading to a lack of clear methodology and unstructured incident response.	There is no clear internal communication when security incidents occur, but in case of risks, a specialized institution affiliated with the Ministry of National Defense must be informed. Coordination between departments is mainly limited to official administrative correspondence.	The institution mainly follows a reactive approach, addressing cybersecurity risks only after they occur or are detected, rather than proactively identifying them. In addition, no regular or systematic risk assessments are carried out.	Insufficient security awareness among employees is a critical factor in the occurrence of cyber incidents, as uninformed staff can become human vulnerabilities that are easily exploited. The level of awareness varies depending on position, age, and experience.	Cybersecurity governance has a fundamental impact on risk management by providing a comprehensive framework that ensures strategic alignment, clearly defines roles and responsibilities (e.g., RACI matrix), enables continuous monitoring through KPIs, and improves incident response capabilities. To improve governance and risk management, it is necessary to establish structured control mechanisms and a well-

						defined plan, while ensuring compliance with applicable laws and regulations.
Director of Statistical Information	The organization has an official cybersecurity framework and approved policies, governed by an Information Systems Security Policy that defines the rules for protecting digital assets. However, assessing the clarity of these policies is difficult from a non-technical perspective, as it requires specialized expertise in information security standards and frameworks.	The respondent indicates that defining cybersecurity roles and responsibilities is outside their scope of duties, and therefore they are not involved in this process. As a result, they are unable to assess or determine the impact on information security risk management or risk strategy effectiveness.	There is effective communication during security incidents through official correspondence sent to all departments, ensuring proper documentation and keeping all units informed. Coordination in cybersecurity is ensured through established instructions that must be strictly followed.	The respondent states that defining risk management approaches and their classification is outside their job responsibilities, as it requires technical expertise from the Information Systems Security Directorate. They also indicate that they cannot confirm whether periodic risk assessments are conducted or how they are carried out, since this falls under the responsibility of internal control and technical audit units.	Poor security awareness among employees significantly increases risks, as it weakens compliance and leads to repeated incidents due to improper use of digital assets. The level of security awareness varies: employees with a university education are generally more aware, while mid-level staff are perceived as having a limited understanding of the consequences of cybersecurity threats.	Cybersecurity governance plays a fundamental role in risk management by providing a regulatory framework that aligns security with the organization's strategic objectives, transforming risk management from a reactive technical response into a continuous and systematic managerial process. However, proposing improvements to governance and risk management is considered beyond the respondent's expertise and requires specialized technical and legal knowledge.