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

« Strategic management and information system »

Risk Management for Information Security within IT Governance in Sustainable Development Projects

Case of: *ESHRA GREEN CAMPUS*

Prepared by:

Ms. HATTAB Asma

supervised by:

Dr. DERRAR Hacene

Dr. BEDAIDA Imad Eddine

2024/2025

ABSTRACT

In today's sustainability-driven landscape, aligning information security, IT governance, and sustainable development is essential for building ethical and resilient systems. This dissertation explores how information security risk management can support institutional sustainability initiatives, using the Smart Green Campus project at the Algiers Higher School of Hospitality and Restaurant Management (ESHRA) as a case study.

Using a qualitative action research methodology, the study evaluates ESHRA's current IT governance and security practices. It integrates semi-structured interviews, document analysis, and Failure Mode, Effects, and Criticality Analysis (FMECA) to identify and mitigate security risks within the Smart Green Campus initiative.

The findings highlight a multidimensional vision of sustainability, encompassing technological, cultural, organizational, and educational dimensions. ESHRA's information system is shown to operate across layered infrastructure and application domains. The initial FMECA revealed 26 failure modes 3 critical, 15 moderate, and 8 acceptable. Post-intervention results showed a successful mitigation of critical risks and a substantial reduction in moderate risks, achieved through targeted measures such as automated patching, role-based access control, and robust backup solutions.

This research contributes to both theory and practice by demonstrating the effectiveness of FMECA in sustainability-oriented information systems and by deepening the understanding of how information security risk management serves as a foundational pillar in achieving sustainable institutional objectives.

Keywords: Information Security, Risk Management, IT Governance, Sustainability, Smart Green Campus, FMECA

Résumé

Dans un contexte institutionnel de plus en plus tourné vers la durabilité, l'alignement entre la sécurité de l'information, la gouvernance des systèmes d'information et les objectifs de développement durable devient essentiel pour bâtir des systèmes éthiques et résilients. Ce mémoire explore comment la gestion des risques liés à la sécurité de l'information peut soutenir efficacement des projets institutionnels orientés vers la durabilité, à travers l'étude de cas du projet Smart Green Campus de l'École Supérieure d'Hôtellerie et de Restauration d'Alger (ESHRA).

En adoptant une méthodologie qualitative de type recherche-action, l'étude évalue les pratiques actuelles de gouvernance des SI et de sécurité de l'information à l'ESHRA. Elle s'appuie sur des entretiens semi-directifs, une analyse documentaire et l'application de l'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) pour identifier et atténuer les risques liés à la sécurité dans le cadre de cette initiative.

Les résultats révèlent une vision multidimensionnelle de la durabilité intégrant les dimensions technologiques, culturelles, organisationnelles et pédagogiques. Le système d'information de l'ESHRA fonctionne selon une structure en couches, entre domaines applicatifs et infrastructurels. L'analyse AMDEC initiale a identifié 26 modes de défaillance : 3 critiques, 15 modérés et 8 acceptables. Les résultats post-intervention ont montré une atténuation réussie des risques critiques et les risques modérés réduits grâce à des mesures ciblées (correctifs automatiques, contrôle d'accès basé sur les rôles, solutions de sauvegarde robustes).

Cette recherche contribue à la fois à la théorie et à la pratique, en illustrant l'efficacité de l'AMDEC dans des projets SI orientés durabilité, et en soulignant le rôle fondamental de la gestion des risques en sécurité dans l'atteinte d'objectifs durables.

Mots-clés : Sécurité de l'information, Maitrise des risques, Gouvernance des SI, Durabilité, Smart Green Campus, AMDEC

الملخص

في سياق مؤسسي يتزايد فيه التركيز على الاستدامة، يُعد التوافق بين أمن المعلومات، حوكمة نظم المعلومات، وأهداف التنمية المستدامة عنصرًا أساسيًا لبناء أنظمة مرنة وأخلاقية. تهدف هذه الدراسة إلى تحليل كيف يمكن لإدارة مخاطر أمن المعلومات أن تدعم المبادرات المؤسسية الموجهة نحو الاستدامة، من خلال دراسة حالة مشروع "الحرم الأخضر الذكي" بالمدرسة العليا للفندقة والإطعام بالجزائر.(ESHRA)

اعتمدت الدراسة منهجية بحث نوعية تعتمد على البحث الإجرائي، حيث قامت بتقييم ممارسات الحوكمة والأمن المعلوماتي الحالية بالمؤسسة. وتم ذلك من خلال مقابلات شبه موجهة، تحليل للوثائق، وتطبيق تحليل أنماط الفشل وتأثيراتها ودرجة خطورتها (FMECA) لتحديد وتخفيف المخاطر الأمنية في إطار المشروع.

كشفت النتائج عن رؤية متعددة الأبعاد للاستدامة تشمل الجوانب التكنولوجية، الثقافية، التنظيمية والتعليمية. ويتكون نظام المعلومات في المؤسسة من طبقات تشمل البنية التحتية والتطبيقات. وقد كشفت FMECA الأولية عن 26 نمطًا للفشل: 3 حرجة، 15 متوسطة، و8 مقبولة. بعد التدخلات أظهرت النتائج بعد التدخل تخفيفًا ناجحًا للمخاطر الحرجة وتقليص المخاطر المتوسطة بشكل كبير، من خلال إجراءات مستهدفة مثل التحديثات التلقائية، التحكم في الوصول بناءً على الأدوار، وحلول النسخ الاحتياطي الفعالة.

تُسهم هذه الدراسة نظريًا وتطبيقيًا من خلال إظهار فعالية FMECA في مشاريع نظم المعلومات ذات التوجه البيئي، وتؤكد أن إدارة مخاطر أمن المعلومات تمثل ركيزة أساسية لتحقيق أهداف الاستدامة المؤسسية.

الكلمات المفتاحية: أمن المعلومات، إدارة المخاطر، حوكمة نظم المعلومات، الاستدامة، الحرم الأخضر الذكي، FMECA

Acknowledgements

بسم الله الرحمن الرحيم

I shall begin to express my gratitude and acknowledgements to Allah, "glorified and exalted be he", whom allow me to walk this long path, whom gave me the patience to spend this journey of my life in seeking knowledge so that it can be dedicated by this humble work.

I will express my gratitude to the members of the juries that they expected to examine my work; moreover, to all of my doctors in ENSM; thank you for all of your efforts during this period.

Now, most importantly; I am expressing my truthful gratitude towards my supervisors Doctor DERRAR Hacene; Doctor BEDAIDA Imad Eddine; So that they helped me the whole duration; Mister DERRAR Hacene thank you for your precious and precise orientations and helpful notes in this dissertation ;Mister BEDAIDA Imad Eddine I would like to express my gratitude for your availability; Corrections and above all you're the moral support you offered me the whole time till the last moment to accomplish this work today, thank you for participating in this work in every step showing patience and kindness.

To the two persons that not only brought me to life but that they see life through me ; to my parents , PAPA Ahmed the man raised me to seek the knowledge in every corner of life ,that has engaged with all he can and have since I have ever remembered , MAMA Thouraya the woman that made the woman I am today ;that planted in me the determination and perseverance , love and kindness , whom structured whatever I am today ;thank you PAPA and MAMA ;this wouldn't of happened without you. This work is for you my dear parents before it is for me.

To my siblings, my only sister Marwa my first and forever best friend; and my brothers Yasser and Youcef; Thank you for always being there for me, my reflection in your eyes as a big sister and a role model for you has always pushed me across the limits.

To my dear Wasilla; Haider that has always encouraged me to be better and seek higher in life and to all of my beloved family thank you for every single kind word that I have ever heard from you.

To all of my friends, my soulmate Ines that knows me more that I know myself; Aya; Manel; Malek; Chaima; and Safa thank you for listening over and over to my complains and removed all my doubts thank you for seeing the good in me even before me.

And lastly; I want to thank myself a lot for this beautiful journey that be have been together, for all the efforts; tears, and laughter; thank you ASMA.

Table of content

Contents

List of tables

List of figures

List of abbreviations

ARPA: Advanced Research Projects Agency

ARPANET: Advanced Research Projects Agency Network

CCPA: California Consumer Privacy Act

CIA: Confidentiality, Integrity, Availability

CISA: Cybersecurity and Infrastructure Security Agency

CNIL: National Commission for Data Protection (France)

COBIT: Control Objectives for Information and Related Technologies

CSPM: Cloud Security Posture Management

DSI: Director of Information Systems

ERM: Enterprise Risk Management

ESHRA: Algiers Higher School of Hospitality and Restaurant Management

FMECA: Failure Mode, Effects, and Criticality Analysis

GDPR: General Data Protection Regulation

IoT: Internet of Things

IS: Information Systems

ISMS: Information Security Management System

ISRM: Information Security Risk Management

ISO: International Organization for Standardization

IT: Information Technology

MFA: Multi-Factor Authentication

NIST: National Institute of Standards and Technology

RBAC: Role-Based Access Control

RPN: Risk Priority Number

WPA3: Wi-Fi Protected Access 3

General Introduction

In the contemporary digital era, organizations are increasingly compelled to navigate a multifaceted landscape where technological innovation must coexist with rigorous demands for information security and sustainability. The rapid pace of digital transformation presents both unprecedented opportunities and complex challenges, particularly as institutions seek to align their strategic objectives with emerging environmental and social imperatives (Melville, 2010). This evolving paradigm necessitates a holistic approach to managing information systems one that integrates robust governance frameworks, effective risk management practices, and a commitment to sustainable development (Günther, 2020).

Information security, traditionally concerned with the protection of data confidentiality, integrity, and availability, now intersects with broader organizational goals of sustainability and responsible resource management (Lozano, 2013). The imperative to safeguard digital assets must be balanced against the pressing need to reduce environmental impact and promote social accountability. This convergence is exemplified by innovative initiatives such as Smart Green Campus project, which leverage cutting-edge digital technologies to create intelligent, eco-efficient environments. (Günther, 2020)These projects demonstrate how information systems can be designed and governed not only to enhance operational efficiency and user experience but also to advance sustainability objectives without compromising security.

As organizations increasingly embed sustainability into their digital strategies, the governance of information systems assumes a critical role in orchestrating these diverse yet interdependent priorities (Weill, 2004). Effective governance mechanisms must ensure that security risks are identified and mitigated proactively, while also fostering innovation that supports sustainable practices. This integrated perspective underscores the importance of developing comprehensive frameworks for managing the risks associated with information security in a way that aligns with sustainable development principles.

This research seeks to explore the intricate relationship between information security risk management within IT governance and sustainability in the context of Smart Green Campus initiatives. By examining how governance structures, risk assessment methodologies, and security policies can be adapted to support sustainable digital transformation, this study aims to contribute to both academic discourse and practical approaches in this emerging field.

Chapter I

Context and problematic

1. Context of the study

Information Systems (IS) governance has become a key strategic lever for organizations seeking to align their digital transformation with their overall objectives. It no longer focuses solely on the technical management of infrastructures, but extends to broader issues such as value creation, risk control, and compliance with regulatory and ethical requirements.

This dissertation is positioned specifically within the field of risk management, a fundamental pillar of IS governance. In an environment where digital data, interconnected systems, and intelligent technologies are ubiquitous, risks related to information security take on a strategic dimension. Data breaches, cyberattacks, human error, or the absence of coherent security policies can jeopardize not only system performance but also the reputation and long-term sustainability of organizations.

This issue becomes even more critical in the context of sustainability-oriented projects, where the resilience of information systems must support environmental and social commitments. The Smart Green Campus project, led by ESHRA, exemplifies this convergence between digital innovation and sustainable development. It aims to integrate Internet of Things (IoT) technologies and smart systems to optimize energy consumption, enhance resource efficiency, and reduce the campus's carbon footprint, while improving the overall user experience. However, ESHRA's current digital infrastructure is still in a phase of modernization, which presents significant challenges in terms of information systems governance and security risk management, particularly in an environment of increasing digital complexity.

However, without a robust IS governance framework that incorporates a rigorous risk management approach, such projects remain vulnerable to internal and external threats. The proactive consideration of information security risks thus becomes a key success factor in this hybrid context of sustainability and digitalization.

2. Research question

Existing IT governance frameworks such as COBIT and ISO 27001 are primarily designed to ensure compliance and operational efficiency. However, they often fall short when it comes to addressing the complex risks linked to information security in sustainability-oriented digital transformation projects. These models tend to treat information security risks as purely technical issues, without fully considering their strategic, ethical, or environmental dimensions.

In projects like Smart Green Campus, where the integration of smart technologies (including IoT) supports long-term sustainability goals, this oversight becomes critical. While IoT is part of the institution's digital vision, the current challenges lie in the governance of information systems, the management of security risks, and the alignment of these practices with sustainable development objectives.

To address these challenges, this research explores how information security risk management can be better integrated into IS governance frameworks to support resilient and sustainable digital initiatives. Using the case of ESHRA's Smart Green Campus, the study aims to contribute to the development of a more inclusive approach that accounts for technical vulnerabilities, organizational culture, and strategic alignment with sustainability.

Based on the context presented above, we pose the following research question:

How can information security risk management, as a pillar of IT governance, support the strategic and ethical objectives of sustainability projects, such as the Smart Green ESHRA?"

Secondary questions:

- *How can IT governance frameworks integrate information security risk management to align with the sustainability objectives of digital projects?*
- *What are the main challenges organizations face in managing information security risks in sustainability-driven digital initiatives?*
- *How can organizations ensure alignment between information security measures and both strategic and ethical goals in sustainability-focused digital projects?*

3. Objective of the study

The main objective of this final project is to explore and Analize the management of risks within IT governance frameworks, using the case of sustainability projects and ESHRA as a starting point for the study, one of the key institutions involved in such projects. The study will focus on identifying the key risk factors and dimensions of IT governance within sustainability initiatives. To achieve this, the project will focus on the following sub-objectives:

- To identify the major information security risks that could affect ESHRA's information system.
- To provide a detailed analysis of risk management practices within ESHRA's IT governance based on qualitative data from real stakeholders.

- ❖ Align IT governance practices with the governance of sustainable development, ensuring that the management of risks supports the broader sustainability goals.

4. Justification for the choice of the topic

This research topic was chosen in light of our specialization in Strategic Management and Information Systems, and reflects our strong interest in the intersections between governance, security, and sustainability key areas for the digital transformation of modern organizations. The convergence of these domains is especially relevant in contexts where institutions are seeking to align their information systems with environmental and social responsibility goals.

Furthermore, we observed a significant lack of academic work focusing on the management of information security risks within sustainable digital projects, particularly in the Algerian context. Few studies have explored how these risks are governed and mitigated in institutions engaged in digital sustainability initiatives, which limits both theoretical understanding and practical guidance.

Therefore, this research offers an original contribution by addressing an underexplored yet critical area. It aims to bridge the gap between sustainable development and information security risk management within the framework of IT governance. In doing so, it provides added theoretical and practical value, especially in light of the emerging Smart Green Campus projects in Algeria, where new risks emerge alongside technological and ecological innovations.

5. Epistemological stance

5.1Epistemological Positioning

In exploring existing approaches to risk management related to information security within sustainable development projects, we identified a gap in the literature concerning the integration of sustainability into information systems governance frameworks. Few studies address how stakeholders perceive and interpret information-related risks in complex and evolving environments such as *Smart Green Campus* initiatives.

In this context, we have adopted an interpretivist epistemological posture, which we consider particularly appropriate for capturing the complexity of human, organizational, and technological dynamics involved. This paradigm is based on the assumption that reality is socially constructed, and that understanding the phenomena under study requires

interpreting the meanings that individuals assign to them (Benhaddouch, M., & El Fathaoui, H., 2022) . The objective is not to generalize findings, but to gain in-depth understanding of the representations, practices, and action logics of those involved in managing information security risks in a sustainable context. This epistemological stance directly informs our choice of a qualitative action research methodology, which emphasizes active collaboration with ESHRA's stakeholders and supports an iterative, context-sensitive inquiry process.

5.2 Research Approach

The methodology for this study is inductive, grounded on systematic observation and analysis of empirical information. As compared to the deductive process, whereby assumptions based on theories are preceded by forming precise hypotheses, our inductive approach is founded on movement from certain observation towards wider generalization. It starts with research in thorough learning about data, which are collected within the field and trends as well as patterns evolve out of it. This approach facilitates the formation of broad conclusions out of specific, context-bound observations, in contrast to preconceived hypo dissertation verification. Thus, the focus of this research is interpreting and exploring empirical data for conceptual framework development, as explained by (Nassou, Y., & Bennani, Z., 2024)

6. Relevance of the Study

The selection of our research topic is the result of careful reflection and extensive reading, enabling us to identify key factors that will guide us in making informed decisions, both theoretically and managerially

Theorical

This study aims to fill the gap in existing literature by exploring the risks related to information security within IT governance frameworks, particularly in the context of sustainability projects. While numerous studies have been conducted on this concept in other sectors and contexts, few have specifically examined the risks within the realm of IT governance in sustainability-focused environments. Therefore, this research will delve into an area that is still underexplored, providing a deeper understanding of the factors influencing risk management and information security in this context, and contributing to the body of knowledge in this field

Managerial

The results of this study, from a practical perspective, will provide concrete recommendations for organizations involved in sustainability projects to develop strategies

for improving their risk management practices within IT governance frameworks. These organizations will be able to adapt their processes, communications, and governance strategies based on the identified risk factors to enhance their overall performance and distinguish themselves from competitors.

The findings will be valuable to decision-makers and stakeholders in the IT governance space in so they will help guide their strategic efforts towards the most critical risk management aspects, ultimately contributing to better decision-making and the long-term success of sustainability initiatives

7. Study framework (location)

Internship location:

Algiers Higher School of Hospitality and Restaurant Management (ESHRA) is a distinguished institution dedicated to hospitality learning and training excellence. Being host organization of this final year internship, ESHRA is strategically placed to shape future leaders and experts in the fields of hospitality and restaurant management. Began in response to the increasing and evolving demands of the hospitality industry, the school started with a clear mission: to provide world class education that is academically rigorous as well as pragmatically relevant.

Figure 1 ESHRA'S LOGO

Source: http://ESHRA.dz/

By its strategic focus on quality, innovation, and sustainability, ESHRA has been able to establish itself as a modern and innovative institution. It offers an exciting learning environment that blends international standards, best practices, and constant improvement. The institution collaborates with industry leaders and international partners to ensure that its curriculum is aligned with the latest global trends and the needs of a fast-paced market.

In line with its objectives, ESHRA is to be a country and regional centre of excellence in hospitality and restaurant professional education. Its mission rests on establishing a culture of excellence anchored by profound and sincere passion for service, hospitality, and customer satisfaction. The school develops the values of professionalism, leadership, and creativity as it aims to produce graduates who not only meet but even exceed the hospitality sector's expectations.

Through such cultivation of vision, ESHRA motivates its people and staff to embrace innovation, adopt responsible practices, and contribute meaningfully to the development of a more resilient, inclusive, and sustainable hospitality sector

MISSION and VALUES

The school's mission is to establish and prepare a new generation of highly competent hospitality and restaurant management professionals. ESHRA aims to equip its students with robust technical competence and managerial know how which will enable them to navigate and adjust to the challenges of a more dynamic and globalized world. Along with scholarly preparation, the school encourages the integration of sustainable development principles into everyday professional behaviour and prepares its graduates to operate with a sense of social and environmental responsibility.

The mission is perpetuated and guided by an interconnected cluster of essential institutional values, which are the anchor pillars of all school activities in its academic, administrative, and strategic activities:

Excellence: As an ongoing aim, excellence is reflected in the school's ongoing emphasis on excellence in teaching, research, operations, and student outcomes. Excellence represents a professional culture of quality improvement and rigor at every level.

Passion: It is at the core of ESHRA's values that there is great passion for the hospitality industry. This inspires students and faculty alike, motivating them to provide outstanding service and maintaining a positive, people focused learning community.

Innovation: Innovation as a force of change is greatly promoted in the institution. It enables the school to take the forefront in seeking education enhancements and be able to address the evolving demands of the hospitality industry.

Responsibility: ESHRA promotes a high level of ethical, social, and environmental responsibility. It is cultivated by way of programs and pedagogical practice that stress sustainability, integrity, and accountability in all aspects of institutional and student existence.

Together, these values underpin an integrated educational model aligned with the broader goals of sustainable development and continued excellence within the hospitality industry.

❖ Presentation of the project Smart Green ESHRA

The *Vision 2030: Smart Green ESHRA* project aims to transform the *École Supérieure d'Hôtellerie et de Restauration d'Alger* (ESHRA) into a sustainable centre of excellence aligned with the Sustainable Development Goals (SDGs). This initiative is part of the broader modernization of Algeria's hospitality and tourism sector by integrating ecological, technological, pedagogical, and economic dimensions.

The ambition is clear: to position ESHRA as a national and international model in green hospitality education and sustainable tourism, while actively contributing to economic development and promoting environmentally and culturally respectful tourism

. Strategy for a Sustainable ESHRA

The strategy is built on several interdependent pillars:

- **Sustainability integration** into governance, curricula, infrastructure, and partnerships.
- **Technological innovation** through AI and digital tools to rethink learning, management, and research.
- **Stakeholder engagement** (students, faculty, staff, businesses, NGOs, local authorities) through co-construction and strong local anchoring.
- **An ecosystem model** promoting responsible education, sustainable entrepreneurship, and social impact.

. Monitoring and Adjustment Mechanisms

The project relies on a smart monitoring system based on:

- **AI dashboards** to manage key performance indicators in real time.
- **Annual evaluations** based on the SDGs and ISO standards.
- **A participatory feedback loop**, incorporating insights from students, faculty, and industry partners to continuously adjust actions.

. Expected Results by 2030

The project's transformational goals include:

- **Youth empowerment**: 50% of graduates as entrepreneurs or managers in green hospitality.
- **International positioning**: Algeria among the top 50 countries in the Travel & Tourism Competitiveness Index.
- **Carbon neutrality** on campus through renewable energy.
- **Digital transformation**: the first hospitality school in Algeria to integrate AI at all levels.
- **Social impact**: 20% reduction in youth and women's unemployment.
- **Economic positioning**: entry into global green markets worth several trillion dollars.

. Roadmap: Foundation Phase (through the end of 2025)

The initial phase lays the structural groundwork:

- **Governance**: Establishment of operational committees and Vision 2030 policies.
- **Assessment**: Energy audits, pedagogical diagnostics, and international benchmarking.
- **Infrastructure**: Detailed plans for renewable energy and campus greening.
- **Partnerships**: Collaboration with green organizations, AI networks, and sustainability stakeholders.
- **Research**: Development of research frameworks in AI applied to sustainable tourism, and grant applications.
- **Awareness**: Strengthening communication and mobilization around the Smart Green ESHRA vision.

Chapter II

Literature review and Conceptual framework

In today's fast-changing digital landscape, the governance of information systems is crucial to organizational success and sustainability. 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 adopt new technologies, they must balance innovation with risk mitigation and long-term sustainability. The review begins with core concepts of IS governance, showing how frameworks like COBIT align technology with organizational goals across various sectors, including education and public administration. 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, it looks at the connection between security and sustainability through initiatives like Smart Green Campuses. By combining global and local research, this chapter proposes a conceptual framework linking theory and practice to show how secure, well-governed IS can support sustainable digital transformation.

1. Literature review

In today's knowledge-driven economy, Information Systems (IS) have become foundational to the functioning and competitiveness of modern organizations. An information system can be defined as a set of interrelated components both technical and human that work together to collect, process, store, and disseminate information to support decision-making, coordination, and control. As highlighted by (Baskerville, R., Davison, R., Kaul, M., Malaurent, J., & Wong, S., 2022) , information systems serve as a nexus between technology and organizational processes, facilitating innovation and strategic alignment. Their importance extends beyond operational efficiency, playing a pivotal role in governance, risk management, and sustainability. In this literature review, we will explore the governance of information systems, the integration of risk management within IS governance, and how information security management systems (ISMS) can contribute to sustainable digital transformation, particularly in the context of smart green campuses.

1. IT governance

The governance of information systems (IS) is crucial for aligning information technology with organizational goals, particularly in the context of sustainable development projects. As

organizations navigate the complexities of digital transformation, international research underscores the importance of effective IS governance frameworks in managing risks and ensuring the strategic alignment of technology with business objectives. (Müller, 2022)argues that IS governance frameworks must evolve to address emerging technologies such as artificial intelligence and blockchain while also safeguarding against information security risks. (Williams, R., & Lebek, B, 2022) emphasize how these frameworks help protect critical data, ensuring the confidentiality, integrity, and availability of information. In parallel, research by (Benzidia, 2023) and (Wahiba, 2024) highlights the increasing need to align IS governance with sustainability objectives, especially in sectors where digital innovation is crucial. However, challenges arise when these global frameworks are applied in local contexts. For instance, (Ladjouzi, 2022) explores IS governance within Algeria's public sector, specifically within the Ministry of National Education. Based on the COBIT framework, her study reveals that while certain processes are in place, they remain informal and underdeveloped, exposing a significant gap in aligning international best practices with local needs. This disparity underscores the necessity for adaptable IS governance practices that can bridge the gap between global standards and local realities.

These studies collectively confirm that IS governance is recognized as a strategic mechanism for ensuring control, compliance, and long-term value creation in digital initiatives. Authors such as (Baskerville, R., Davison, R., Kaul, M., Malaurent, J., & Wong, S., 2022), (Müller, 2022)and (Williams, R., & Lebek, B, 2022)highlight the essential role of governance frameworks in managing risks and aligning technology with organizational objectives. At the same time, (Benzidia, 2023)and (Wahiba, 2024) draw attention to the growing emphasis on sustainability, stressing the need for IS governance to incorporate long-term environmental and social considerations. However, as illustrated by (Ladjouzi, 2022)the application of global frameworks such as COBIT can be limited in local settings, where informal and underdeveloped practices persist. This demonstrates the importance of adapting governance models to fit specific organizational and national contexts.

2. Information Security Management System (ISMS)

International research on Information Security Management Systems (ISMS) highlights a range of sector-specific challenges and success factors related to their implementation. (Benyettou, 2018)examine the integration of management systems in Algerian companies, pointing to organizational hurdles that hinder adoption. Similarly, a study at Payam Noor University in Iran emphasizes the role of organizational readiness, ranking barriers to

implementation and showing how preparedness impacts success. (Hamdi, 2019)provide a comparative review across multiple sectors, identifying diverse challenges and recommending tailored strategies. (Domínguez-Domínguez, 2023)focus on a higher education institution in Mexico, where training, administrative engagement, and institutional commitment are seen as key drivers of ISMS success. (Ibrahim, 2019)studying the Malaysian public sector, stress policy enforcement, security awareness, and regulatory compliance as critical factors.

Taken together, these studies demonstrate that ISMS implementation is a multidimensional process requiring both technical and organizational alignment. Common success factors across contexts include policy enforcement, organizational awareness, and readiness, as highlighted by (Benyettou, 2018); (Hamdi, 2019), and (Hamdi, 2019). Meanwhile, (Domínguez-Domínguez, 2023)underline the importance of training and internal commitment in academic environments. While the core principles of ISMS are broadly recognized, the diversity of contexts industrial, academic, and public reveals that effective implementation depends on a flexible, context-sensitive approach.

3. Foundations of Risk Management

Risk management has evolved from a traditionally reactive process into a critical strategic discipline supporting organizational resilience and value creation. (Aven, 2016)reviews recent advances, emphasizing the integration of uncertainty and variability in risk modelling. (Aven, 2016) and (Renn, 2020) highlight foundational issues such as addressing ambiguity and complexity, advocating for a unified theoretical framework across disciplines. (Floricel, S. T., & Miller, R. , 2015)critique traditional risk approaches for their limitations in handling organizational complexity and diverse stakeholders. (Lam, 2018)expands on Enterprise Risk Management (ERM) as a means to embed risk thinking into strategic and operational processes. (Knight, 2021) analyses the ISO 31000:2018 standard, a principles-based framework promoting the integration of risk management into decision-making.

These studies collectively recognize risk management as a vital strategic function that must move beyond reactive responses to uncertainties and align with organizational goals. They emphasize addressing ambiguity and complexity to develop robust risk frameworks. While (Aven, 2016) and (Renn, 2020) argue for a unified approach (Floricel, S. T., & Miller, R. , 2015) note the inadequacy of traditional models in complex socio-technical systems,

underscoring the need for context-sensitive adaptation. Overall, integrating risk management into organizational decision-making is essential for long-term stability and success.

In the specific domain of Information Security Risk Management (ISRM), Hansen et al. (2021), Choo et al. (2017), and (Da Veiga, 2015) concur on the necessity of real-time, dynamic risk assessment models to tackle growing cybersecurity challenges. They stress continuous risk assessment and mitigation, combining technical defences with fostering an organizational culture of security. (von Solms, 2016)advocate for a governance-driven approach elevating information security to a strategic priority. Divergences arise in implementation methods: (Hansen, 2021) promote adaptive models for critical infrastructure, while (Flores, 2023) focus on GDPR-compliant ISRM based on ISO 27005, highlighting regulatory alignment in Europe. This illustrates the importance of region- and sector-specific ISRM approaches. Collectively, these works suggest that effective ISRM requires a multi-dimensional strategy integrating technical, cultural, and regulatory factors to address evolving information security risks.

3.1. Information security risk management

Information Security Risk Management (ISRM) has evolved into a foundational component of organizational governance, especially as cyber and information risks continue to grow in complexity. (Hansen, 2021)emphasize the need for real-time, adaptive risk assessment models in critical infrastructures, while (Choo, 2017) examine the challenges of securing medical information systems, highlighting the intersection of ISRM and privacy in healthcare. (Da Veiga, 2015) focus on organizational culture, demonstrating how employee behaviour and awareness play a pivotal role in mitigating risks. Similarly, (von Solms, 2016)advocate a governance-driven approach that treats information security not just as a technical issue but as a management priority that spans all levels of an organization. (Mayer, 2017)contribute a framework for aligning ISRM with enterprise architecture methodologies like TOGAF and ArchiMate, fostering integration across systems and decision-making processes. In a European context, (Flores, 2023)propose a GDPR-compliant ISRM methodology based on ISO 27005, reinforcing the importance of regulatory alignment in modern risk strategies. Meanwhile, (Brunner, 2020) uncover limitations in ISRM adoption across the DACH region ,where reliance on manual processes and underutilized tools hampers efficiency. In Algeria, recent studies on digital transformation in financial institutions (2023) and AI adoption in customs (2023) reveal context-specific risks,

emphasizing the need for adaptive ISRM practices that respond to local technological and regulatory realities. moreover, in the public sector, the importance of a structured and context-specific risk management approach is emphasized by (Nurdin, 2024), who integrates ISO 31000 and NIST SP 800-30 into a governance-oriented framework for electronic-based government systems. This approach demonstrates how structured methodologies can guide risk prioritization using a risk matrix, linking asset vulnerabilities to threat vectors. The research identifies outdated IT policies as a major risk, underscoring the need to institutionalize continuous policy updates and risk integration into IT governance. The study also reinforces the critical role of risk management as a foundational pillar of IT governance, highlighting how the systematic identification and integration of operational risks are essential for ensuring strategic coherence, enhancing decision-making, These findings are echoed in the Smart Green Campus initiatives (Benali, 2023), where environmental sustainability intersects with IS risk management. Collectively, this body of work highlights that effective ISRM demands a multi-dimensional strategy one that integrates cultural, regulatory, technical, and organizational variables to build resilience in a rapidly evolving digital ecosystem.

3.2. FMECA: General Framework and Applications

The FMECA (Failure Mode, Effects and criticality Analysis) method is a structured approach for identifying and prioritizing potential failure modes within systems. It is widely used in manufacturing, aerospace, and healthcare sectors to anticipate risks and implement corrective actions before failures occur. (Alaoui, 2022)propose a theoretical framework that integrates FMECA into risk management by treating risks as both threats and opportunities. Practical industrial engineering guidance, such as from (Kaizen, 2025)illustrates how FMECA enhances operational resilience and process reliability.

Comparative studies by Benantar et al. acknowledge FMECA's effectiveness in identifying technical failures but highlight the need for adaptations when applied to information systems. (Shevchenko, 2021)demonstrate FMECA's practical benefits in improving customer satisfaction through systematic analysis and mitigation of product-related failures.

These studies agree on FMECA's strength as a systematic tool to anticipate and prioritize risks before they cause disruption. However, divergence arises in application focus:

(Alaoui, 2022) emphasize a theoretical integration into risk management, while Benantar et al. highlight practical, sector-specific adaptations. (Shevchenko, 2021)further stress that adapting FMECA for information systems is necessary, given its original design for physical systems.

Overall, FMECA remains a versatile and valuable risk identification and mitigation tool, though successful implementation in digital or information security contexts requires tailored adjustments.

3.3. FMECA in Information Security Risk Management

The adaptation of FMECA to ISRM reflects a broader trend of applying engineering-based risk models to digital systems. (Silva, 2014)propose a multidimensional model that integrates FMECA with approximate reasoning techniques to address risks across five dimensions of information security: access control, communication security, infrastructure, security management, and systems development. This hybrid approach enhances traditional FMECA by incorporating uncertainty handling, making it better suited for dynamic and complex IT environments.

Building on this, (Gusmão, 2016)introduce a decision-theoretic model based on approximate reasoning that quantifies information security risks more effectively than binary methods, emphasizing the value of combining qualitative expert input with structured analytical tools. Cybersecurity practitioners, such as those at (Haseeb, 2021), have further adapted FMECA for cyber risk analysis by evaluating cyber threat criticality through severity, likelihood, and detectability, thus providing a quantitative framework for cybersecurity governance decisions.

These studies concur that integrating advanced uncertainty modelling techniques or decision-theoretic frameworks with FMECA enhances its capacity to handle the dynamic nature of information security risks. (Silva, 2014)and (Gusmão, 2016)stress the importance of tailoring FMECA to specific information security dimensions. Divergence exists in their models' scope and focus: Silva et al. (2014) emphasize a comprehensive five-dimensional framework, whereas Gusmão et al. (2016) prioritize a soft computing-driven decision-theoretic quantification. This divergence highlights the need for flexibility in applying FMECA within various IT risk contexts.

Collectively, these works demonstrate FMECA's potential to strengthen ISRM by offering a systematic method for risk identification, assessment, and mitigation in digital environments.

4. Sustainability and information security

The integration of Information Security Management Systems (ISMS) with sustainability is essential for ensuring secure and environmentally responsible digital infrastructures (Benali, 2023)As sustainable development projects increasingly rely on IoT, cloud computing, and AI, they introduce new security risks, including IoT vulnerabilities (Khan, 2025), cloud data protection challenges (Almeida, 2023)and the need for energy-efficient cybersecurity measures (Williams, R., & Lebek, B, 2022)

To mitigate these risks while aligning with sustainability goals, organizations must adopt best practices such as Green Cryptography, which reduces the energy consumption of encryption processes by up to 40% compared to traditional methods (Odumesi, 2024)Similarly, Edge Computing for Security optimizes data processing by minimizing unnecessary transfers a strategy validated by Algeria's Smart Green Campus initiatives, where edge nodes cut energy use by 25% without compromising security (Benali, 2023)Emerging tools like AI-driven threat intelligence further enhance proactive risk detection. For instance, a 2023 study by (Benzidia, 2023)demonstrated that machine learning models can predict 90% of zero-day attacks while slashing computational overhead by 35%, making cybersecurity both smarter and greener.

The articles highlight the need for integrating ISMS with sustainability practices. Benali et al. (2023) and Williams & Lebek (2022) stress security challenges in digital transformations, while solutions like (Odumesi, 2024)'s Green Cryptography and edge computing aim to reduce energy consumption and enhance security. These approaches align on creating secure, sustainable digital infrastructures.

Current IT governance frameworks (COBIT, ISO 27001) reveal significant shortcomings in managing information security risks within sustainability-driven digital projects. Primarily designed to ensure compliance and operational efficiency, these frameworks often neglect how information security risk management must strategically align with environmental, social, and governance (ESG) goals. For example, they rarely incorporate risk metrics related to sustainability, and treat information security risks as isolated technical issues rather than integrated strategic priorities. Furthermore, the dynamic nature of emerging threats such as AI-driven misinformation or cyber-physical attacks on critical infrastructures is not sufficiently addressed, leaving gaps in frameworks like ISO 31000 to capture the cascading impacts on sustainability, like increased carbon reliance due to smart grid disruptions. This fragmentation perpetuates a disconnect between technical risk management and sustainability objectives, enabling vulnerabilities through falsified emission data.

By theorizing information security risk management within the broader umbrella of IT governance, this research bridges these gaps by exploring the links of information security risks to ESG outcomes, embedding ethical risk prioritization aligned with sustainable development goals. The Smart Green Campus case study empirically validates this framework, illustrating how anticipatory risk modelling and stakeholder-aligned governance protocols transform information security risk management into a driver for resilient, ethical, and sustainable innovation.

2. Conceptual framework

1.1. Information Systeme :

An Information System (IS) is a coordinated network of components that work together to produce, distribute, and process information. It is a formal, socio-technical organizational system designed to collect, process, store, and distribute information. From a socio-technical perspective, information systems are composed of four components: tasks, people, structure (or roles), and technology (Kroenke & Auer, 2015)

The organization can be divided into three subsystems: the decision system, the information system, and the operating system. Each system provides services to the others

Decision-making System

The Decision-making System is at the apex of the organizational hierarchy. It is the organization's strategic leadership and sets overall goals and maps the direction for all operations. The system includes the executive team and key decision-makers who develop strategic plans, make major decisions, and allocate the resources required to achieve the organization's goals. Through the use of clear direction and control, decision-making ensures the organization is dedicated to its vision and is poised to respond to external and internal changes.

Information System

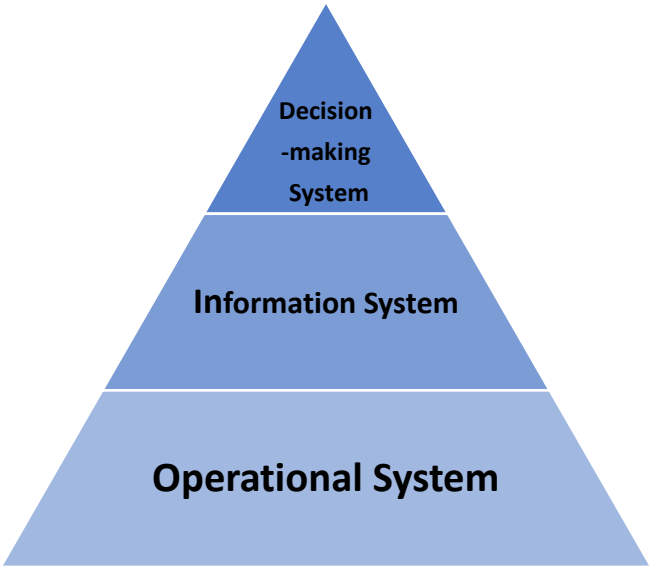
Information System is in the centre of everything, keeping the entire organization intact. It plays a role in gathering, processing, storing, and distributing information needed in strategic planning and day-to-day operations. Information System is referred to as the technology and information infrastructure, hardware, software, networks, databases, and applications. It acts as a crucial linkage between the operational system and the decision system in the sense of delivering timely and appropriate information for decision-making and performance management. Without a proper information system, neither strategic leadership nor operational implementation would be able to function effectively.

Operational System

The Operational System includes all the daily operational activities and processes of the organization. It addresses various functional departments such as production, sales, marketing, finance, and human resources. It is responsible for carrying out the fundamental functions of the organization and supplying products or services to customers. It takes assistance from the information supplied by the Information System to carry out day-to-day operations such as order processing, rendering services, customer communication, and

transactions. The operating system ensures that strategic objectives are translated into concrete results, thereby making a direct contribution to the success of the organization.

Figure 2 Information system pyramid



Source: developed by us based on the theorical framework

1.2. Information Sysmtem Governance :

Governance refers to a collection of organizations that make decisions to manage a specific area of activity. It involves a governance system and system dynamics (governance processes, management activities, etc.) (Larousse Dictionary).

The term governance is used to describe the ability of an organization to manage and rule over its own operations to avoid conflicts of interest in terms of the differentiation between stakeholders (shareholders) and actors. (COBIT 2019 Framework, released by ISACA).

1.2.1. IT Governance:

No general definition of the term "IT Governance" is available. Literature review identified that it is challenging to define the term since it is multidisciplinary. Thus, different researchers have proposed different definitions,

As per, (Abdelmalek Sadok , al, 2020) IT governance has been described as the structures of leadership and processes to align an organization's IT with its strategy and goals.

As ITGI (2006) describes, IT governance is executive management and board of directors' responsibility. IT governance entails leadership, organizational structure, and processes that ensure an organization's IT in supporting and enabling it to meet its business goals and strategies.

Furthermore, IT governance includes the organizational processes, accountability mechanisms, leadership processes, and structures instituted within a firm to ensure that the firm's overall goals and strategy remain in line with the IT activities. It includes the responsibility of the executive management and board of directors in managing and overseeing IT, with the institution of structures and processes that enable that IT effectively supports the business goals of the firm.

Also the term governance refers to an organization's ability to control and regulate its own functioning in order to avoid conflicts of interest related to the separation between stakeholders (shareholders) and operational actors (Ladjouzi, 2022) in addition Roland Pérez offers the following definition: "Corporate governance refers to the institutional and behavioural mechanisms that govern the relationships between a company's executives and its stakeholders."

1.2.2. 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

Key Domains of IT Governance (ISACA., 2009)

a. Strategic Alignment

IT governance ensures harmony between an organization's IT strategy and its broader business objectives. This is achieved through cross functional collaboration among management levels to address technology related opportunities and challenges.

b. Value Delivery

This domain focuses on delivering timely, budget compliant IT services and solutions that yield intended financial and non-financial benefits. It prioritizes investments in value adding IT assets while phasing out non value adding ones.

c. Risk Management

Proactively addresses IT related risks that could disrupt business operations, emphasizing the preservation of organizational value through mitigation strategies.

d. Resource Management

Ensures the availability of adequate IT capabilities and resources (human, technological, and financial) to execute IT strategies. Includes workforce training and competency development to maintain IT staff proficiency.

e. Performance Measurement

Establishes monitoring frameworks to evaluate IT effectiveness, ensuring continuous improvement. Without measurable KPIs, the preceding domains cannot achieve their intended outcomes.

Figure 3 IT Govenrance domains

Source: (Ross, 2004)

1.2.3. The Importance of IT Governance:

According to (Ross, 2004) Effective IT governance is the single most important predictor of the value an organization generates from IT. Organizations with strong IT governance have profits that are 20% higher than those with poor governance, given the same strategic objectives. IT governance ensures that IT investments support business goals, and it clarifies who makes decisions and who is accountable for the results

Aligning IT with Business Strategy

Effective IT governance makes every IT project tightly connected to the organization's strategic objectives. Through the connection of technology investments with business goals, governance models help companies concentrate on projects that develop competitive advantage, growth, and operational efficiency. This alignment saves resources and positions IT as a true driver for business success.

Optimizing Value Generated from IT Investments

One of the most basic benefits of IT governance is that it is possible to achieve maximum value out of IT expenditures. Through careful prioritization, performance monitoring, and

benefit realization practices, mechanisms of governance make sure that investments in IT result in measurable returns. Organizations with effective IT governance typically have better profitability and enhanced project success rates compared to poorly controlled organizations

Defining Clear Decision-Making Authority and Accountability

IT governance establishes clear directions that specify who possesses decision rights and who owns IT outcomes. By establishing roles, responsibilities, and decision hierarchies, governance eliminates internal wars, streamlines approval cycles, and offers transparency. It also creates an ownership culture where decision makers are fully accountable for success or failure of their IT projects.

Increasing the Value Provided by IT Investments

One of the basic strengths of IT governance is that it can optimize the return on IT investments. By prioritization, performance measurement, and benefit realization practices, governance controls ensure that IT investments deliver tangible benefits. Well-controlled organizations typically have higher profitability as well as better-performing projects compared to poorly controlled organizations.

1.2.4. Risk Management as a Core Governance Domain

In their book "*IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002"* by Alan Calder and Steve Watkins state that Risk management is a fundamental part of IT governance. Proper governance ensures that information technology-related risks like data breaches, system failures, and regulatory compliance are addressed appropriately. By integrating risk management practices into IT governance models, organizations can ensure that their IT plans align with their business objectives as a whole. This includes risk identification and mitigation to protect confidential information, automate business processes, and comply with industry regulations. The objective is to create a secure and stable IT infrastructure that enables sustainable growth and minimizes the potential threats to the organization's objectives."

2. Information security and risk management

2.1. 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. This

discipline extends beyond digital systems to encompass all information formats, ranging from electronic records and physical documents to proprietary intellectual property, corporate trade secrets, and sensitive personally identifiable information (PII). (Baggia, 2025)

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. It is structured around several key dimensions, including security governance and policies, asset classification and management, and individual security measures aimed at mitigating human related risks such as theft, fraud, or the misuse of resources. Additionally, access control plays a crucial role in this framework.

An effective information security policy must be clear, concise, and tailored to the organization's specific needs. Implementing rigorous control mechanisms is essential to ensuring accountability among stakeholders and structuring interactions between information systems. The overarching objective of information security is to safeguard the strategic interests of the organization by protecting information and communication systems that facilitate data distribution while minimizing vulnerabilities to potential threats.

Achieving this goal requires robust protection mechanisms to maintain data integrity and prevent unauthorized modifications, particularly through a well-defined internal control system and effective access management strategies. (MEKIMAH Sabri, 2022)

2.1.1. THE importance Of Information security:

The importance of information security is based on several key aspects (MEKIMAH Sabri, 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.

2.1.2. Brief History of Information Security and Cybersecurity

In the mid-1960s, computer systems moved beyond administrative and professional domains to become part of everyday life. Airlines began using computerized reservation systems, while financial transactions took the form of electronic funds transfers (EFT). Universities started offering computer science courses. At that time, security was rather rudimentary, primarily consisting of physical access protection and the use of passwords.

In 1969, the Advanced Research Projects Agency (ARPA), a research organization under the U.S. Department of Défense (DoD), developed the ARPANET computer network. This network, which allowed computers to communicate via telephone lines without relying on a central machine, is considered the precursor to the Internet.

A few years later, in 1971, developer Bob Thomas created a program called *Creeper* (often regarded as the first non-malicious computer virus), which displayed a message on an "infected" computer, initiated the printing of a file, and then moved to another machine before completing the task and continuing its journey through the network. A year later, the "antivirus" program "*Reaper"* was created to track down and eliminate "*Creeper"*.

These developments led government agencies, major corporations, research institutions, and computer security specialists to define the foundational principles of information security. In 1977, the Institute for Computer Sciences and Technology of the National Bureau of Standards (which later became NIST) organized the first *Audit and Security of Computer Systems* conference. This event highlighted methods and best practices for detecting threats and implementing effective protective measures within government agencies. In the introduction to the conference paper, Ruth Davis, President of the Institute for Computer Sciences and Technology, urged government agencies and businesses to collaborate with auditors to assess threats, potential losses, the probability of such losses, and the cost of implementing appropriate controls.

Since then, the legal framework surrounding data privacy and information protection has been updated and expanded. In the European Union, the General Data Protection Regulation (GDPR), which came into effect in 2018, marked a significant milestone in data privacy and security. In the United States, various states have enacted their own data privacy laws, such as the California Consumer Privacy Act (CCPA). These regulations require companies to

implement measures to protect consumer data, promptly report any breaches, and give individuals greater control over their personal information.

As technology continues to integrate into daily life, discussions about data privacy and security remain at the forefront. These concerns raise new questions and necessitate the continuous review of security protocols and legislation to safeguard users and their data from emerging threats. (Parsons, 2023)

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

The table below summarise all the aspects of differences between cybersecurity and information security.

Table 1 The difference between information security and cybersecurity

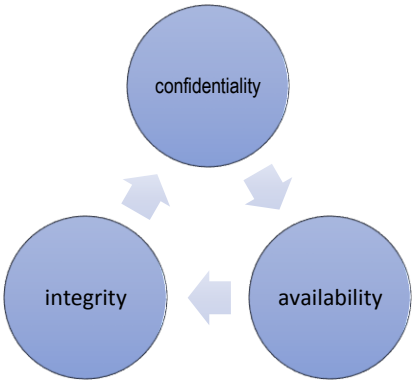
Aspect	Information Security (InfoSec)	Cybersecurity
Definition	Protects all forms of information digital, physical, and verbal from unauthorized access, alteration, disclosure, and destruction.	Focuses on protecting digital systems, networks, and data from cyber threats such as hacking, malware, and 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

2.1.3. 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. See Figure 1.1 for a visual representation of the following three pillars:

Figure 4 CIA TRIAD



Source: developed by us according to the information below

a. Confidentiality (Anthony Anyanwu1, 2024)

Confidentiality refers to the measures an organization implements to ensure that sensitive information remains private and secure. In practice, this involves restricting access to data, thereby preventing unauthorized disclosure or exposure. Effective confidentiality safeguards such as authentication mechanisms (passwords) and encryption (for data both in transit and at rest) help mitigate risks of unauthorized access. For confidentiality to be upheld, sensitive information must be accessible exclusively to authorized personnel whose roles necessitate such access. This principle is critical for preventing data breaches and ensuring that confidential information does not fall into the wrong hands.

b. Integrity

Integrity, in the context of information security, denotes the preservation of data accuracy and consistency by preventing unauthorized or unintended alterations, deletions, or additions. At its core, integrity ensures that data remains reliable and untainted by unauthorized modifications. This principle is closely tied to “non repudiation”, which guarantees that actions performed on data or systems can be irrefutably traced to their source, thereby holding parties accountable. Maintaining data integrity is especially crucial in legal and regulatory contexts, where demonstrating the authenticity and unaltered state of records

is paramount. Techniques such as cryptographic hashing, digital signatures, and digital certificates are commonly employed to uphold data integrity and verify its trustworthiness.

c. Availability

For any organization, possessing critical systems, applications, or data becomes meaningless if authorized users cannot reliably access them when needed. Availability ensures that all systems and services function as intended, providing timely and dependable access to resources. This principle is vital for enabling informed decision making, as data and services must be accessible precisely when required.

The usability of systems and services hinges on availability, as they must remain operational to meet user demands without interruption. To uphold availability, organizations implement strategies such as:

- **Redundancy** (duplication of critical systems to prevent single points of failure).
- **Hardware fault tolerance** (designing systems to continue operating despite component failures).
- **Regular backups** (ensuring data can be restored in case of corruption or loss)
- **Comprehensive disaster recovery plans** (predefined protocols to restore operations swiftly after disruptions).

By prioritizing these measures, businesses can minimize downtime and maintain seamless access to essential resources.

2.1.4. Application of information security:

a. Physical and Environmental Security

Physical and environmental security encompasses all the measures to shield systems and their operational environments (LASSON, 2023). It is crucial in offering the resilience and integrity of information systems by neutralizing risks of physical threats and environmental hazards from different angles:

- Protection of Energy Sources and Climate Control Systems Security of power supply, cooling systems, and backup energy sources to prevent operation disruption.
- Environmental Risk Management: Proactively taking measures to minimize risks of fires, floods, seismic events, and temperature and humidity conformity to safeguard infrastructure.
- Access Control and Security Governance: Establishing strict mechanisms for managing and monitoring physical access to facilities, equipment, and infrastructure, including entry logging and rigorous key management practices.

❖ Reliability and Resilience of Equipment: Utilize equipment and hardware with high operating reliability to minimize vulnerabilities related to physical failures or hostile tampering.

❖ Asset Marking and Theft Prevention: Applying marking and tracking methods to prevent unauthorized acquisition of assets and facilitate their recovery when required.

❖ Comprehensive Maintenance Strategy: Integrating preventive and corrective maintenance strategies, including regular testing of systems and the availability of critical spare parts, to ensure operating continuity and effectiveness.

b. Operational security

Operational security ensures the stability, efficiency, and resilience of information systems through structured processes like maintenance, diagnostics, and change management. Its effectiveness depends on automation, real-time monitoring, and seamless integration with system design and application development. By embedding security at every stage of the software lifecycle, organizations can enhance reliability, minimize risks, and maintain business continuity in an evolving digital landscape.

c. Logical, Application, and Information Security

Logical security refers to the implementation of software-based security mechanisms that ensure the proper functioning of programs, services, and data protection. It generally relies on:

- High-quality software development and security testing to prevent vulnerabilities.
- Proper implementation of cryptography to guarantee data integrity and confidentiality.
- Logical access control and authentication procedures to secure system access.
- Mechanisms for detecting malware, intrusions, and incident management to anticipate and counter threats.
- Adequate resource allocation, system redundancy, and secure backup and recovery procedures, ensuring application resilience and critical data protection.

By integrating these measures, organizations can strengthen their information systems against cyber threats while ensuring operational continuity and data security.

d. Security of Telecommunication Infrastructures

Telecommunication security consists of providing the end user and communicating applications with reliable end-to-end connectivity. This involves establishing a secure network infrastructure at both network access points and during data transmission (security of name and address management, routing security, transmission security) and relies on

appropriate architectural measures, the use of secure hardware and software platforms, and high-quality network management.

However, telecommunication security alone cannot guarantee information security. It is only one link in the security chain, as it is also essential to secure the IT infrastructure where programs are executed. In a broader sense, this includes the physical and environmental security of systems (user workstations, servers, or information systems).

2.2. Information security risk management

2.2.1. RISK

In the context of information security, risk is commonly understood as the potential for threats to exploit vulnerabilities, resulting in adverse impacts on an organization. According to ISO/IEC 27001 (2022), risk is defined as the combination of the probability of an event and its consequences. Similarly, ISO 31000 (2018) and AFNOR (2016) define risk as *"the effect of uncertainty on objectives"*, emphasizing the unpredictable nature of events that can hinder strategic or operational goals.

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:

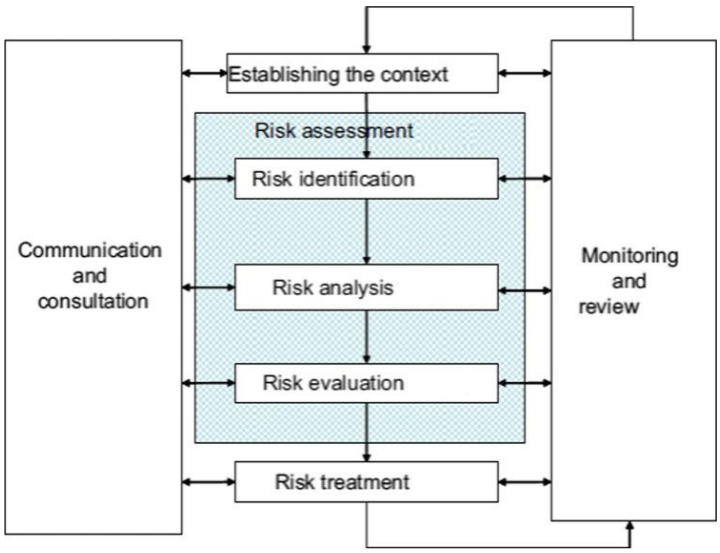
Risk = Threat × Vulnerability × Impact

- **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.

2.2.2. **Risk management principles**

Risk management involves a structured approach to identifying, assessing, and mitigating risks, particularly in security and cybersecurity contexts. It aims to protect systems and data from threats such as unauthorized access by maintaining awareness of risks, identifying issues, and responding to incidents (Sondes Ksibi, 2022). According to ISO 31000, the process includes key activities like communication, context establishment, risk assessment (identification, analysis, evaluation), risk treatment, and ongoing monitoring and review. This systematic approach ensures continuous improvement and resilience in managing risks.

Figure 5 Risk management process iso 31000



Source: (Sondes Ksibi, 2022)

Assets identification is the first step of the risk management process. It entails compiling a list of all of the organization's assets, be they business or system assets, that need to be protected. Some of these assets may include sensitive information, IT infrastructures, hardware, software, etc.

Once the assets are identified, security goals are associated with them. These security goals are used to preserve the confidentiality, integrity, and availability of the assets and also conform to the security requirements.

The risk is then analysed by finding out its causes, and thereby the potential threats that could act on the assets, and the vulnerabilities that could be exploited by these threats and its effect. Threats may be cyber-attacks, natural disasters, human mistakes, etc., while vulnerabilities are openings or frailties in processes or systems that threats might exploit.

In order to address risk, specific controls are applied based on the threats and vulnerabilities assessment. These may be technical security controls, antivirus software and firewalls; operational policies, data backup and access policies; and organizational controls, employee training and security awareness.

2.2.3. Types of information security risks

a. Technical Risk

Technical risks are caused by software, hardware, or network vulnerabilities. Malware attacks, such as the 2017 WannaCry ransomware that encrypted 200,000+ systems (Europol, 2017), exploit unpatched software. Social engineering and phishing, causing 74% of breaches (Verizon, 2023), trick users into sharing credentials. Zero-day exploits, such as the 2021 Microsoft Exchange breach (CISA, 2021), attack unknown vulnerabilities. Denial-of-service attacks, such as the Mirai botnet (Krebs, 2016), overwhelm systems. Mitigation includes patch management, MFA, and intrusion detection systems.

b. Human-Centric Risks

Employees unknowingly facilitate breaches. Insider attacks, responsible for 20% of attacks (IBM, 2023), result from negligence or malice. Weak passwords like "123456" (NordPass, 2023) and poor security awareness responsible for 85% of breaches (IBM, 2023) heighten risk. Mitigation includes training, password managers, and least-privilege access controls.

c. Organizational & Compliance Risks

Systemic government failures risk organizations. The Equifax breach of 147 million records in 2017 (FTC, 2019) highlights ineffective data protection. Fines for non-compliance, like Amazon's €746 million GDPR fine (CNIL, 2021), emphasize regulatory adherence. Third-party risk, including the SolarWinds attack (CISA, 2021), necessitates vendor assessments. Controls include audits, automated compliance tools, and incident response procedures (NIST, 2022).

d. Physical & Environmental Risks

Physical threats are device loss, improper access, and disasters. Lost laptops or drowned data centres (ISO 22301, 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, 2023), expose sensitive data. AI-created deepfakes, like the $25M CEO scam (CNN, 2023), enable high-profile frauds. IoT vulnerabilities, found in 57% of all devices (HP Wolf Security, 2023), provide entry points. Minimizing risks is by AI-detection technology and cloud security posture management (CSPM).

2.2.4. Risk calculation

The formula calculates risk by dividing the product of the threat and the vulnerability by the countermeasures. This means that:

• A high risk is associated with a high threat and high vulnerability, combined with weak countermeasures.

• A low risk is associated with a low threat or low vulnerability, or with strong countermeasures.

2.2.5. The process of risk management

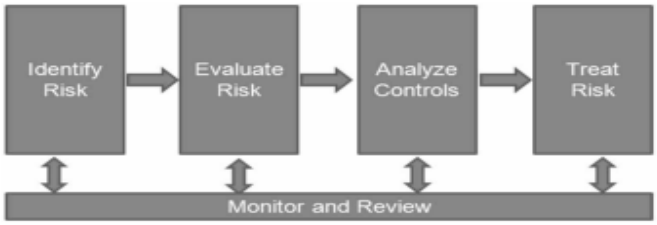
According to (Al-Dhahri, S., Al-Sarti, M., & Abdaziz, A., 2022)Firms ready to adopt a risk management process should, as an initial step, first establish an IT Risk Management Team. Such a team of individuals should oversee the process of risk management and guide the organization along the way. Moreover, roles and responsibilities should be defined. All the players should be assigned and alerted to invest a serious amount of time into the process. The basic IT risk management process can be found in Figure below. First, the organization's risks have to be defined and evaluated as to the impact the risks are able to have on the organization given its risk tolerance.

Then, the controls needed that already exist or must exist in order to mitigate the specified risks must be reviewed to treat the risk in the right manner which is the last step of the process. In the meantime, a regular monitoring and reviewing mechanism must be performed at the same time.

a. Identify Risks

Risk is the probability of a threat exploiting a vulnerability that can inflict damage on the organization's business processes. The owners of the risk have to designate the threats and vulnerabilities of the individual risks. There can be diverse approaches to identifying the risks. There is a point of observation that people coming from a technically oriented background approach risks in the context of vulnerabilities compared to people coming from a business-oriented background who approach risks in the context of threats.

Figure 6 The process of risk management



Source: (Al-Dhahri, S., Al-Sarti, M., & Abdaziz, A., 2022)

Risk owners would generally be nominated from the technical department of the organization due to the reason that they are with an understanding of the environment they are working within, and therefore, in a position to identify the areas of potential risk. When attempting to define risks, it is helpful to take a list of the individual risks along with the vulnerability which generates the risk and the asset which might be affected

b. Evaluate the Risks

To evaluate the risks, as there could be many, risk owners need to determine the likelihood and impact of the risk. This will provide a risk score that will, at a future point, help decide the risk that will take precedence during the treatment phase of the risk management process. Because it is impossible both in terms because of labour and cost limitations to mitigate all risks at once, the risk score will help organisations prioritize the risks that need to be treated urgently as opposed to others that may not even occur.

Figure 7 Risk Assessment Matrix

		Impact		
		Low	Medium	High
Likelihood	High	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

Source: (Al-Dhahri, S., Al-Sarti, M., & Abdaziz, A., 2022)

Likelihood is the probability that the organisation will be required to endure the risk and can be measured as a percentage or qualitatively as low, medium, and high.

Impact is the loss (tangible and intangible) the organisation will incur if the risk materialises. This could be a loss of an asset, an IT asset (server). and the cost to replace such an asset. Because there are assets whose contents hold information that is highly critical, loss of such an asset may be extremely costly, both in terms of resources and reputation to the organisation. The difference in the importance of an asset raises the question of asset value. Assets hold values of confidentiality, integrity and availability. And as stated earlier, an impact table needs to be created so as to provide standardization of the risk assessment. The impact values should be calculated in financial, reputation, loss of service and customer satisfaction terms. The ultimate risk score is usually calculated as the product of likelihood and impact. This is precisely inherent risk.

c. Analyse Controls

Inherent risk is the risk level without the application of any controls or measures in place. Organisations put controls in place to mitigate risks. They may be the result of other organisational processes like day-to-day operations change management, access management, configuration management. Some controls mitigate the likelihood level, and some mitigate the impact. For example, putting access management lowers the likelihood of unauthorized changes. Backup controls minimize the impact of a failure. The risk owner has to consider these controls and re-estimate the likelihood and impact of the risk. The re-estimated risk is referred to as residual risk. The risk owner has to act according to the severity of the risk.

d. Treat the Risks

The firm has to set a threshold for risk. Above this threshold, the risk owner will have to put new controls as a response to the risk. Each risk response will be determined based on cost-benefit analysis.

Some response strategies may be more expensive than their effects. Risk response strategies are:

• Risk Avoidance: preferring lower impact/cost risks alternatives

• Risk Sharing/Transfer: transferring or sharing the risk with/to other partner(s). For example, purchasing insurance is transferring a portion of the risk to the third party or outsourcing a service.

• Risk Acceptance: if it occurs, the loss subsequently would be accepted. Risks with low probability or low consequence are always accepted because most of the time it costs more to mitigate the risk than to accept it.

• Risk Reduction/Mitigation: taking action in order to lessen the likelihood or impact of the risk. A risk action plan is made and deadlines are set. This method is normally utilized for high likelihood and/or high impact risks.

e. Monitoring and Review

all the processes, inputs and outputs must be monitored in order to put in place an effective risk management process. There is supposed to be a risk committee to express the IT risk management of the firm.

At the end of the process, the outputs such as high-level risks, uncontrolled risks, and limitations are to be reported. The risk committee is required to include IT members

alongside other department members. there for Outputs are to be reported and integrated into enterprise risk management

2.2.6. Tools and Methods for Risk Analysis

Information system (IS) risk management is complex and requires a detailed understanding of concepts and processes. Faced with over 200 risk management approaches to select from, organizations are challenged in determining the most suitable technique. Organizations adapt customized methodologies and tools for structuring their risk management processes, tailoring these frameworks to their own needs or even developing in-house solutions. Some of the most widely used risk management methodologies include EBIOS, OCTAVE, and MEHARI. EBIOS, developed by the French Network and Information Security Agency (DCSSI), is primarily about articulating security requirements and defining primary goals. OCTAVE, developed by the Software Engineering Institute (SEI), is typified by emphasizing the use of internal organizational capabilities to assess threats and vulnerabilities. MEHARI, backed by the CLUSIF (French Information Security Club), offers an exhaustive, overall risk analysis methodology addressing both the strategic and the operational dimensions of information security.

On a normative basis, COSO and COBIT are widely recognized and applied. COSO, developed by the Committee of Sponsoring Organizations, is a comprehensive enterprise risk management framework, whereas COBIT, published by the Information Systems Audit and Control Association (ISACA), deals specifically with assessing and managing IT services in organizational settings.

Besides, numerous risk management tools are available whose selection largely depends on the nature and scale of the projects of the organization. Among the tools, Virtual Private Networks (VPNs) are most critical as they establish secure communication channels between devices and private networks, thereby guaranteeing data confidentiality, integrity, and availability during internet transactions. Similarly, issue and bug tracking software, such as Symantec's Bug Track, facilitates tracking, prioritisation, and remedying of software vulnerabilities. Business continuity planning tools are a requirement for the creation and maintenance of plans to attain or restore operations continuity in light of potential threats or disruptions. Lastly, vulnerability scanners such as Nessus play an important role in determining the security stance of networks by discovering likely vulnerabilities and providing detailed reports for use in effecting corrective measures

While the two methods widely used in France: EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) and MEHARI (Méthode Harmonisée d'Analyse de Risques). These methods distinguish an organization's assets from technical vulnerabilities and threats to identify potential risks and propose appropriate security measures to mitigate them.

Among these solutions are risk analysis methods for information systems. The most commonly used methods are :

– EBIOS (expression des besoins et identification des objectifs de sécurité) développée par l'agence nationale de la sécurité des systèmes d'information (ANSSI).

– MEHARI (méthode harmonisée d'analyse des risques) développée par le club de la sécurité de l'information français (CLUSIF).

– CRAMM (CCTA Risk Analysis and Management Method) développée par l'organisation du gouvernement britannique ACTC (agence centrale de communication et des télécommunications).

–OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), développée par l'université de Carnegie Mellon aux États-Unis. (Salia, 2023)

❖ **EBIOS**

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives) (GRALL, 2018) is a method for analysis, evaluation and action on risks relating to information systems. It generates a security policy adapted to the needs of an organization. The method was created in 1995 and is now maintained by the ANSSI, a department of the French Prime Minister.

The five steps of the EBIOS method are:

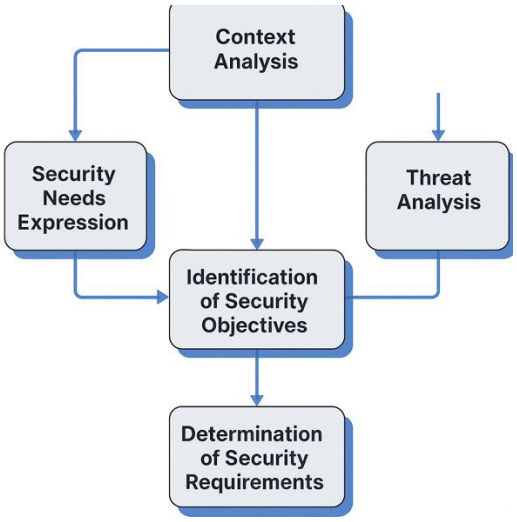
1. **Context Analysis:** This initial phase
2. aims to comprehensively identify the security target and contextualize it within its operational environment. It involves the identification of constraints imposed on the security target, ensuring a thorough understanding of its functional and regulatory boundaries.
3. **Articulation of Security Requirements:** At this stage, a structured inventory of functional security needs is established these are fundamental requirements that the proposed solution must fulfil, independent of any specific technological implementation. Security needs are defined in relation to key security principles, including availability, integrity, and confidentiality, ensuring a robust foundational framework.

4. **Threat Assessment:** A rigorous threat analysis is conducted to facilitate risk evaluation. This phase is designed to systematically identify potential threats affecting the security solution. The threats recognized at this stage are uniquely tailored to the security target, with their characterization being directly contingent upon the functional security requirements outlined earlier.

5. **Definition of Security Objectives:** This step entails an in-depth examination of the potential impact of identified threats on functional security needs. A risk gradation model is employed to establish security objectives that the system must achieve to maintain a secure and resilient operational state. These objectives form the cornerstone of the security strategy, ensuring that identified risks are adequately mitigated.

6. **Specification of Security Requirements:** Based on the previously established security objectives, a comprehensive set of security requirements is formulated. These requirements delineate, with high precision, the specific security functionalities essential for addressing all security objectives. This ensures the integration of security mechanisms that provide an optimal level of protection while aligning with the overarching risk management strategy.

Figure 8 EBIOS risk management steps



Source: (GRALL, 2018)

EBIOS is primarily designed for governmental and commercial entities, particularly those collaborating with the Ministry of Defence and handling confidential or classified defence information. Its primary function is to facilitate well-informed security decision-making. The methodology serves two key objectives: first, to anticipate and prepare for potential

security challenges in newly developed information systems; and second, to identify vulnerabilities and implement corrective measures in operational systems, thereby enhancing security protocol

❖ MEHARI

The MEHARI method (Harmonized Risk Analysis Method) was developed in the 1990s by CLUSIF *(Club de la Sécurité de l'Information Français – French Information Security Club*). Initially, this methodology focused solely on risk analysis. Over time, it has evolved to support the comprehensive management of an organization's security within an open and geographically distributed environment.

MEHARI Method

The MEHARI method has been widely adopted by thousands of organizations globally and remains the leading risk analysis approach in France, particularly within the industrial sector. Its software is freely accessible for use and distribution, and several knowledge bases are available to support its implementation. Additionally, a case study has been developed to illustrate its application and facilitate user adoption.

MEHARI is rooted in two earlier methodologies that have since been phased out: MARION (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau) and MELISA (Méthode d'Évaluation de la Vulnérabilité Résiduelle des Systèmes d'Armement).

In contrast to the EBIOS method, which follows a different analytical approach, MEHARI is structured around risk scenarios, enabling organizations to systematically identify potential threats within their operational environment. It is designed as a comprehensive security management framework, offering adaptability in risk assessment based on strategic priorities, organizational policies, or specific situational requirements. The methodology is structured into modular components, each focused-on risk evaluation and mitigation, ensuring a tailored and dynamic approach to security management.

The MEHARI methodology is structured into three key modules, each designed to provide a systematic approach to risk analysis and security management.

Module 1: Risk Analysis and Classification

This module focuses on identifying and assessing an organization's assets while evaluating security-related challenges. It is built upon four fundamental principles:

1. Establishing Methodological Metrics This step involves defining the methodology's quantification parameters, including the assessment of likelihood, impact, and overall risk levels.

2. Prioritization of Security Objectives The organization's leadership sets security priorities based on its specific operational context and strategic goals.

3. Asset Classification Organizational resources are systematically identified and categorized according to their criticality in terms of availability, integrity, and confidentiality.

4. Implementation of Security Policies and Guidelines This phase ensures the formalization and deployment of the organization's security policies and governance framework.

Module 2: Security Services Management

This module leverages the MEHARI knowledge base on security measures to address vulnerabilities through structured action plans. Key activities include:

- Identifying and mitigating weaknesses in security controls.
- Evaluating the effectiveness of implemented security measures.
- Assessing residual risks resulting from existing vulnerabilities.
- Conducting security audits based on recognized standards and best practices.

Module 3: Risk Scenario Analysis

This final module synthesizes the results from previous security measures and provides a dynamic assessment framework. It involves:

- Selecting performance indicators aligned with the objectives defined in Module
- Comparing actual security outcomes against predefined benchmarks.
- Establishing a continuous monitoring system to track the evolution of information security levels over time.

The MEHARI approach is characterized by a top-down security governance model, where strategic decisions are delegated from executive management to operational entities. This structure makes MEHARI particularly well-suited for multi-environment organizations that require a harmonized security management system. Furthermore, the methodology aligns with the requirements of ISO/IEC 27001, ensuring compliance with internationally recognized information security standards.

❖ **FMECA**

Failure Mode and Effects Analysis (FMECA), known in French as AMDEC (*Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité)*, is a structured and systematic methodology used to identify potential failure modes within a system, analyse their effects,

and assess their criticality. It is an inductive method that combines both qualitative and quantitative dimensions to evaluate the security, reliability, or robustness of systems. According to Benabdellah (2022), FMECA examines possible system failures, their causes, and the consequences of those failures on overall performance. Through prioritization based on risk levels (criticality), it helps to initiate and monitor corrective and preventive actions aimed at mitigating or eliminating failures.

Historical Context of FMECA

The earliest history of the FMECA technique stretches back to the 1940s in America, where it was originally designed for military and aerospace uses with an emphasis on enhancing the dependability of advanced systems. (Faucher, 2006)It was later applied in manufacturing sectors such as automobiles, energy, and industrial operations. Over time, FMECA has evolved into an even more powerful tool that helps in the risk management of digital systems and information security systems. Faucher states that its application has been expanded to include information systems and cybersecurity because of the increasing complexity of digital platforms and the need for systematic risk identification and prioritization.

Types of FMECA

FMECA can be classified into different types depending on the field of application:

- Design FMECA (DFMECA): Looks for product design failures that could affect quality or safety.
- Process FMECA (PFMECA): Observes operational or production processes, reviewing for possible defects in workflow or system functions.
- System FMECA: Looks at system-level risks and subsystem failure interactions, particularly useful for complex IT environments.
- Software FMECA: Looks for software-specific failures such as security flaws or programming errors, which are essential in digital media.

Key Characteristics of the FMECA Technique

The technique consists of a number of key steps:

- Identification: Listing all the potential failure modes of a given system or process.
- Assessment: Analysis of the causes and consequences of each failure.
- Prioritization: Calculation of a criticality score using the formula:

$$\mathbf{C = S \times O \times D}$$

where:

- S (Severity) is the seriousness of the consequences,
- O (Occurrence) is the probability that the failure will occur,

- D (Detection) is the probability that the failure will be discovered before it can have a detrimental effect.
- Action: The implementation of corrective and preventive measures to reduce the effect or probability of failures.
- Monitoring: Regular inspection and adjustment of measures to take account of the changing nature of risk.

❖ **FMECA Implementation Process**

The FMECA implementation, according to (Faucher, 2006), consists of the following formal steps:

1. System Definition: Define the limits of the system or process to be analysed
2. Failure Mode Identification: List all defined or potential failure modes (data breaches, server failure).
3. Cause and Effect Analysis: Identify the root causes and effects of every failure.
4. Risk Evaluation: Calculate the Risk Priority Number (RPN) using severity, occurrence, and detection ratings (1 to 4 scale).
5. Prioritization: Rank the failure modes by RPN to determine those requiring high-priority intervention.
6. Action Planning: Suggest risk reduction activities, software changes, user training, or system redesign.
7. Review and Monitoring: On a regular basis, review the performance of actions taken and update as appropriate to make sure continuous improvement.

This official approach assists in making sure organisations actively manage expected and unexpected risks in their digital systems.

Relevance to Sustainable Digital Risk Management

In digital sustainability, particularly initiatives such as the Smart Green Campus, FMECA provides an important framework for security assurance, performance, and environmental congruence. FMECA helps to recognize and rank potential digital system vulnerabilities and therefore finds itself aligning with the broader goals of sustainable development, including minimizing digital waste, improving data protection, and ensuring guaranteed continuity of service. FMECA promotes anticipatory and systemic reaction to cyber and operational threats in digital transformation initiatives.

2.3. Sustainability and information security

Sustainability is a multifaceted concept which has risen to the top of modern development philosophy, ranging from information system design to risk management. According to the Brundtland Report (1987), sustainability has been defined as the ability to "*meet present needs without compromising the ability to meet future ones*" (World Commission on Environment and Development, 1987). This definition at the roots reveals the sense of intergeneration obligation in sustainable development. United Nations (2015) complements this with a further declaration that sustainability encompasses bringing into realization the balance of economic development, conservation of environment, and inclusivity, such as in the case of 17 Sustainable Development Goals (SDGs). Furthermore, the International Organization for Standardization (ISO 26000:2010) widens the scope by placing sustainability in the framework of social responsibility, highlighting stakeholder expectations to be included, compliance with law, and action by the organization. Together, these definitions put a focus on the necessity for an integrated, long-term approach towards development one that is on the basis of ethical, environmental, and governance principles

Sustainable development cannot exist without secure digital infrastructures. By embedding information security into governance structures, organizations support long-term resilience and responsible innovation.

2.3.1. Green IT and Energy Efficiency

The shift towards environmentally friendly technologies relies increasingly on Green IT, its mission to reduce environmental imprints left by information systems by optimal use of power, reducing digital wastage, and adopting green methods. Adding an Information Security Management System such as ISO 27001 reinforces these efforts because it brings with it a dimension of safe, sound, and compliant bases. Impressive advancements in green cryptography, like the post-quantum algorithm CRYSTALS-Kyber, lead to up to 40% less energy consumption compared to normal RSA encryption (Leclerc et al., 2023). Meanwhile, infrastructure virtualization with the aid of tools like VMware provides server consolidation, reducing the hardware needs by 60% and power consumption drastically (Benzidia et al., 2023). At a larger scale, companies like Google have carbon-sensitive data centres that dynamically shift workloads to renewable-energy-based areas, resulting in a 30% decrease in carbon emissions (Google Sustainability, 2024). In Algeria, the USTHB Smart Green Campus initiative is a fine example of this intersection of sustainability and security through the combination of solar-powered edge computing with ISO 27001 controls, which led to a

25% reduction in energy consumption while blocking 98% of cyberattacks (Benali et al., 2023). To advance these efforts, organizations are encouraged to conduct energy audits using tools like Microsoft's Sustainability Calculator, migrate legacy encryption to NIST-recommended post-quantum algorithms, and integrate ISO 27001 into their long-term sustainable cybersecurity strategies.

2.3.2. Risk Management for Sustainable Digital Infrastructure

The growing digitization of essential infrastructure such as power grids, water supplies, and industrial plants creates new vulnerabilities that, when exploited, have the potential to cause devastating environmental and societal damage. Cyberattacks on such infrastructures not only cause disruptions to essential services but also squander energy, pollute resources, and compromise sustainability initiatives. For example, a 2023 cyberattack on a German wind farm resulted in the loss of 300 MWh of renewable energy, enough to supply 100 homes for a year (IEA, 2024). Likewise, the 2021 Oldsmar water system hack in Florida came close to causing a public health disaster when hackers tried to change chemical levels in the drinking water supply (CISA, 2022). To mitigate such threats, organizations are implementing risk management standards like the NIST Cybersecurity Framework (CSF) and ISO 27005 that provide a structured approach to discover, analyse, and oversee cyber threats. Compliance requirements like NIST SP 800-53 also mandate the encryption of industrial IoT devices used in critical infrastructure to ensure protection from unauthorized access. ANSI Critical Infrastructure Guidelines (2020) require Algeria to implement NIST-based security controls for water and smart grid systems, enhancing national resilience against cyber-attacks. Beyond compliance, proactive initiatives are called for, including sustainability-focused risk analysis modelling the carbon footprint of cyber-attacks, and OT and IT convergence security training specialized in Operational Technology, such as Siemens' Cybersecurity for Energy Systems program. Through the integration of cyber resilience and sustainability, organizations are able to deliver both the security and environmental performance of digital infrastructure**.**

2.3.3. IoT Security in Smart and Green Environments

The large-scale deployment of Internet of Things (IoT) technology across smart cities, campuses, and grids is an essential enabler of sustainable development goals, particularly increased energy efficiency and dynamic management of resources in real time. The built-in cybersecurity vulnerabilities of IoT systems pose severe risks to both operational integrity and environmental sustainability. For instance, insecure smart meters were found to double energy wastage as much as 20%, cancelling out any environmental benefits (Khan et al.,

2024). In this respect, Algeria's ANSI IoT Standard (2021) mandates post-quantum encryption algorithms to protect IoT devices from advanced persistent threats, particularly in critical infrastructure. One of the major applications of secure IoT in the real world is the Algiers Smart City project, wherein the use of secure streetlight sensors lowered power consumption by 30% and also successfully repelled over 1.2 million cyberattacks per month (Benali et al., 2023). To increase the resilience of such infrastructures, stakeholders are recommended to apply NIST IR 8259 for establishing IoT cybersecurity baselines and use zero-trust architectures to secure device communication in smart grids. By integrating cybersecurity into the very core of IoT systems, smart environments can achieve their dual objectives of technological innovation and ecological sustainability

2.3.4. ISO 2700 Family: Core Standards & Sustainability Links

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 2700X family and sustainability

Standard	Purpose	Sustainability Link
ISO/IEC 27001	Requirements for establishing, implementing, and maintaining an ISMS.	Mandates energy audits for data centres, aligns with Green IT strategies (solar-powered edge computing).
ISO/IEC 27002	Guidelines for selecting security controls (encryption, access control).	Supports secure lifecycle management of IT assets, reducing e-waste through reuse/recycling.
ISO/IEC 27005	Risk management framework for ISMS.	Assesses environmental impact of cyber risks (attacks on smart grids wasting energy).
ISO/IEC 27009	Sector-specific adaptations of ISO 27001 (healthcare, energy sectors).	Tailors' security to sustainable industries (e. securing Algeria's renewable energy grids).

Standard	Purpose	Sustainability Link
ISO/IEC 27013	Guidance on integrating ISO 27001 with ISO 20000 (IT service management).	Optimizes IT operations for energy efficiency (cloud resource allocation).
ISO/IEC 27014	Governance of information security.	Ensures alignment of security policies with ESG goals (GDPR/CSRD compliance).
ISO/IEC 27032	Guidelines for cybersecurity in cyberspace.	Protects IoT ecosystems in smart cities, ensuring energy/resource optimization.

Source: developed by us based on the theorical framework

This comprehensive review of literature reveals the intricate interplay between information systems governance, risk management, and sustainability in the digital age. Through examining diverse theoretical frameworks and empirical studies across international and local contexts, several key insights emerge. First, effective IS governance transcends mere technical implementation, requiring careful adaptation to organizational contexts while balancing global standards with local realities as evidenced by the gap between COBIT frameworks and their practical application in settings like Algeria's public education sector. Second, successful Information Security Management Systems depend on multidimensional factors beyond technology, including organizational culture, leadership commitment, and regulatory alignment. Third, risk management approaches have evolved from reactive measures to strategic imperatives, with methodologies like FMECA demonstrating particular value when adapted to information security contexts through integration with approximate reasoning-based logic and decision-theoretic models. Perhaps most significantly, this review highlights the emerging synergy between information security and sustainability initiatives in order simultaneously strengthen their digital resilience and environmental responsibility. As digital transformation continues to reshape organizational landscapes while this conceptual framework offers a foundation for future research and practice one that recognizes the essential role of secure, well-governed information systems in achieving sustainable development objectives across sectors, from smart campuses to financial institutions. The integration of these domains not only addresses current challenges but also anticipates future directions where information security becomes inseparable from broader sustainability goal

Chapter III

METHODOLOGICAL FRAMEWROK

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 management under the context of a sustainable development project.

1. Presentation of the Research Methodology: Action Research

In the context of our study, we have chosen action research as our research approach. This methodology is particularly well-suited for exploring and improving risk management practices related to information security within the implementation of sustainable digital solutions at ESHRA, notably as part of the Smart Green Campus initiative. It allows for the active involvement of key stakeholders in a collaborative process of reflection and action.

Action research is inherently qualitative in nature (Kemmis, 2000). According to (Coghlan, 2014), "qualitative research aims to provide a comprehensive understanding of a phenomenon through the construction of a model." Initially developed in the 1940s by German psychologist Kurt Lewin, action research stems from the social sciences (Checkland, 1998). As noted by Lewin, it is possible to make theoretical advancements while simultaneously fostering social change through action research.

(Reason, 2008)defines action research as "*a participatory process concerned with developing practical knowledge in the pursuit of worthwhile human purposes. It seeks to bring together action and reflection, theory and practice, in participation with others, in the pursuit of practical solutions to issues of pressing concern to people, and more generally the flourishing of individuals and their communities*." Practical action research is thus based on the idea of integrating field experience with theoretical inquiry in a complementary manner. This principle makes it possible to balance theoretical reflection with the uncertainties that may arise during real-world implementation, as emphasized by (Walsham, 1995). Unlike approaches focused purely on theory-building, action research aims to resolve concrete problems while drawing on theoretical insights.

Steps of Implementation

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

Diagnostic Phase: The initial step is to diagnose the current risk management practices in ESHRA through in-depth interviews and observation of key stakeholders involved in the

Smart Green Campus project. It will determine prevailing issues, loopholes, and areas of improvement with regard to information security and sustainability.

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 and sustainability goals.

Evaluation Stage: The final step involves assessment of the solutions put in place through processes such as FMECA to ascertain their effectiveness towards risk mitigation and improvement of information security. The stage will also include stakeholder feedback to assess and improve the solutions based on their practical impact and viability.

This methodology is particularly appropriate for our research, which examines the integration of information security risk management into the Smart Green Campus project at ESHRA. Our goal is to contribute to the development of secure and sustainable digital practices by engaging with internal stakeholders and co-constructing practical, context-sensitive solutions.

We justify our choice of a qualitative action research approach for the following reasons:

- Through our literature review, we observed that qualitative approaches are commonly used in research addressing the intersection of information systems, risk management, and sustainability
- Action research is particularly appropriate for improving practices and performance in organizational settings. In our study, we aim to identify ways to enhance the management of information security risks within a sustainability project, by actively collaborating with the stakeholders involved in the Smart Green Campus project.
- Action research makes use of several qualitative data collection methods, such as observation, document analysis, and interviews. These methods will enable us to gather detailed insights into current practices, perceptions, and needs, in order to design effective and sustainable interventions.

2. Data Collection Method

Data gathering is the systematic process of collecting and getting information about the variables of interest in the hope of providing answers to some questions of research, testing hypotheses, and evaluating results. It is key to all scholarly disciplines, such as the physical and social sciences, the humanities, and business administration. While the specific

procedures employed might vary between fields, the emphasis on accuracy, clarity, and ethical integrity in data collection is of paramount significance to all fields. The ultimate aim of data collection is to generate high quality evidence that enables viable examination and provides support for sound and persuasive conclusions. Regardless of whether research is conducted using quantitative or qualitative data, the precision with which data are gathered is fundamental to the validity and reliability of the research endeavour overall. The decision on appropriate data collection techniques available, adapted, or created from scratch moreover establishing explicit protocols for their application drastically reduces the likelihood of mistakes and maximizes the validity of the findings.

The Central Position of Data Gathering in Research

Data collection is a fundamental process in the execution of any research study where it is a highly intricate process that demands meticulous planning, methodological consistency, patience, and unwavering commitment to ensure success. The process begins with the identification of the specific type of data to be gathered in an effort to meet the research requirements. This is followed by the accurate selection of a representative sample from a given population. Then the researcher must use an effective data collection instrument to obtain appropriate data systematically from the selected sample. All these activities must be carried out with precision so that research outcomes can become reliable and valid

2.1. Observation

Observation is a built-in method for understanding complex and often hard-to-perceive environments, particularly within organizations. While human perception enables us to interpret our surroundings through our senses, observation as a research methodology goes beyond merely seeing and hearing. As (Stenhouse, 1975)defines research as a "systematic inquiry made public," observation, to serve this purpose, must be conducted with methodological rigor and precision.

In environments overloaded with information, researchers must consciously focus on specific elements deemed most critical to their investigative goals. Within this research, observation was employed in a focused and structured way to capture essential features of the organizational environment, particularly in relation to information security governance and sustainability strategies.

This approach required the development of predefined observational criteria, such as employees' compliance with security protocols, the integration of digital tools into daily workflows, and the degree to which technological solutions are understood and aligned with

sustainable practices. To ensure transparency and analytical reliability, all observations were systematically documented, allowing for thorough and careful interpretation.

Observation proved especially valuable in evaluating the organization's management culture, adherence to established procedures, and the extent to which secure and sustainable digital technologies were effectively implemented key dimensions in building intelligent, resilient, and environmentally responsible information systems. (Thietart, 2017)

Unstructured non-participant observation is what we adopted in this study because this method to better understand the real-life context in which the Smart Green ESHRA project is evolving. By observing the behaviours, interactions, and dynamics within the institution from an external standpoint, we were able to gather rich, spontaneous insights that would not necessarily emerge through interviews alone. This approach provided valuable contextual elements on how sustainability and information security principles are applied in practice, and it contributed to a deeper interpretation of the data obtained through other qualitative methods.

2.2. Documentary Research:

Document analysis is a qualitative research method that involves the structured and systematic review of written sources such as reports, journal articles, books, field notes, and archival records. It serves as a valuable tool for exploring research questions and generating data for case studies, field investigations, and comparative analyses (Kempf, 2000)

In our study, document analysis will primarily focus on internal and institutional sources collected during the observation phase. This includes Smart Green Campus project documents, such as strategic planning files and progress reports, as well as internal audits and evaluation records relevant to information systems. We will also examine content published on ESHRA's institutional website, which reflects its sustainability goals and digital initiatives. Additionally, although ESHRA does not have formal internal security policies, the institution refers to established information security standards as part of its risk management efforts. These include international frameworks and technical documentation aligned with best practices. The analysis will also integrate the Algerian Law 18-07 on the protection of personal data, which provides a legal framework for information security practices in public institutions. These documents will help identify existing practices, highlight areas for improvement, and support the triangulation of data collected through interviews and observations.

2.3. 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 three principal research interview types:

a. Structured Interview (Directive Interview):

Also called a standardized interview, this type of format follows a rigid structure to give similar questioning conditions to all the respondents. The rigid structure facilitates comparison of results. Questions are typically closed-ended, requiring yes/no answers or multiple-choice responses, which can be readily subjected to statistical analysis.

One of the advantages of this method is that interviewers have questions prepared, which can be used to make the interviewee feel comfortable. A major disadvantage, however, is the lack of flexibility, the interviewer cannot follow up in greater detail on a topic or easily establish a rapport with the participant.

b. Unstructured Interview (Open or Non-directive Interview):

Also known as an "open interview," this type is defined by the lack of set format or prepared questions. The interviewer states a broad topic and intervenes only to urge the respondent to continue or expand. The interviewer takes on a listening, understanding, and neutral position. This method allows the respondent to speak freely and expand on their ideas, perhaps revealing new hypotheses in the process.

Yet the conversation can be derailed from the intent, since the respondent may provide responses that are unrelated to the primary question. The researcher will need to redirect the conversation back on course when needed, which can place additional workload on the researcher.

c. 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 a component of our research aimed at information security risk management in sustainable digital transformation, we chose semi-structured interviews for two reasons. Firstly, this is a method that facilitates gathering abundant and varied information without being too prescriptive regarding outcomes beforehand. Secondly, using an interview guide, there is a safeguard from permitting the conversation to digress from our research objective while allowing space for examining related emerging issues.

a. Interview guide

The interview guide was developed to ensure the depth and organization of our research. It aims at experts and stakeholders in information systems governance, digital security, and sustainability especially in the scope of the Smart Green Campus project. The guide is composed of two general categories:

- General Section:

Developed to understand the background, role, and involvement in smart green ESHRA project

- Thematic Section on Risk Management and Sustainability Practices

With a focus on information security risk attitudes and practices, such as risk determination, mitigation approaches, tools and standards applied, organizational challenges, alignment of digital tools with sustainability objectives, and suggestions for establishing resilience and long-term digital sustainability. This model was developed to align with our primary study research questions. We ensured ethical compliance by assuring confidentiality and using the information obtained only for study and research purposes ANNEX

b. Justification for Sample Selection

The sample selected for our research consisted of five employees from ESHRA. These individuals were chosen due to their direct involvement in the Smart Green Campus project and based on organizational constraints related to availability and access. Given their roles

in the institution's digital and sustainability initiatives, they represent key stakeholders for understanding the management of information security risks in this specific context.

The saturation of data will be evaluated after the interview analysis, in order to ensure that the collected insights are sufficient to draw meaningful conclusions and reflect recurring themes within the scope of the study.

Table 3 The interveiwees

Interviewee	Position	Date & Location	Duration
Interviewee 01	CHEF IT DEPARETEMENT	EHSRA	1 : 45 Min
Interviewee 02	AUDITOR	EHSRA	1 :13 Min
Interviewee 03	one of the interviewees of ESHRA	ESHRA	25 Min
Interviewee 04	A member in the project (RSE doctor)	ESHRA	50Min
Interviewee 05	A member in the project (responsible for ai; doctor)	ESHRA	30Min

Source :Devoleped by us

4. Data treatment

In this study, data treatment will be conducted in two complementary phases. First, qualitative data from the semi-structured interviews will be analysed using NVivo 15, a specialized software for qualitative research. This tool will help code and categorize the interview content, allowing the identification of key themes, recurring patterns, and significant insights related to information security risks and sustainable practices. Once the qualitative analysis is complete, the results will serve as a foundation for the second phase, where the FMECA (*failure mode effect and criticality analysis*) method will be applied. FMECA will be used to evaluate and prioritize the identified risks in a structured and systematic manner, enabling the proposal of targeted actions to strengthen information security within a sustainable digital context.

4.1. Nvivo15

NVivo is a strong qualitative data analysis computer software that allows researchers to organize, analyse and interpret big volumes of data, for instance, interview transcripts. It has sophisticated features for coding, classifying, and visualizing text data, making it an extremely useful computer program for gleaning useful information from qualitative research. we used NVivo 15 to analyse data from the interviews and data gathered in this research. The instrument helped me systematically examine the responses and identify broad themes and trends with regard to information security risks and risk management measures. we were able to draw out specific risk factors, establish their implications, and ensure proper understanding of the issues faced while managing security risks.

4.2. FMECA (Failure Modes, Effects, and Criticality Analysis)

To evaluate and prioritize potential risks associated with information security, an FMECA (Failure Modes, Effects, and Criticality Analysis) matrix was developed. This structured risk assessment tool helps identify critical failure points and supports the formulation of targeted action plans to mitigate them. The matrix is organized into the following key components:

Activities or Operations includes essential security-related processes and operations within the digital platform that are subject to risk evaluation.

Observations capture relevant observations collected during the analysis phase, especially after the implementation of corrective or preventive measures.

Constraints lists limitations or conditions that may affect system performance, such as technical, organizational, or compliance-related constraints.

Failure Mode describes potential failures or vulnerabilities for each activity answering the question: "What could go wrong?"

Potential Effects specifies the likely consequences of each failure mode: "What would happen if this failure occurred?"

Possible Causes identifies root causes behind each failure: "Why might this failure occur?"

Severity (S) evaluates the impact of each failure on a scale from 1 (low impact) to 4 (very severe impact).

Occurrence (O) estimates how often the failure is likely to occur, rated from 1 (rare) to 4 (very occurrent).

Detection (D) assesses the likelihood of detecting the failure before it causes damage, using a scale from 1 (very likely to detect) to 4 (very unlikely to detect).

Criticality (C) represents the overall level of risk, calculated as C = S × F × D. This score helps prioritize risks for treatment.

Action Plan proposes concrete corrective or preventive measures to eliminate or reduce the likelihood of each failure.

Responsibility assigns accountability for the execution of each action plan to specific individuals or teams.

This table down below presents a 4-level rating scale for the three key criteria used in FMECA (*Failure Modes, Effects and Criticality Analysis*): severity, occurrence, and detection. These criteria are fundamental for systematically identifying, assessing, and prioritizing potential failures within a system or process. By providing a structured evaluation framework, the table facilitates the identification of critical risks and supports the design of targeted action plans aimed at reducing vulnerabilities and improving the overall reliability and safety of the system under analysis.

Table 4 scale of the criteria (severity, concurrency, detection)

Scale	Severity (S)	Occurrence (O)	Detection (D)
4	Catastrophic	Very Occurrent	Undetectable
3	Critical	Occurrent	Hard to Detect
2	Moderate	Occasional	Detectable
1	Acceptable	Rare	Easily Detectable

Source: Developed by us

Our research adopts a qualitative methodological framework grounded in action research, supported by data collection techniques such as observation and semi-structured interviews. To enhance the rigor of the analysis, qualitative data were processed and coded using NVivo 15, enabling a structured and in-depth thematic exploration. This methodological approach allows for a nuanced understanding of the security challenges faced by digital platforms and supports the development of contextually grounded, actionable recommendations. Particular attention is given to assessing the relevance and effectiveness of the FMECA (Failure Modes and Effects and criticality Analysis) methodology as a strategic tool for risk management and decision-making.

Chapter IV

Results Analysis and discussion

This chapter presents the analysis and discussion of the findings obtained through qualitative interviews with key stakeholders involved in the Smart Green Campus project at ESHRA. The objective of this research is to explore how information security risk management can support sustainable digital transformation in a higher education context. Specifically, it aims to examine the relationship between information security risk management within IT governance, and sustainability within the Smart Green Campus initiative.

Section 1: Results analysis

1. Diagnostic of Information System and Sustainability Practices at ESHRA

This section provides an overview of ESHRA's existing information system infrastructure and its alignment with current sustainability practices. The diagnostic focuses on identifying strengths and weaknesses in the governance of digital resources, the level of integration between technological tools and sustainability objectives, and the degree of awareness among stakeholders regarding information security and environmental responsibility. It sets the foundation for understanding the institutional context and framing the subsequent risk analysis.

Figure 9 Word cloud of the general overview of the Thematic area

Source: developed by us using Nvivo15

The word cloud generated with NVivo 15 offers a preliminary diagnostic of the thematic landscape emerging from the interviews. Dominant terms like 'information', 'security', and 'systems' indicate that information security risk management is a central concern for stakeholders. The presence of words such as 'sustainability', 'green', and 'smart campus'

reflects the project's strong alignment with sustainable development objectives. Meanwhile, the frequent appearance of terms like 'governance', 'compliance', and 'risks' suggests an awareness of the need for structured frameworks to guide secure and responsible digital transformation. The recurrence of operational terms such as 'infrastructure' and 'cybersecurity' highlights the technical challenges tied to implementing these ambitions

1.1. Vision of Sustainability in the Smart Green Campus Context at EHSRA

The analysis of semi structured interviews reveals a multidimensional vision of sustainability within ESHRA's Smart Green Campus project. This vision articulates around several complementary axes that demonstrate a holistic approach integrating technological, organizational, and human considerations.

Figure 10 word cloud of Vision of Sustainability in the Smart Green Campus Context

Source: developed by us using Nvivo15

1.1.1. Integration of Sustainability into Digital Strategy

Sustainability appears as a central and structuring element of the Smart Green Campus project, as explicitly emphasized by one of the interviewees: "Sustainability is central to Smart Green Campus". This centrality demonstrates an institutional commitment to anchor digital initiatives within a sustainable development perspective. The IT engineer perceives this initiative as a strategic opportunity to align information technologies with sustainability objectives: "The Smart Green Campus is a chance to align IT with sustainability".

This strategic vision translates into concrete initiatives aimed at transforming technological infrastructure. The IT engineer mentions the exploration of "energy efficient systems and eco-friendly storage solutions "while one of the interviewees refers to tangible improvements: "We're improving energy efficiency in our data centre and we are able to

adopt greener hardware while maintaining security". These testimonies illustrate a pragmatic approach where energy efficiency and the adoption of more environmentally friendly hardware constitute priority intervention areas

The auditor confirms this trend by noting the increasing integration of "sustainability considerations such as energy efficiency and eco design" in audit processes, although these practices are still in their early stages. This observation suggests a progressive evolution of evaluation frameworks to integrate sustainability criteria.

1.1.2. Synergies Between Information Security and Sustainability

A particularly significant aspect emerging from the interviews is the recognition of synergies between information security management and sustainability objectives. The auditor clearly identifies these "synergies between robust information security management and achieving sustainability goals, especially within the Smart Green Campus initiative". This perspective is reinforced by one of the interviewees, who categorically states: "Cybersecurity and sustainability go hand in hand; if it's not secure, it's not sustainable". This statement establishes a fundamental link between these two dimensions, suggesting that the sustainability of information systems necessarily relies on their security.

This integrated vision is also manifested in the IT engineer's approach who, while acknowledging that "Right now, our focus is security like surveillance and data protection", expresses the ambition to "transition toward sustainable technologies". This evolutionary perspective indicates a development trajectory where security constitutes a prerequisite for the adoption of sustainable technologies.

1.1.3. Technological Innovation Serving Sustainability

Technological innovation appears as an essential lever for realizing the vision of sustainability. one of the interviewees, as the AI lead for the Smart Green ESHRA project, expresses marked optimism regarding "the implementation of emerging technologies to drive sustainability and innovation". This vision translates into concrete achievements, such as the development of an "application focused on energy efficiency to monitor and optimize consumption across campus buildings". This initiative perfectly illustrates the use of advanced technologies like AI to achieve measurable sustainability objectives.

In the same vein, one of the interviewees mentions the development of specific tools such as "an open-source project management platform and a centralized information portal", demonstrating the importance given to open and integrated technological solutions to support the vision of sustainability.

1.1.4. Human and Cultural Dimension of Sustainability

Beyond purely technological aspects, the interviews reveal a strong awareness of the human and cultural dimension of sustainability. one of the interviewees clearly identifies that "The challenge isn't funding it's cultural resistance to new, sustainable practices". This observation highlights that obstacles to sustainability are not primarily financial or technical but rather relate to cultural resistance to change.

This perspective is also present in the auditor's testimony, which mentions the "challenges persist in embedding sustainability fully within the security governance framework, including cultural resistance and limited formal policies linking these domains". These observations emphasize the importance of addressing cultural and organizational aspects to successfully integrate sustainability into institutional practices.

one of the interviewees offers a particularly profound vision of sustainability by stating that "Real sustainability means forming competent leaders, able to adapt and innovate in an uncertain world". This conception considerably broadens the notion of sustainability beyond environmental or technological considerations, anchoring it in the development of adaptive and innovative leadership skills.

1.1.5. Education and Awareness as Pillars of Sustainability

Education and awareness emerge as essential components of the sustainability strategy. one of the interviewees mentions the organization of "workshops are held to raise awareness among staff about password management, data sharing, and cybersecurity". These educational initiatives aim to develop a digital security culture that underpins sustainable practices.

one of the interviewees goes further by proposing "a cybersecurity lab to run workshops for staff and students not just for protection, but to build a digital responsibility culture". This broader vision of education explicitly aims to develop a culture of digital responsibility, thus establishing a direct link between education, security, and sustainability.

1.1.6. Data Sovereignty as a Component of Sustainability

A specific aspect emerging from the interviews concerns data sovereignty as a component of sustainability. one of the interviewees emphasizes the importance of "ensuring that data remains in Algeria", specifying that "storing sensitive information abroad is illegal". This concern for data localization and sovereignty is part of a vision of sustainability that integrates legal considerations and national governance.

1.1.7. Towards an Integrated Sustainability Strategy

The analysis of the interviews reveals a clear awareness of the need for a more integrated and formalized approach to sustainability. The auditor emphasizes that "continuous efforts are needed to develop comprehensive strategies that marry security and sustainability imperatives". This observation highlights the need for increased formalization of policies linking security and sustainability.

one of the interviewees also evokes the need for an integrated approach by mentioning discussions on "setting up a connected network for campus wide educational apps", while emphasizing the security imperative: "but it has to be secure". This perspective illustrates the vision of a campus wide digital ecosystem that integrates both educational objectives and security imperatives.

In conclusion, the analysis of the interviews reveals a rich and multidimensional vision of sustainability within ESHRA's Smart Green Campus project. This vision integrates technological, organizational, cultural, and educational considerations, and explicitly recognizes the synergies between information security and sustainability. The identified challenges primarily concern cultural resistance and the need for increased formalization of policies integrating security and sustainability. Ongoing initiatives, particularly in the field of energy efficiency and education for digital responsibility, demonstrate a pragmatic approach aimed at realizing this vision of sustainability.

1.2. Governance and information security

The analysis of the interviews reveals a structured information governance and security architecture but with certain organizational and operational limitations. This section explores the different dimensions of this governance a s they emerge from the collected testimonies.

Figure 11 word cloud of Governance and information security

Source: developed by us using Nvivo15

1.2.1. Stratified Architecture of the Information System

ESHRA's information system presents a clearly stratified architecture structured around three fundamental layers: the application layer, the infrastructure layer, and the organizational layer. As described by the IT engineer (DSI): "Our information system is structured across several layers. We have an application layer with tools like ARUBA Controller, Active Directory, and Kaspersky Controller. The infrastructure layer includes a local data centre with firewalls and backups on Google Cloud." This application layer includes business software used across technical and functional departments, such as ARUBA, Active Directory, Smart PSS for technical operations, and tools like PCompta and PCPaie for administrative management. The infrastructure layer comprises physical equipment and network architecture, including servers, firewalls, and backup systems. This technical architecture is complemented by a clear functional distribution of responsibilities within the IT department. As the same engineer explained: "The IT department manages the network, server administration, and security, including monitoring tools and antivirus systems." This organizational layer encompasses internal roles in system administration, infrastructure management, user support, and security operations. Together, these layers illustrate a coherent and technically sound approach to information systems governance, reflecting a classic model centred on the operational and technical management of digital systems.

1.2.2. Regulatory and Normative Framework

A significant element of information security governance at ESHRA lies in its anchoring in a solid regulatory and normative framework. The auditor emphasizes that "At ESHRA, governance of information security relies heavily on compliance with national laws such as the Personal Data Protection Law 18 07, and we align our audit practices with international standards like ISO 27001 and ISO 27005." This dual reference to national legislation and international standards demonstrates a willingness to inscribe governance practices within a recognized and structured framework.

The testimony also specifies that "The governance framework is reinforced by presidential decrees and internal audit cycles to ensure that all IT processes comply with these regulations." This mention of presidential decrees and internal audit cycles reveals the existence of formal mechanisms for control and verification of compliance, essential to effective governance.

1.2.3. Access Control and Data Protection

Access management and sensitive data protection appear as central concerns of security governance. one of the interviewees clearly states: "We ensure that access to our systems is strictly controlled and that sensitive data is protected. Internal traffic is also regulated, and only authorized personnel can access key applications and files." This restrictive approach to access management demonstrates an acute awareness of the issues of data confidentiality and integrity.

This concern for data protection falls within the broader framework of regulatory compliance mentioned previously, particularly regarding the personal data protection law (18 07).

1.2.4. Organizational Limitations and Governance Challenges

Despite these structuring elements, the analysis reveals certain significant organizational limitations. The auditor observes that "the IT department's structure shows a strong technical focus, with the IT Manager also functioning as the network engineer. This dual role may limit strategic oversight". This dual function of the IT manager illustrates a tendency to prioritize technical expertise potentially at the expense of strategic vision, which can constitute a brake on effective governance.

The testimony adds that "some staff tend to remain within their traditional scopes without extending towards integrated governance responsibilities". This observation highlights a compartmentalization of responsibilities that can hinder the emergence of an integrated approach to governance, necessary in the face of the increasing complexity of information security issues.

one of the interviewees confirms these organizational challenges by noting that "there's still confusion about how to coordinate between developers, users, and administrative bodies" and by emphasizing the need for "clear procedures to guide digital transformation". These observations reveal a need for clarification of roles and processes to effectively support digital transformation initiatives.

1.2.5. Human Dimension of Governance

A particularly significant aspect emerging from the interviews concerns the human dimension of governance. one of the interviewees observes with insight that "Managing an information system is one thing, but managing people and getting them on board with a project is much more complex." This reflection emphasizes that governance challenges are not only technical but fundamentally involve human and organizational issues.

This perspective is reinforced by one of the interviewees, who defines governance as ensuring that "everyone understands their role from decision makers to technical teams".

This conception of governance cantered on the clarity of roles and shared understanding of responsibilities highlights the importance of the human factor in the success of information security initiatives.

1.2.6. 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. one of the interviewees states that "Digitalization is the very foundation of the project. We can't talk about AI, dashboards, or informed decisions without reliable, structured data." This observation emphasizes that the quality and reliability of data constitute a fundamental prerequisite for the development of advanced applications and informed decision making.

This perspective highlights the importance of effective data governance as an essential component of the overall governance of information systems, particularly in the context of innovative initiatives like the Smart Green Campus.

1.2.7. Towards Integrated Governance

The analysis of the interviews reveals a clear awareness of the need to evolve towards a more integrated approach to governance. The identified organizational limitations, particularly the compartmentalization of responsibilities and confusion in coordination between different stakeholders, call for a redefinition of governance processes.

The vision expressed by one of the interviewees regarding the need for "clear procedures to guide digital transformation" suggests an orientation towards increased formalization of governance processes. This evolution appears essential to effectively support the ambitions of the Smart Green Campus project and ensure alignment between technological initiatives and the institution's strategic objectives.

In conclusion, the analysis of the interviews reveals information security governance at ESHRA characterized by a structured technical architecture and solid anchoring in a regulatory and normative framework. However, significant challenges persist, particularly in terms of organization, clarification of roles, and coordination between different stakeholders. The human dimension of governance and the importance of structured data emerge as essential aspects to consider in the evolution towards a more integrated approach to governance.

1.3. Information Security Risk Management

The analysis of the interviews reveals an approach to information security risk management that combines formal and informal elements, with significant challenges in the systematic

implementation of risk treatment processes. This section explores the different dimensions of this risk management as they emerge from the collected testimonies.

1.3.1. Risk Identification and Categorization

The interviews highlight a clear awareness of the different categories of risks the institution faces. The IT engineer (DSI) specifically identifies several types of risks: "We manage risks like unauthorized access to Wi Fi, consoles, cameras, and accounting systems." This enumeration reveals particular attention to risks related to unauthorized access, which constitute a major concern for information security.

The testimony also mentions other risk categories: "Misconfigurations and patching issues are serious concerns" as well as "risks like intrusions, poor update management, and potential espionage through connected systems." This diversity of identified risks demonstrates a relatively comprehensive approach to the identification of potential threats.

one of the interviewees complements this vision by mentioning a specific risk: "One of our biggest risks is infection through USB devices. We estimate the risk at around 5%". This risk quantification suggests an attempt at formal evaluation, although the underlying methodological approach is not explicated.

1.3.2. Methodological Framework for Risk Management

The auditor describes a structured methodological framework for risk management: "We follow a formal risk management process inspired by ISO 27005 that includes identification, evaluation, treatment, and continuous monitoring of security risks." This explicit reference to the ISO 27005 standard demonstrates a willingness to anchor risk management practices in a recognized and standardized framework.

The testimony also specifies that "Evaluating risk severity incorporates compliance with national and international regulations", thus highlighting the integration of regulatory requirements in the evaluation of risk severity. This approach reflects an awareness of the importance of regulatory compliance in risk prioritization.

1.3.3. Control and Mitigation Measures

The interviews reveal various control and mitigation measures implemented to manage identified risks. The IT engineer mentions the use of "access controls and frequent audits" as general measures, as well as more specific actions: "We work on encryption for HR and financial data and ensure traceability for all system actions." These measures particularly target the protection of sensitive data and the traceability of actions, two essential aspects of information security.

one of the interviewees also mentions protection measures: "our firewall and protocols help mitigate it (the risk of USB infection)" and "We tightly control access to shared files and regularly update protocols to handle new threats." These testimonies emphasize the importance given to access controls and regular updating of protocols to adapt to the evolution of threats.

1.3.4. Role of Audits in Risk Management

Audits appear as a central element of the risk management system. The auditor emphasizes that "Audits serve as critical corrective tools, enabling us to detect non conformities and recommend actionable measures." This vision of audits as corrective tools highlights their role in identifying non conformities and formulating actionable recommendation this perspective is consistent with the IT engineer's mention of "frequent audits" as a component of the risk management approach. The Occurrence of audits suggests a willingness to maintain continuous vigilance against emerging risks.

1.3.5. Implementation Challenges and Organizational Limitations

Despite the existence of a structured methodological framework, the interviews reveal significant challenges in the effective implementation of risk management processes. The auditor observes that "implementation faces challenges, notably insufficient engagement from some departments, implicit risky behaviours among users, and gaps in cybersecurity training." This observation highlights three major obstacles: lack of engagement from certain departments, risky user behaviours, and gaps in cybersecurity training.

The testimony adds that "risk treatment is not fully generalized across all units, creating vulnerabilities that need addressing." This non generalization of risk treatment across all units constitutes a significant vulnerability that compromises the overall effectiveness of the risk management approach.

one of the interviewees identifies a specific organizational limitation: "Poor implementation is a key threat. No dedicated cybersecurity team general IT handles it, which increases exposure." The absence of a dedicated cybersecurity team, with the delegation of this responsibility to the general IT team, is perceived as a factor increasing risk exposure.

1.3.6. Human and Cultural Dimension of Risks

A particularly significant aspect emerging from the interviews concerns the human and cultural dimension of risks. one of the interviewees observes that "More than 50% of digital transformation projects fail not due to lack of resources, but because of resistance to change" and adds the striking formula: "Culture eats strategy for breakfast." These reflections

emphasize that the most significant risks are not necessarily technical but cultural, related to resistance to change and human behaviours.

This perspective is consistent with the auditor's observation regarding "implicit risky behaviours' among users" as one of the implementation challenges. It highlights the importance of taking into account human and cultural factors in any effective risk management strategy.

1.3.7. Evolution of Risk Management Practices

The interviews suggest a progressive evolution of risk management practices, with a trend towards increased formalization and systematization. one of the interviewees mentions that "We... regularly update protocols to handle new threats", demonstrating an adaptive approach to the evolving threat landscape.

The auditor also mentions the need for continuous efforts to improve risk management practices, particularly regarding the generalization of risk treatment across all units. This recognition of current limitations and the need for continuous improvement suggests a positive evolutionary dynamic.

1.3.8. Integration of Risk Management into the Global Strategy

A final aspect worth highlighting concerns the integration of risk management into the institution's global strategy, particularly in the context of the Smart Green Campus project. Although this integration is not explicitly detailed in the interviews, it appears in filigree through mentions of synergies between security and sustainability.

Effective management of information security risks constitutes an essential prerequisite for the realization of the Smart Green Campus project's ambitions, as implicitly suggested by one of the interviewees 's statement: "Cybersecurity and sustainability go hand in hand; if it's not secure, it's not sustainable." This perspective emphasizes the strategic importance of risk management for the overall success of the project.

In conclusion, the analysis of the interviews reveals an approach to information security risk management at ESHRA that combines formal elements, with an explicit reference to the ISO 27005 standard, and more informal practices. Significant challenges persist, particularly in terms of department engagement, user behaviours', and generalization of risk treatment. The human and cultural dimension of risks emerges as an essential aspect to consider in the evolution towards a more integrated and effective approach to risk management.

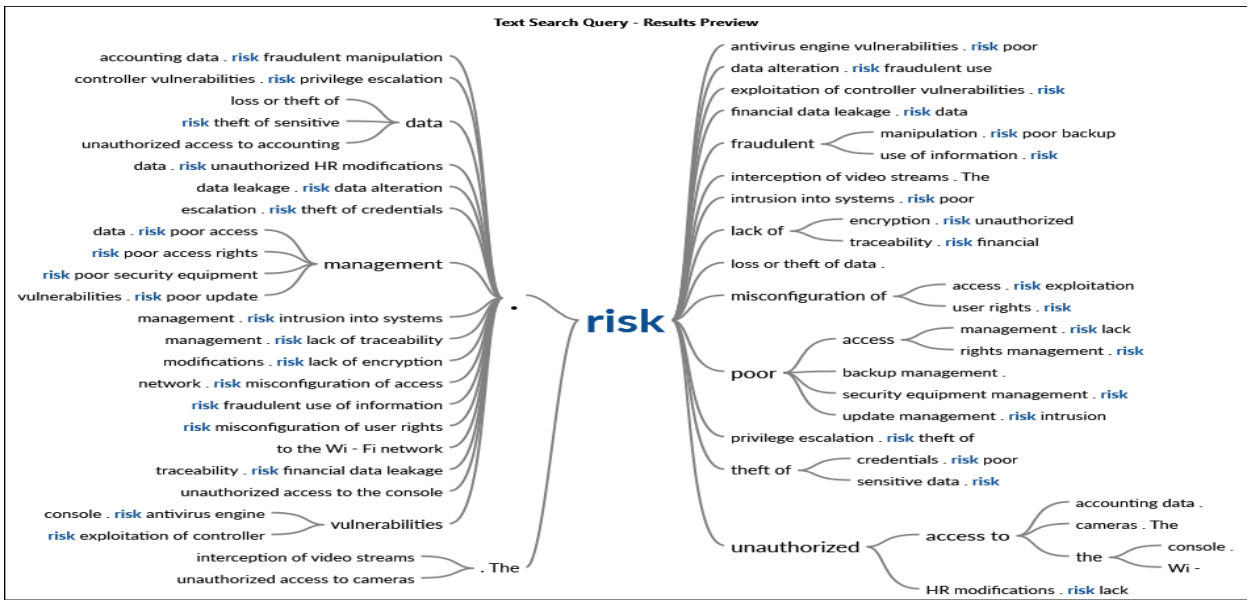
2. Applying FMECA for Risk management of information security:

The risk management of information security using the FMECA methodology was informed by various insights gathered through interviews. These revealed differing approaches across departments: while a general risk-aware culture is present, formal methods remain underdeveloped in some areas. Despite an openness to adopting structured frameworks, their practical application is still emerging. The analysis proceeded through several key phases, including the identification of existing risks, the development of a comprehensive mind map of information security vulnerabilities, and the use of NVivo 15 to structure and visualize these findings

2.1. Identification

The identification phase focused on uncovering existing information security risks across the institution, with particular attention given to the application layer. This phase was essential to lay the groundwork for a structured risk analysis and to highlight vulnerabilities already recognized by stakeholders. All risks related to the application layer were thoroughly analysed and addressed

Figure 12 Mind map of information security risks



Source: developed by us using Nvivo15

The mind map provides a comprehensive overview of all the existing possible risks related to information security, capturing the various threats and vulnerabilities identified throughout the analysis. Following this, the table below details these risks specifically

according to the different applications used at ESHRA, allowing for a clearer understanding of the risk landscape within the institution's digital environment.

Table 5 Identified Security Risks by Application and Function

Application	Function	Risks
Aruba Controller	Access point control	Unauthorized access to the Wi-Fi network
		Misconfiguration of access
		Exploitation of controller vulnerabilities
Active Directory	Session and user management	Privilege escalation
		Theft of credentials
		Poor management of access rights
Kaspersky Controller	Antivirus control	Unauthorized access to the console
		Vulnerabilities in the antivirus engine
		Poor update management
GTC	Centralized technical management	Intrusion into systems
		Poor security equipment management
Smart PSS	Camera surveillance	Unauthorized access to cameras
DLGC	Storage management	Loss or theft of data
		Poor management of access
		Lack of traceability
DLGC	Billing	Financial data leakage
		Data alteration
		Fraudulent use of information
PCPaie	Payroll management	Theft of sensitive data
		Unauthorized modification of HR data
		Absence of encryption
PCCompta	Accounting	Unauthorized access to accounting data
		Poor backup

Source: Developed by us

2.2. Risk Categorization Based on the CIA Security Principles

In this table, we classified the risks into five key categories which are 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 evaluated to determine its impact, with an 'X' indicating where it affects Confidentiality (C), Integrity (I), or Availability (A)

Table 6 Risk Categorization Based on the CIA Security Principles

Category	Risk	Confidentiality (C)	Integrity (I)	Availability (A)
Access and Rights Management	Unauthorized access to the Wi-Fi network	X		
	Misconfiguration of access	X	X	X
	Privilege escalation	X	X	
	Theft of credentials	X		
	Poor management of access rights	X	X	
	Poor configuration of user rights	X	X	
	Poor management of access	X	X	X
	Unauthorized access to the console	X		
	Unauthorized access to cameras	X		
	Unauthorized access to accounting data	X		
Technical and Configuration Risks	Exploitation of controller vulnerabilities	X	X	
	Vulnerabilities in the antivirus engine	X	X	
	Poor update management		X	X
	Intrusion into systems	X	X	X
	Poor security equipment management	X	X	X
	Absence of encryption	X		
	Poor backup			X
Sensitive Data Risks	Loss or theft of data	X	X	X
	Financial data leakage	X		
	Theft of sensitive data	X		
	Fraudulent use of information	X	X	

	Unauthorized modification of HR data		**X**	
	Data alteration		**X**	
	Lack of traceability	**X**	**X**	
Connected Systems & Physical Risks	**Espionage via connected systems**	**X**		
	Interception of video streams	**X**		
Human Risks	**Fraudulent manipulation**	**X**	**X**	

Source: developed by us according to interviews

2.3. Prioritization

After identifying the potential risks related to the security of information systems within the Smart Green Campus project, we proceeded to evaluate them. This evaluation was carried out by calculating the **criticality** of each risk using the formula: **C = S × O × D**, where *S* represents **Severity**, *O* **Occurrence**, and *D* **Detectability**. Each of these criteria was assed using a scale from **1 to 4**, in accordance with the methodology outlined in the first section of the previous chapter. This method allowed us to classify and prioritize the identified risks based on their level of criticality

Table 7 risk criticality interval according to (severity, occurrence, detectability)

Criticality Interval	Occurrence	Severity	Detection	Justification
1 to 8	1 to 2	1 to 2	1 to 2	The first interval (from 1 to 8) corresponds to a combination of criteria ranging from (1×1×1) to (2×2×2).
9 to 27	2 to 3	2 to 3	2 to 3	The second interval (from 9 to 27) covers the values from (2×2×2) to (3×3×3).
28 to 64	3 to 4	3 to 4	3 to 4	The third interval (from 28 to 64) represents the levels from (3×3×3) to (4×4×4).

Source: developed by us

The risk intervals were established based on the levels of each criterion: **Occurrence**, **Severity**, and **Detectability**. The first interval (from 1 to 8) corresponds to a combination of criteria ranging from (1×1×1) to (2×2×2). The second interval (from 9 to 27) covers values from (2×2×2) to (3×3×3). The third interval (from 28 to 64) represents the *levels* from

(3×3×3) to (4×4×4). This classification enables a clearer evaluation and prioritization of risks based on their criticality.

2.4. Risk Assessment

According to the analysis established using NVivo, we were able to assess and the identified risks based on their level of criticality.

Table 8 scale of prioritisation according to the criticality level

Assessed Risk Level	Risk Definition	Acceptability
1 to 8	Acceptable risk	Acceptable with implemented measures
9 to 27	Moderate risk	Not acceptable: mid-term risk management measures required
28 to 64	Intolerable risk	Not acceptable: urgent risk control measures obligatory

Developed by us

Based on this analysis, we were able to calculate the level of criticality for each failure mode, and we found the following results:

Table 9 Classification of the acceptability of the risks

Assessed Risk Level	Accepetability	Numbe
1S C8	Acceptable risk	8
9S C27	Moderate risk	15
28S C64	Intolerable risk	3

Source: developed by us

The table presents the assessment of identified risks according to their acceptability levels and corresponding frequency counts. Out of the total risks evaluated, 8 fall under the category of acceptable risk, indicating these risks are within tolerable limits and may require minimal monitoring or controls. The majority, 15 risks, are classified as moderate risk, suggesting a need for careful management and mitigation measures to prevent escalation. Finally, 3 risks are deemed intolerable, highlighting critical vulnerabilities that demand immediate attention and robust corrective actions to ensure the security and resilience of the system.

2.5. Treatment

During our study, we implemented preventive measures to reduce risks, particularly when their likelihood was high or their potential impact was significant. The objective was to minimize the chances of system dysfunctions and to mitigate undetected risks.

Corrective and preventive actions were defined based on the risk level of each identified vulnerability, with proposals emerging from all contributors interviewed. This participatory approach allowed us to leverage the insights of each stakeholder involved in the Smart Green Campus initiative.

The following tables presents the treatment of the highest criticality risks identified, while the remaining risk treatments are detailed in the FMECA analysis table

Table 10 Risk 1: Poor Update Management

Element	Details
Failure	Outdated antivirus definitions leave systems vulnerable to new threats, increasing the risk of malware and ransomware attacks.
Criticality	36
Recommendations	- Configure Kaspersky Security Centre for automatic updates - Monitor update status via console - Set up alerts for failed updates - Ensure update source accessibility - Define update management policy - Diagnose and fix failures, force update, scan affected machines
Responsibilities	- **IT Department**: Configure and monitor updates - **Department Head**: Ensure critical systems are updated - **Users**: Report issues or anomalies
Timeline	- **Immediate**: Configure updates and alerts - **30 Days**: Train staff - **60 Days**: Verify updates on all endpoints - **90 Days**: Conduct audit
Appendices	- Update audit report - Update management procedure - Security training program
Follow-up	Monthly monitoring by IT; quarterly audits to assess update process effectiveness

Source: developed by us

Table 11 Risk 2: Poor Security Equipment Management

Element	Details
Failure	Poorly configured or unmaintained security equipment (firewalls, sensors) increases exposure to attacks.
Criticality	36
Recommendations	- Enforce secure configuration policies - Schedule maintenance and firmware updates - Monitor equipment status and logs - Train personnel - Fix misconfigurations or failures
Responsibilities	- **IT Department**: Define and monitor configuration policies - **Department Head**: Oversee equipment maintenance - **Users**: Report anomalies
Timeline	- **Immediate**: Set policies - **30 Days**: Train staff, schedule maintenance - **60 Days**: Complete updates - **90 Days**: Audit configurations
Appendices	- Equipment audit report - Equipment maintenance procedure - Update log
Follow-up	Regular updates from IT; audits every 90 days

Source: developed by us

Table 12 Risk 3: Poor Backup Management

Element	Details
Failure	Inadequate or missing backups increase risk of data loss during incidents like ransomware or system failures.
Criticality	32
Recommendations	- Define clear backup policy - Automate backups - Use secure, separate (preferably offsite) storage - Test restoration regularly - Monitor jobs and set alerts - Encrypt backups - Analyse failures and improve strategy
Responsibilities	- **IT Department**: Implement and monitor backup policy - **Department Head**: Ensure restoration of critical data - **Users**: Participate in tests
Timeline	- **Immediate**: Define policy - **30 Days**: Automate and encrypt - **60 Days**: Test restoration - **90 Days**: Audit strategy
Appendices	- Backup audit report - Backup procedure - Restoration test log

Follow-up	Monthly monitoring by IT; quarterly audits to assess backup reliability

Source: developed by us

2.6. Monitoring and control

As part of our project on information security risk management within the Smart Green ESHRA initiative, we conducted a Failure Modes and Effects Analysis (FMCEA) to assess vulnerabilities across key digital systems. This analysis allowed us to identify twenty-six major failure modes. Each failure mode was evaluated based on its criticality to prioritize the associated risks. The results are presented in the FMECA table **APPENDIX III**, providing a structured and transparent view of the most significant threats and supporting the development of appropriate mitigation strategies.

Having approximated the criticality of each failure mode, we prepared action plans for each of them according to the person responsible for each plan. We prepared a total of 80 preventive/corrective action proposals. The fundamental purpose of this step was reducing the impact of criticality and preventing potential threats. These were set while constructing the matrix on May 05, 2025. After implementing the action plans, which contained both preventive and corrective actions for each failure mode, we re-assessed the criticality of each one of these modes. This reassessment was done after consultations with the project managers. We re-classified the failure modes according to their new criticality as follows:

Table 13 Risk classification after treatment

Assessed Risk Level	Accepetability	Number
1S C8	Acceptable risk	24
9S C27	Moderate risk	2
28S C64	Intolerable risk	0

Developed by us

Table 14 Comparative analysis of criticality

Accepetability	Number BEFORE	Number AFTER
Acceptable risk	8	24

Moderate risk	15	2
Intolerable risk	3	0

Developed by us

By evaluating the effectiveness of our action plans, we successfully reduced the number of Intolerable risks from **3 to 0** by taking immediate measures to bring them down to acceptable or moderate levels, as recommended. We also observed an increase in acceptable risks, rising from **8 to 24**, and a slight decrease in moderate risks from **15 to 2**. This progression is due to our enhanced ability to control and manage these risks through the preventive and corrective measures we implemented, such as automated patch management, role-based access controls, and robust backup solutions. These results demonstrate our commitment and effectiveness in reducing the criticality of risks related to our digital platforms. They also highlight the added value of our preventive and corrective actions, which have helped strengthen the security and reliability.

Second section: Discussion

The Smart Green Campus project at ESHRA represents a significant case study in the integration of information security risk management with sustainability objectives in higher education. This discussion examines the findings from the practical implementation at ESHRA, contextualizes them within the broader literature on information security governance and risk management, and evaluates the effectiveness of the FMECA methodology in addressing information security risks in sustainable digital transformation initiatives.

The practical results from ESHRA reveal a profound recognition of the synergies between information security management and sustainability objectives. As articulated by one stakeholder, "information security and sustainability go hand in hand; if it's not secure, it's not sustainable." This perspective aligns with emerging literature on the integration of security with sustainability, where researchers like Benzidia (2023) and Wahiba (2024) emphasize the increasing need to align information systems governance with sustainability objectives. The ESHRA case demonstrates how this theoretical alignment manifests in practice, with stakeholders actively working to develop applications focused on energy efficiency while simultaneously addressing security concerns.

The recognition of these synergies at ESHRA represents an evolution in thinking about both information security and sustainability. Traditionally, these domains have been treated as separate concerns, with security focused on protecting information assets and sustainability cantered on environmental impact. However, the ESHRA case illustrates how these domains are increasingly converging, with security recognized as a prerequisite for sustainable digital transformation. This convergence is particularly evident in the treatment plans developed for high-criticality risks, which address not only immediate security concerns but also long-term sustainability considerations.

For instance, the treatment plan for "Poor Update Management" includes not only technical measures like configuring automatic updates but also organizational elements like defining update management policies and training staff. This holistic approach reflects the literature's emphasis on information security as a multidimensional process requiring both technical and organizational alignment (Benyettou, 2018; Hamdi, 2019). The significant improvement in risk profile after implementing these treatment plans reducing intolerable risks from 3 to 0

and increasing acceptable risks from 8 to 24 demonstrates the effectiveness of this integrated approach.

Despite the recognized synergies, the ESHRA case also reveals significant governance challenges and organizational limitations that affect the implementation of information security risk management in the Smart Green Campus context. The practical results highlight issues such as dual roles that "may limit strategic oversight" and compartmentalization of responsibilities that can hinder an integrated approach to governance. These challenges echo findings in the literature, particularly Ladjouzi's (2022) study of IS governance within Algeria's public sector, which revealed informal and underdeveloped processes that expose gaps in aligning international best practices with local needs.

The organizational challenges at ESHRA reflect a broader tension in information security governance between technical expertise and strategic vision. As noted in the practical results, the IT manager at ESHRA also functions as the network engineer, potentially limiting strategic oversight. This dual role exemplifies what Floricel et al. (2015) describe as the limitations of traditional risk approaches in handling organizational complexity and diverse stakeholders. The literature suggests that effective information security governance requires elevating security concerns from purely technical considerations to strategic priorities (von Solms, 2016), a transition that appears to be in progress but not yet fully realized at ESHRA.

The human and cultural dimensions of governance emerge as particularly significant in the ESHRA case. As one stakeholder observed, "Managing an information system is one thing, but managing people and getting them on board with a project is much more complex." This insight aligns with Da Veiga's (2015) focus on organizational culture and employee behavior as pivotal factors in mitigating information security risks. The recognition at ESHRA that "the challenge isn't funding, it's cultural resistance to new, sustainable practices" highlights the importance of addressing cultural factors in successful information security risk management.

The application of FMECA methodology at ESHRA provides valuable insights into its effectiveness for information security risk management in the context of sustainable digital transformation. The FMECA data reveals a systematic approach to risk assessment and treatment, with risks evaluated based on Severity (S), Occurrence (O), and Detectability (D) criteria on a 1-4 scale. This approach aligns with the literature's description of FMECA as a structured method for identifying and prioritizing potential failure modes (Alaoui, 2022; Kaizen, 2025).

However, the implementation at ESHRA differs from some approaches suggested in the literature. While researchers like Silva (2014) and Gusmão (2016) advocate for integrating approximate reasoning techniques logic with FMECA to better handle the uncertainty inherent in information security risks, the ESHRA implementation uses a more traditional deterministic approach. This divergence raises questions about the adaptability of FMECA to the dynamic nature of information security risks in digital environments.

Despite this limitation, the practical results demonstrate the effectiveness of the FMECA methodology in identifying and addressing critical information security risks. The detailed treatment plans developed for high-criticality risks like "Poor Update Management" and "Poor Security Equipment Management" illustrate how FMECA can guide not only risk identification but also the development of comprehensive mitigation strategies. The significant improvement in risk profile after implementing these treatment plans provides empirical evidence of FMECA's value in information security risk management.

The ESHRA case also highlights the importance of adapting FMECA to the specific context of information security. As noted by Shevchenko (2021), FMECA was originally designed for physical systems, and its application to information security requires tailored adjustments. The categorization of risks at ESHRA based on the CIA security principles (Confidentiality, Integrity, Availability) represents one such adaptation, aligning the FMECA methodology with established information security frameworks.

The ESHRA case illustrates the strategic importance of integrating risk management into digital transformation initiatives, particularly those with sustainability objectives. The practical results show how information security risk management supports the broader goals of the Smart Green Campus project, with risk treatment plans addressing not only immediate security concerns but also long-term sustainability considerations. This strategic integration aligns with Knight's (2021) analysis of ISO 31000:2018, which promotes embedding risk management into decision-making processes.

The literature emphasizes the evolution of risk management from a traditionally reactive process into a critical strategic discipline supporting organizational resilience and value creation (Aven, 2016; Renn, 2020). The ESHRA case provides a practical example of this evolution, with risk management serving not as an isolated function but as an integral component of the Smart Green Campus initiative. The detailed treatment plans in the FMECA data demonstrate how risk management can create value by not only mitigating threats but also enhancing operational efficiency and supporting sustainability objectives.

However, the practical implementation at ESHRA also reveals gaps in the strategic integration of risk management. While the literature suggests a unified theoretical framework for risk management (Aven, 2016; Renn, 2020), the ESHRA implementation shows a more pragmatic, context-specific approach. This divergence reflects the challenges of applying theoretical frameworks in real-world settings, particularly in contexts with specific organizational and cultural characteristics.

The FMECA data also reveals a focus primarily on technical and operational risks, with less attention to strategic risks that are emphasized in the literature's discussion of Enterprise Risk Management (Lam, 2018). This gap suggests opportunities for further development of the risk management approach at ESHRA, potentially incorporating a broader range of risk categories and a more explicit alignment with strategic objectives.

The ESHRA case offers several implications for both practice and theory in the domain of information security risk management for sustainable digital transformation. For practitioners, the case demonstrates the value of a structured risk management approach like FMECA in identifying and addressing information security risks. The significant improvement in risk profile after implementing treatment plans provides empirical evidence of the effectiveness of this approach. The case also highlights the importance of addressing organizational and cultural factors alongside technical considerations, suggesting that practitioners should adopt a holistic approach to information security risk management.

For theory, the ESHRA case provides empirical support for the integration of information security with sustainability objectives, contributing to the emerging literature on this topic. The case also raises questions about the adaptability of risk management frameworks like FMECA to the dynamic nature of information security risks, suggesting avenues for further research on hybrid approaches that combine structured methodologies with more flexible, context-sensitive elements.

The gap between the theoretical emphasis on approximate reasoning techniques logic and the practical implementation of a more deterministic approach at ESHRA highlights the need for further research on bridging theory and practice in information security risk management. Similarly, the focus on technical and operational risks in the FMECA data suggests opportunities for expanding risk management frameworks to more explicitly address strategic risks in the context of sustainable digital transformation.

The Smart Green Campus project at ESHRA provides a valuable case study in the integration of information security risk management with sustainability objectives in higher education. The practical results demonstrate the effectiveness of a structured risk management approach

like FMECA in identifying and addressing information security risks, while also revealing challenges in governance and organizational alignment. The case illustrates both the synergies between information security and sustainability and the complexities of implementing theoretical frameworks in real-world settings.

The significant improvement in risk profile after implementing treatment plans reducing intolerable risks from 3 to 0 and increasing acceptable risks from 8 to 24 provides empirical evidence of the value of information security risk management in supporting sustainable digital transformation. However, the case also reveals gaps between theory and practice, particularly in the adaptation of risk management frameworks to the dynamic nature of information security risks and the integration of risk management with strategic objectives.

As organizations increasingly pursue digital transformation initiatives with sustainability objectives, the lessons from the ESHRA case offer valuable guidance for both practitioners and researchers. The case highlights the importance of a holistic approach to information security risk management, one that addresses technical, organizational, and cultural factors while aligning with broader strategic objectives. It also underscores the need for continued research on adapting risk management frameworks to the specific challenges of information security in sustainable digital transformation.

These insights have significant implications for both theory and practice. From a theoretical perspective, they contribute to the evolving understanding of IS governance by highlighting the importance of integrating sustainability considerations into established frameworks and by emphasizing the role of information security risk management as a strategic enabler for sustainability-driven initiatives. From a practical perspective, they offer valuable guidance for organizations embarking on similar initiatives, emphasizing the importance of a holistic approach to IS governance that addresses not only technical and operational concerns but also strategic alignment, cultural factors, and ethical considerations. By adopting such an approach, organizations can enhance their capacity to leverage information security risk management as a strategic tool for achieving sustainability objectives while also ensuring the integrity, confidentiality, and availability of their information assets.

In summary, this chapter demonstrates that in sustainability-driven digital projects like ESHRA's Smart Green Campus, IT governance and information security risk management are not optional they are essential enablers of success. Drawing from theoretical frameworks, key literature, and FMECA based analysis, the study highlights the need for a structured, proactive, and governance led approach to managing digital risks.

The transition toward a smart and sustainable campus depends on building a secure and resilient digital infrastructure, supported by clear governance and aligned with institutional sustainability goals. Addressing the identified technical, organizational, cultural, and governance challenges is crucial for turning digital ambitions into long-term strategic outcomes.

Ultimately, integrating risk management into IT governance is not just best practice it is a strategic necessity. This study outlines a path forward through risk assessment, stakeholder engagement, awareness initiatives, and robust governance, ensuring that digital transformation contributes meaningfully to sustainability.

General conclusion

In the rapidly evolving landscape of digital transformation, this dissertation has explored the critical intersection between information security risk management, IT governance, and sustainability objectives through the case study of the Smart Green Campus project at the Algiers Higher School of Hospitality and Restaurant Management (ESHRA). As organizations increasingly embed sustainability into their strategic vision, the governance of information systems assumes a pivotal role in orchestrating these diverse yet interdependent priorities, ensuring that security risks are identified and mitigated proactively while fostering innovation that supports sustainable practices.

Despite the growing interest in digital sustainability, little is known about how organizations can effectively integrate information security risk management within IS governance frameworks to support sustainability-oriented transformation. This gap is particularly visible in the context of emerging economies such as Algeria, where digital innovation is often challenged by limited resources, resistance to change, and the lack of structured governance practices. This dissertation addresses this critical gap by investigating how information security risk management can be structured to support both technical security and broader environmental and organizational sustainability goals

The research has demonstrated that effective information security risk management serves as a foundational pillar for achieving sustainable institutional objectives, particularly in initiatives that leverage advanced digital technologies to create intelligent, eco-efficient environments. To investigate these complex and interrelated dynamics, the study employed a qualitative action research methodology, allowing for an in-depth exploration of stakeholder experiences and institutional practices in real-time. This approach combined data collection through semi-structured interviews, direct observation, and internal documentation, which was subsequently analysed using NVivo 15. The action-oriented nature of the methodology enabled both diagnostic insight and practical intervention. The findings revealed a multidimensional vision of sustainability at ESHRA, encompassing technological, cultural, organizational, and educational dimensions. This holistic perspective emphasizes that sustainable digital transformation is not limited to technological upgrades but requires robust governance structures, effective risk management frameworks, and a culture that supports long-term resilience and innovation.

Following targeted interventions, including automated patching, role-based access control, and robust backup solutions, the post-intervention results demonstrated a remarkable improvement in the institution's security posture. The complete elimination of critical risks and substantial reduction in moderate risks underscores the effectiveness of a structured approach to information security risk management in sustainability-oriented digital projects. This transformation not only enhanced the technical resilience of ESHRA's information systems but also strengthened the alignment between security measures and the institution's broader sustainability objectives.

The research contributes significantly to both theoretical understanding and practical application in several ways. First, it addresses a notable gap in the literature concerning the integration of information security risk management into sustainability-focused digital initiatives, particularly in the Algerian context. By exploring this underexplored intersection, the study provides valuable insights into how organizations can align their information security practices with environmental and social responsibility goals.

Second, the research demonstrates the effectiveness of the FMECA methodology in sustainability-oriented information systems, offering a structured framework for identifying, evaluating, and mitigating security risks in complex digital environments. This adaptation of an engineering-based risk model to the domain of information security provides organizations with a practical tool for enhancing the resilience of their digital infrastructure while supporting their sustainability objectives.

Third, the study deepens our understanding of how information security risk management serves as a critical enabler for sustainable digital transformation. By highlighting the interconnections between security, governance, and sustainability, the research emphasizes that robust information security practices are not merely technical considerations but strategic imperatives that directly impact an organization's ability to achieve its sustainability goals.

The findings also reveal important insights into the human and cultural dimensions of information security risk management. It has been highlighted that the most significant risks are often related to resistance to change and human behaviours rather than purely technical vulnerabilities. This observation underscores the importance of fostering a security-conscious organizational culture and addressing the human factors that can either enable or impede effective risk management.

Furthermore, the research highlights the strategic importance of integrating information security risk management into an organization's global strategy, particularly in the context of sustainability initiatives

Finally, this dissertation has demonstrated that information security risk management, when effectively integrated into IT governance frameworks, can significantly enhance an organization's ability to achieve its sustainability objectives. By providing a structured approach to identifying, evaluating, and mitigating security risks, it enables organizations to build resilient, secure, and sustainable digital infrastructures that support their environmental and social responsibility goals. As digital transformation continues to reshape organizational landscapes, this integrated approach to security, governance, and sustainability will become increasingly critical for organizations seeking to navigate the complex challenges of the digital era while contributing to a more sustainable future.

This study provides valuable insights into integrating information security risk management within IS governance frameworks for sustainability-driven digital initiatives; however, it has several limitations.

First, the research focuses on a single case study ESHRA’s Smart Green Campus project which limits the generalizability of the findings. The results may not be fully applicable to other organizations, sectors, or geographical contexts.

Second, the study primarily uses a qualitative approach. While this provides rich insights into stakeholders’ perceptions and experiences, it may not capture the full complexity of the relationships between IS governance, risk management, and sustainability.

Third, the FMECA conducted for ESHRA offered useful information but did not utilize standard Risk Priority Number (RPN) calculations. Instead, it relied on a criticality score, which may reduce the precision in prioritizing and comparing risks.

Looking forward, several avenues for future research and practical application emerge from this study.

Future research could adopt a comparative approach, examining how different organizations across various sectors and geographic regions integrate information security risk management into there IS governance frameworks for sustainability-driven initiatives.

Mixed-methods approaches could also be employed to provide a more comprehensive understanding of the complex interactions between IS governance, risk management, and sustainability.

Subsequent studies could improve upon the FMECA method by adopting standardized RPN calculations, enabling more nuanced risk prioritization and comparison.

Moreover, further research could investigate the long-term impact of integrated security and sustainability approaches on organizational performance, resilience, and environmental outcomes.

Finally, comparative studies across different sectors and cultural contexts would offer valuable insights into the adaptability and transferability of governance frameworks and risk management methodologies developed in this research.

Bibliography

Bibliography

Abdelmalek Sadok , al. (2020). *Gouvernance des systèmes d'information : principes, enjeux et pratiques* .

Alaoui, M. E. (2022). Intégration de l'FMECA dans la gestion des risques : une approche théorique et sectorielle. . *Revue Marocaine de Recherche en Management et Marketing,* , 26, 50–65.

Al-Dhahri, S., Al-Sarti, M., & Abdaziz, A. (2022). An Overview of the IT Risk Management Methodologies for Securing Information Assets. *International Journal of Engineering Trends and Technology*, 221-225.

Almeida, F. &. (2023). Information security and sustainability: Towards a green digital transformation. . *Journal of Cleaner Production*, 405, 137012.

Anthony Anyanwu1, T. O. (2024). DATA CONFIDENTIALITY AND INTEGRITY: A REVIEW OF ACCOUNTING AND CYBERSECURITY CONTROLS IN SUPERANNUATION ORGANIZATIONS. *Computer Science & IT Research Journal, Volume 5, Issue 1*, 237-253.

Asma, F. (2019). *The Level of Information Security in Algerian Institutions and Its Impact by the Nature of Threats and Applied Protection Measures.* algeria telemcen.

Aven, T. (2016). Risk management and risk assessment: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.

Baggia, A. B. (2025, 01 15). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. (A. M. Alsobeh, Ed.) *Multidisciplinary Digital Publishing Institute*, 13-52. doi:https://doi.org/10.3390/systems13010052

Baskerville, R., Davison, R., Kaul, M., Malaurent, J., & Wong, S. (2022). The nexus of information systems and sustainability: Past, present, and future. *Journal of the Association for Information Systems*, 23(1), 2–20.

Benali, Y. Z. (2023). oward a smart and sustainable campus in Algeria: Framework and challenges. . *International Journal of Smart and Sustainable System*, 7(1), 45–58.

Benhaddouch, M., & El Fathaoui, H. (2022). Paradigmes épistémologiques et choix méthodologiques en science de gestion . *Revue de littérature. Revue Française d'Économie et de Gestion, 3(5).*

Benyettou, S. &. (2018). Empirical study on the integrated management system in Algerian companies. *Journal of Industrial Engineering and Management 11(1),*, 135–160.

Benzidia, S. M. (2023). Digital Transformation and Sustainability: The Role of IT Governance in Achieving ESG Goals. *International Journal of Information Management Volume 71*, 1015–1034.

Bounabat, Z. K. (2022). IT Management and Governance Framework for Formulating a Digital Transformation Strategy. In *Advanced Intelligent Systems for Sustainable Development (AI2SD'2020), Volume 2* (pp. 475-498). Springer. doi:10.1007/978-3-030-90639-9_39

Brunner, M. S. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. . *Computers & Security*, 93, 101751.

Bulsuk, K. (2009, 02 02). *Taking the First Step with the PDCA (Plan-Do-Check-Act) Cycle*. Retrieved from https://www.bulsuk.com/: https://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html

Campbell, T. (2016). *Practical Information Security Management A Complete Guide to Planning and Implementation.* Australia : Apress.

Checkland, P. &. (1998). Action research: Its nature and validity. . *Systemic Practice and Action Research,*, 11(1), 9–21.

Choo, K.-K. R.-K. (2017). Information security risk management for medical devices and systems. . *Health Information Science and Systems,*, 5(1), 1–8.

CMMI PRODUCT TEAM. (2002). *Capability Maturity Model Integration (CMMI), Version 1.1: CMMI for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing.* USA: Carnegie Mellon University, Software Engineering Institute.

Coghlan, D. &. (2014). *Doing Action Research in Your Own Organization (4th ed.).* . Sage Publications.

Da Veiga, A. &. (2015). mproving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162–176.

Death, D. (2023). *A comprehensive handbook on ISO/IEC 27001:2022 compliance.* Grosvenor House 11 St Paul's SquareBirminghamB3 1RB, UK: Packt Publishing.

Domínguez-Domínguez, R. F.-L.-L. (2023). Evaluation of an information security management system at a Mexican higher education institution. *arXiv preprint arXiv:2306.11050.*

Faucher, J. (2006). *Pratique de l'AMDEC: Assurez la qualité et la sûreté de fonctionnement de vos produits et équipements (2e éd.).* . Dunod.

Flores, D. A. (2023). A GDPR-compliant Risk Management Approach based on Threat Modelling and ISO 27005. *arXiv*.

Floricel, S. T., & Miller, R. . (2015). Risk management: History, definition, and critique. *RISK MANAGEMENT*, 17(3), 57–81.

Gibson, D., & Igonor, A. (2020). *Managing risk in information systems (3rd ed.).* Jones & Bartlett Learning.

GRALL, M. (2018). *EBIOS : la boîte à outils pour gérer les risques.* 72 avenue Gaston Boissier, 78220 VIROFLAY : Club EBIOS.

Günther, W. A. (2020). Digitalization and sustainability in information systems research: A review and research agenda. . *Business & Information Systems Engineering, 62(6),* , 543–559.

Gusmão, A. P. (2016). nformation security risk analysis model using fuzzy decision theory. . *International Journal of Information Management, 36(1)*, 25–34.

Hamdi, Z. N. (2019). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. *Journal of Physics: Conference Series, 1339*.

Hansen, D. R. (2021). Real-time cyber risk management in critical infrastructures. . *information & Management, 58(1), 103379*, 58(1), 103379.

Haseeb, J. M. (2021). Failure Modes and Effects Analysis (FMEA) of Honeypot-Based Cybersecurity Experiment for IoT. *In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN)*, 1–8.

Ibrahim, R. &. (2019). Key success factors for ISMS implementation in the Malaysian public sector. *Journal of Information and Communication Technology*, 18, 123–137.

ISACA. (2023). *Capability Maturity Model Integration (CMMI) Version 3.0. ISACA.*

ISACA. (2009). *COBIT 4.1: Control Objectives for Information and Related Technologies.* . ISACA.

ISO. (31000:2018). *ISO 31000:2018 — Risk management: Guidelines. ISO.*

ISO27001. (2022). *International Organization for Standardization (ISO). (2022). Systèmes de management de la sécurité de l'information — Exigences (ISO/CEI 27001:2022).* ISO.

ITGI, L. T. (2006).

Kaizen. (2025). *Using FMECA to enhance operational resilience: A step-by-step guide.* Kaizen Institute.

Kefalas, S. (2023, 07 03). *Solving standards implementation issues with a global ISMS. ISACA Journal, 4. Retrieved*. Retrieved from https://www.isaca.org/: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-4/solving-standards-implementation-issues-with-a-global-isms

Kemmis, S. &. (2000). *Participatory action research. In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of Qualitative Research (2nd ed., Sage Publications.* Sage Publications.

Kempf, K. W. (2000). *Analyzing documents for qualitative research.* Newbury Park, CA: Sage Publications.

Khafidh Sunny Al Fajri, R. H. (2024). Information Security Management System Assessment Model by Integrating ISO 27002 and 27004. *ndonesian Journal ofMachine Learningand Computer Science*, 498-506.

Khan, W. L. (2025). Is Cybersecurity a Social Responsibility? *Information Systems Frontiers.*

Knight, F. H. (2021). SO 31000:2018 Setting a new standard for risk management. *Risk Analysis,*, 41(9), 1339–1346.

Kroenke & Auer, J. (2015). *Database Concepts (7th edition.* Pearson.

Ladjouzi, S. (2022). La gouvernance des systèmes d'information dans l'administration algérienne : Cas du Ministère de l'Éducation Nationale. *Revue des Sciences de Gestion,*, 40(2), 81–94.

Lam, J. (2018). Enterprise risk management: A review of the literature . *International Journal of Management Reviews,* , 20(4), 730–752.

LASSON, A. D.-H. (2023). *sécurité informatique – Ethical Hacking : Apprendre l'attaque pour mieux se défendre.* ENI Editions.

Lozano, R. (2013). Sustainability inter-linkages in sustainability reporting: an analysis of the GRI reports of 2010. *Journal of Cleaner Production, 35,* , 123–138.

Mayer, N. A. (2017). An integrated conceptual model for information system security risk management and enterprise architecture management based on TOGAF, ArchiMate, IAF, and DoDAF. *Software & Systems Modeling,* , 18(3), 2285–2312.

MEKIMAH Sabri, Z. A. (2022). The evaluation of the information security management system (ISMS) In accordance. *Revue des Sciences Humaines & Sociales*, 853-870.

Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS Quarterly,* , 34(1), 1–21.

Müller, S. D. (2022). Sustainable IT governance: Aligning digital strategies with the UN SDGs. *Journal of Business Ethics, 180(3)*, 1015–1034.

Nassou, Y., & Bennani, Z. (2024). Cadrage épistémologique d'un travail de recherche en science de gestion: Revue de littérature et technique de positionnement.Cadrage épistémologique d'un travail de recherche en science de gestion: Revue de littérature et technique de positionnement. *Alternatives Managériales Economiques, 6(2).*

Nurdin, I. E. (2024). Development of an integrated IT risk management framework for electronic-based government systems. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, 1331-1353.

Odumesi, B. &. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Advanced Research and Reviews*, 19(03), 344–360.

Parsons, M. (2023, 12 08). *C-RISK*. Retrieved from www.c-risk.com/: https://www.c-risk.com/fr/blog/fondamentaux-securite-information

Pereira, R., Santos, H., Rosado, T., & Bernardino, J. (2020). Aligning cybersecurity and sustainability in smart cities: A risk management perspective. *Sustainability, 12(21), Article 9018.*

Philip A. Williams and Bianca Lebek. (2022). Sustainable cybersecurity: Balancing energy efficiency and data protection. *Computers & Security, 121, Article 102844.*

Pinet, C. (2023). *10 clés pour la securité de l'information.* FRANCE : AFNOR edition.

Reason, P. (2008). *The SAGE Handbook of Action Research: Participative Inquiry and Practice (2nd ed.).* Sage Publications.

Renn, O. (2020). Foundational issues in risk assessment and risk management. *Risk Analysis*, 40(11), 2245–2257.

Ross, P. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* . Harvard Business Review Press.

Salia, L. (2023). Toward a better adoption of information systems security standards in Burkina Faso. *Revue Internationale du Chercheur «Volume 4 : Numéro 3»* , 820 – 844.

Shevchenko, H. S. (2021). Information Security Risk Analysis SWOT. *Cybersecurity Providing in Information and Telecommunication Systems*, 309–317.

Silva, M. M. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. . *Computers in Industry,*, 65(2), 211–220.

Siti Suhaida Marhad, S. Z. (2023). Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*, 197-203.

Sondes Ksibi, F. J. (2022). *A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach.* tunisia: Mobile Networks and Applications .

Stenhouse, L. (1975). *An introduction to curriculum research and development.* LONDON: London: Heinemann Educational Books.

Thietart, R. A. (2017). *Méthodes de recherche en management (5e éd.).* . Paris: : Dunod.

von Solms, B. &. (2016). Cybersecurity governance: A component of corporate governance. *Information & Computer Security,* , 24(5), 580–594.

Wahiba, Y. R. (2024). Cybersecurity Challenges And International Cooperation “balancing Personal Data Protection And Information Sharing”. *Journal of law and humanities Sciences*, 31-48.

Walsham, G. (1995). Interpretive case studies in IS research: Nature and method. *European Journal of Information Systems,* , 4(2), 74–81.

Weill, P. &. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press.* Harvard Business School Press: HARVARD.

Williams, R., & Lebek, B. (2022). Enhancing IS governance frameworks to manage data security in digital enterprises. . *Information Systems Frontiers,*, 24(4), 789–803.

Yuwen Zhu, L. Y. (2023). Key Node Identification Based on Vulnerability Life Cycle and the Importance of Network Topology. *International Journal of Digital Crime and Forensics*.

Appendix

Appendix I – Interview Guide

Interview Guide

Risk management for information security within IT governance in a sustainability development project

This semi-structured interview guide is designed to explore the perceptions and practices related to information security risk management in the context of a sustainability-oriented digital initiative the Smart Green Campus project at ESHRA. The questions aim to gather qualitative insights from key stakeholders involved in governance, IT management, auditing, and everyday use of information systems. The guide is structured around three main analytical axes:

Vision of sustainability in the Smart Green Campus initiative

Governance and information security practices

Information security risk identification, assessment, and treatment

Axis	Question
Representative Questions:	Can you briefly introduce yourself? (Name, position, years in the organization, professional background) What is your current role at ESHRA? What are your main tasks or responsibilities on a daily basis? How do you interact with information systems in your work? (Daily use, responsibilities related to security, etc.)
1. Vision of Sustainability in the Smart Green Campus Context	How do you define sustainability in the context of the Smart Green Campus?
	What motivated ESHRA to launch a sustainability-focused digital initiative?
	What role do digital technologies play in achieving your sustainability goals?
	How are stakeholders (staff, students, administrators) engaged in this vision?
	What challenges have you encountered in integrating sustainability into digital strategies?
2. Governance and Information Security	How is the governance of information systems structured at ESHRA?
	Who is responsible for ensuring the security and integrity of information systems?
	Are there specific governance mechanisms (committees, policies, roles) overseeing digital initiatives like Smart Green Campus?
	How do you ensure compliance with legal and regulatory requirements for information security?
	How are sustainability principles reflected in information governance policies?

3. Information Security Risk Management	How are information security risks identified and assessed within the organization?
	What are the most common or critical risks currently facing your systems?
	Do you use any specific tools or frameworks (FMECA, ISO 27005) to manage risks?
	How are risks classified and prioritized for treatment?
	What kind of actions are taken to mitigate these risks technical, organizational, or both?
	How do you ensure that risk management aligns with sustainability objectives?
	Have you faced any trade-offs between implementing security controls and maintaining energy efficiency or digital accessibility?
	What recommendations would you give to better integrate risk management and sustainability in digital transformation projects?

Appendix II – Verbatim matrix

Interviewee	IT Governance and Information Security	Risk Management in Information Security	Information Security and Sustainability (Smart Green Campus)
01	"Our information system is structured across several layers. We have an application layer with tools like ARUBA Controller, Active Directory, and Kaspersky Controller. The infrastructure layer includes a local data centre with firewalls and backups on Google Cloud." "The IT department manages the network, server administration, and security, including monitoring tools and antivirus systems."	"We manage risks like unauthorized access to Wi-Fi, consoles, cameras, and accounting systems. We use access controls and frequent audits." "Misconfigurations and patching issues are serious concerns. We work on encryption for HR and financial data and ensure traceability for all system actions." "We're also tackling risks like intrusions, poor update management, and potential espionage through connected systems."	"The Smart Green Campus is a chance to align IT with sustainability. We're looking at energy-efficient systems and eco-friendly storage solutions." "Right now, our focus is security like surveillance and data protection but we want to transition toward sustainable technologies."
02	"We ensure that access to our systems is strictly controlled and that sensitive data is protected. Internal traffic is also regulated, and only authorized personnel can access key applications and files."	"One of our biggest risks is infection through USB devices. We estimate the risk at around 5%, but our firewall and protocols help mitigate it." "We tightly control access to shared files and regularly update protocols to handle new threats."	"Sustainability is central to Smart Green Campus. The challenge isn't funding it's cultural resistance to new, sustainable practices." "We're improving energy efficiency in our data centre and adopting greener hardware while maintaining security." "Workshops are held to raise awareness among staff about password management, data sharing, and cybersecurity."
03	"Managing an information system is one thing, but managing people and getting them on board with a project is much more complex." "Digitalization is the very foundation of the project. We can't talk about AI, dashboards, or informed decisions without reliable, structured data."	"More than 50% of digital transformation projects fail not due to lack of resources, but because of resistance to change." "Culture eats strategy for breakfast."	"Real sustainability means forming competent leaders, able to adapt and innovate in an uncertain world." "We must ensure that data remains in Algeria. Storing sensitive information abroad is illegal." "We're developing tools like an open-source project management platform and a centralized information portal."
04	"At ESHRA, governance of information security relies heavily on compliance with national laws such as the Personal Data Protection Law 18-07, and we align our audit practices with international standards like ISO 27001 and ISO 27005. The	"We follow a formal risk management process inspired by ISO 27005 that includes identification, evaluation, treatment, and continuous monitoring of security risks. Evaluating risk severity incorporates compliance with national and international	"In our audit processes, we increasingly integrate sustainability considerations such as energy efficiency and eco-design, although these remain in early stages. We recognize clear synergies between robust information security management and

	governance framework is reinforced by presidential decrees and internal audit cycles to ensure that all IT processes comply with these regulations." "However, the IT department's structure shows a strong technical focus, with the IT Manager also functioning as the network engineer. This dual role may limit strategic oversight, and some staff tend to remain within their traditional scopes without extending towards integrated governance responsibilities."	regulations. Yet, implementation faces challenges, notably insufficient engagement from some departments, implicit risky behaviours among users, and gaps in cybersecurity training." "Audits serve as critical corrective tools, enabling us to detect non-conformities and recommend actionable measures. Despite this, risk treatment is not fully generalized across all units, creating vulnerabilities that need addressing."	achieving sustainability goals, especially within the Smart Green Campus initiative." "Challenges persist in embedding sustainability fully within the security governance framework, including cultural resistance and limited formal policies linking these domains. Continuous efforts are needed to develop comprehensive strategies that marry security and sustainability imperatives."
05	"Governance means making sure everyone understands their role from decision-makers to technical teams." "There's still confusion about how to coordinate between developers, users, and administrative bodies. We need clear procedures to guide digital transformation."	"Poor implementation is a key threat. No dedicated cybersecurity team general IT handles it, which increases exposure."	"As the AI lead for the Smart Green ESHRA project, I'm very optimistic about the implementation of emerging technologies to drive sustainability and innovation." "My team developed an application focused on energy efficiency to monitor and optimize consumption across campus buildings." "Cybersecurity and sustainability go hand-in-hand; if it's not secure, it's not sustainable." "I proposed a cybersecurity lab to run workshops for staff and students not just for protection, but to build a digital responsibility culture." "We discussed setting up a connected network for campus-wide educational apps, but it has to be secure."

Appendix III – FMECA

Application	Function	Risk	Explanation	Failure Mode	Effect	S	O	D	criticality	responsable	Action plan	D	O	D	criticality
Kaspersky Controller	Antivirus control	Poor update management	Outdated antivirus definitions leave systems vulnerable to newly discovered threats.	Loss of electrical power or major disaster	System downtime, loss of critical data and services	4	3	3	36	IT Security Team	Configure Kaspersky Security Centre to automatically download and distribute virus definition and software module updates. - Monitor the update status on all endpoints via the administration console. - Set up alerts for endpoints that are not receiving updates correctly. - Ensure update sources (Kaspersky servers or internal distribution servers) are accessible by all clients. - Define and communicate a clear update management policy. Corrective - Identify the cause of update failures (network issue, configuration, disk space, etc.) and correct it. - Manually force updates on affected endpoints. - Verify that endpoints have received the latest definitions after fixing the problem. - Perform an antivirus scan on machines that were outdated to ensure they were not compromised.	4	2	2	16
GTC	Centralized technical management	Poor security equipment management	Security devices like firewalls and sensors may be improperly configured or maintained, increasing attack exposure.	Use of outdated systems and technologies	Incompatibility with new systems, higher maintenance costs	4	3	3	36	IT Operations	- Define and apply standard and secure configuration policies for all equipment. - Schedule and perform regular maintenance and firmware updates for security equipment. - Monitor the operational status and logs of security equipment. - Train responsible personnel in the secure management and maintenance of this equipment. Corrective	4	2	2	16

											- Immediately correct identified misconfigurations. - Replace or repair faulty equipment. - Analyse the impact of poor management (undetected security breach) and take appropriate measures. - Review and improve security equipment management procedures				
PCCompta	Accounting	Poor backup management	Inadequate or missing backups increase the risk of data loss in case of incidents like ransomware or system failures.	Backup data not properly maintained or updated	Data loss, difficulty in restoring services	4	2	4	32	Finance Department	Define a clear backup policy for PCCompta (frequency, retention, backup type). - Automate backups as much as possible. - Store backups on a separate and secure medium (ideally offsite for one copy). - Regularly test backup restoration to ensure their viability. - Monitor backup job success and set up alerts for failures. - Encrypt backups. Corrective - In case of an incident requiring restoration, use the last valid backup. - Analyse the cause of backup failure if that's the issue. - Immediately implement or improve the backup strategy if it is deemed insufficient. - Assess data loss if the last backup is not recent enough	4	1	2	8
Active Directory	User and session management	Privilege escalation	Improperly configured user roles may allow attackers to gain higher access rights than permitted.	Unauthorized individuals access financial data	Financial data theft and potential financial losses	4	2	3	24	System Administration	Apply the principle of least privilege for all user and service accounts. - Regularly audit user rights and permissions, especially for privileged accounts. - Implement strict separation of administrative roles. - Actively monitor for privilege escalation attempts (via Windows security logs, SIEM). - Promptly apply Windows Server security	4	1	2	8

											patches, especially those related to privilege escalation. - Use dedicated administrative accounts separate from standard user accounts. CORRECTIVE. - Identify the compromised account and immediately revoke its privileges. - Analyse the privilege escalation method used and patch the underlying vulnerability. - Verify actions performed by the compromised account with elevated privileges. - Force password resets for potentially affected accounts. - Restore affected systems from clean backups if necessary				
DLGC	Storage management	Lack of traceability	Without proper logging, it becomes difficult to track who accessed or changed data, complicating audits or breach investigations.	Mistakes made by employees or users	System misconfiguration, accidental data loss	4	3	2	24	Data Management Team	Enable and configure event logging in DLGC (access, data modifications, etc.). - Archive and protect audit logs. - Perform regular log reviews to detect suspicious activities. - Ensure each action is attributable to a unique user. Correction - If a breach or unauthorized modification is suspected, analyse available logs to reconstruct events. - Implement or improve logging mechanisms if existing ones are insufficient. - Train staff on the importance of traceability and log usage	4	2	1	8
PCPaie	Payroll management	Theft of sensitive data	Personal salary or employee information could be stolen,	False claims about sustainability initiatives	Damaged reputation, legal consequences	4	2	3	24	HR Department	Encrypt the PCPaie database and backups. - Restrict access to PCPaie software and its data to authorized HR/Payroll personnel only. - Use strong, unique passwords for PCPaie access. - Secure workstations used to access PCPaie	4	1	2	8

			leading to identity theft or internal fraud.								(antivirus, firewall, updates). - Implement controls to prevent unauthorized export of payroll data. - Train HR/Payroll staff on personal data protection. Correction - Identify the source and extent of the data theft. - Take immediate action to stop the theft and secure the data. - Notify affected employees and competent authorities (DPA) in accordance with regulations. - Change all access passwords and strengthen security measures				
PCCompta	Accounting	Unauthorized access to accounting data	Access by unauthorized users could lead to data theft or tampering.	Data not being encrypted during transmission	Data breaches, unauthorized access to sensitive info	4	2	3	24	Finance Department	Use strong, unique passwords for PCCompta access. - Define user profiles with granular access rights to different PCCompta modules and features. - Restrict physical and logical access to the server hosting PCCompta. - Regularly update PCCompta and the server's operating system. - Enable and monitor PCCompta audit logs. - Encrypt the accounting database and backups. Correction - Immediately change all PCCompta access passwords. - Identify the source of unauthorized access and block it. - Analyse logs to determine actions performed by the intruder. - Verify the integrity of accounting data and restore from backup if necessary.	4	1	2	8
Kaspersky Controller	Antivirus control	Antivirus engine vulnerabilities	Bugs or unpatched flaws in the	Failure to update security patches	Increased exposure to	3	3	2	18	IT Security Team	Ensure antivirus engine and signature database updates are applied automatically and promptly on all endpoints.	3	2	1	6

			antivirus software may allow malware to bypass detection.		known vulnerabilities						- Follow Kaspersky security bulletins to stay informed about vulnerabilities affecting the antivirus engine. - Test new antivirus engine versions in a pre-production environment before widespread deployment. - Segment the network to limit the spread of an attack if an engine vulnerability is exploited. Corrective - Immediately apply the patch or engine update as soon as it is available. - Isolate potentially compromised machines if a vulnerability is actively exploited. - Perform a full system scan with the updated engine to detect any prior infections. - Analyse logs for signs of vulnerability exploitation.				
DLGC	Billing	Fraudulent use of information	Misuse of client or internal billing data for personal or malicious purposes.	Lack of defined security standards or procedures	Increased security risks, uncoordinated response	3	2	3	18	Data Management Team	Implement clear policies regarding the use of billing information. - Train employees on fraud risks and reporting procedures. - Monitor transactions and access to billing data for suspicious activities. - Perform background checks for employees with access to sensitive financial data. - Limit rights to export and print billing data. Correction - Investigate any suspicion of fraudulent use. - Take disciplinary and/or legal action against those responsible. - Assess the impact of the fraud and take steps to recover losses if possible. - Strengthen internal controls to prevent future incidents.	3	1	2	6

Active Directory	User and session management	Poor access rights management	Excessive or poorly defined permissions may lead to unauthorized access or data exposure.	Attacker exploits flaws in system controls	System manipulation, potential data corruption	4	2	2	16	System Administration	Conduct regular and systematic reviews of access rights (at least quarterly). Implement a formal access request and approval process. - Use security groups to assign permissions rather than direct user assignments. - Promptly remove or disable inactive accounts. - Implement alerts for changes to high-privilege groups (Domain Admins). - Clearly document roles and responsibilities associated with each access level. Corrective - Immediately revoke excessive or incorrect access upon identification. - Analyse the potential impact of inappropriate access (unauthorized data viewing). - Identify the cause of incorrect rights assignment and improve the process. - Conduct a full audit of rights to ensure no other similar cases exist.	4	1	1	4
Smart PSS	Video surveillance	Interception of video streams	Unencrypted or poorly secured streams could be captured by unauthorized individuals.	Unauthorized access to confidential data	Privacy violations, regulatory penalties	4	2	2	16	Security Operations	Use encrypted connections (HTTPS, VPN) to access video streams remotely. - Regularly audit network configuration for weaknesses. Corrective - Identify the interception point and secure communication (set up VPN, fix network flaw). - Analyse the extent of the interception (which cameras, for how long). - Assess the impact of the information leak. - Change encryption keys if necessary	4	1	1	4
Aruba Controller	Access point control	Misconfiguration of access	Poorly set access parameters could allow unintended	Attacker gains unauthorized access to control system	Risk of system manipulation and data corruption	4	1	3	12	Network Administration	Establish and enforce a strict configuration management policy for access points. - Use standardized configuration templates and perform peer reviews for any changes. - Implement role-based access control (RBAC)	4	1	2	8

			users or devices to connect to sensitive parts of the network.								for Aruba controller administration. - Regularly audit access point configurations for compliance with security policies. - Limit physical access to access points. - Train IT staff on secure configuration practices for Aruba equipment. - Use a centralized management system (Aruba Central) to ensure configuration consistency. - Regularly back up access point configurations.				
GTC	Centralized technical management	Intrusion into systems	Weaknesses in centralized management could allow full access to critical systems by unauthorized users.	Mismanagement of physical security infrastructure	Increased risk of unauthorized access or theft	3	2	2	12	IT Operations	Secure physical and logical access to GTC (Centralized Technical Management) systems. - Use secure and encrypted communication protocols for GTC data exchange. - Segment the GTC network from the company's general IT network. - Regularly update software and firmware of GTC components. - Implement strong authentication for access to GTC management interfaces. - Conduct regular security audits of GTC systems. Corrective - Isolate compromised GTC systems from the rest of the network. - Identify the intrusion method and patch the exploited vulnerability. - Analyse the extent of the compromise and actions performed by the intruder. - Restore systems from a clean backup if necessary. - Change all access credentials for GTC systems.	3	1	1	3
Smart PSS	Video surveillance	Unauthorized access to cameras	Attackers might view or control surveillance cameras,	Financial data exposed to unauthorized parties	Major financial loss, compliance issues	4	1	3	12	Security Operations	Use strong, unique passwords for each camera and for the Smart PSS system, and change them regularly. - Update camera firmware and Smart PSS software as soon as patches are available.	4	1	2	8

			breaching physical security.								- Segment the video surveillance camera network from the company's main network. - Restrict access to the Smart PSS system and camera feeds to authorized users only. - Disable unused services and ports on cameras (Telnet, UPnP). - Use encryption for video streams if supported (HTTPS, SRTP). Corrective - Immediately change all access passwords for cameras and the Smart PSS system. - Identify and block unauthorized access. - Analyse logs to determine if feeds were viewed or configurations modified. - Check if recordings were compromised or exfiltrated. - Apply missing security patches				
DLGC	Storage management	Loss or theft of data	Unsecured storage may lead to accidental loss or external theft of sensitive data.	Attackers infiltrating the network via devices	Data theft or system manipulation	3	2	2	12	Data Management Team	Implement regular and automated backups of DLGC data. - Regularly test backup restoration. - Secure physical access to servers and backup media. - Use encryption for stored data and backups. - Implement strict access control to the DLGC database. - Monitor access to sensitive data Corrective - In case of loss, restore data from the last valid backup. - In case of theft, identify the source of the leak and take measures to seal it. - Analyse the extent of data loss or theft and notify affected parties if necessary. - Change access credentials and strengthen security measures.	3	1	1	3

DLGC	Storage management	Poor access management	Inappropriate access configurations can enable unauthorized users to access or alter data.	Malicious actors intercepting video feeds	Privacy breach, potential data misuse	3	2	2	12	Data Management Team	Define user profiles with specific access rights to DLGC modules and data. - Apply the principle of least privilege. - Regularly audit user access rights in DLGC. - Implement a formal process for user account management (creation, modification, deletion). - Use strong passwords for DLGC access. Correction - Immediately revoke or correct inappropriate access. - Analyse if data was accessed or modified without authorization. - Strengthen access controls and review user profiles.	3	1	1	3
PCPaie	Payroll management	Unauthorized HR modifications	Personnel files or payroll data could be altered without proper authorization, affecting salaries or benefits.	Attackers gaining unauthorized access to systems	Data manipulation, theft, service disruption	4	1	3	12	HR Department	Implement a validation system (dual approval) for critical changes in Papay (salaries, bank details). - Use audit trails to track all changes to employee records and payroll data. - Limit modification rights to authorized and trained users only. - Perform regular reconciliations between Papay data and paper HR files or other source systems. - Regularly back up the Papay database. Correction - Identify unauthorized modifications and their author. - Cancel incorrect modifications and restore accurate data. - Analyse the impact of modifications (incorrect payments) and take corrective actions. - Strengthen access controls and validation procedures.	4	1	2	8
Aruba Controller	Access point control	Exploitation of controller vulnerabilities	Security flaws in the Aruba Controller	Malicious users gain access to	Risk of data leakage and	3	1	3	9	Network Administration	Implement a vulnerability management program, including monitoring for new vulnerabilities published by Aruba.	3	1	2	6

			could be exploited to gain control over network traffic or access points.	surveillance systems	surveillance breaches						- Segment the network to limit the potential impact of a controller compromise. - Restrict administrative access to the Aruba controller (management interfaces) to authorized users and networks only. - Use strong, unique administrative passwords for the controller. - Perform regular vulnerability scans on controllers. - Implement an IDS/IPS to monitor traffic to and from the controller. CORRECTIVE - Isolate the compromised controller from the network if possible. - Apply security patches or workarounds recommended by Aruba. - Analyse logs to identify the extent of the compromise and the attacker's actions. - Restore the controller from a clean backup, if necessary, after patching the vulnerability. - Change all administrative credentials. - Audit configurations and connected systems for other signs of compromise				
Aruba Controller	Access point control	Unauthorized access to the Wi-Fi network	Attackers could exploit unsecured or weak Wi-Fi access to infiltrate the network, compromising data and internal systems.	Unauthorized users gaining access to the network	Compromise of network security and data integrity	1	2	4	8	Network Administration	Implement robust Wi-Fi security protocols (WPA3). - Use unique, complex passwords for Wi-Fi access and change them regularly. - Enable MAC address filtering if feasible and relevant. - Segment the network to isolate critical systems from general Wi-Fi access. - Regularly update firmware and software for Aruba controllers and access points. - Conduct regular security audits and penetration tests of the Wi-Fi network. - Disable unused SSIDs and rigorously secure	1	1	2	2

											guest networks.. - Train users on Wi-Fi security best practices (not connecting to unknown networks, identifying phishing). - Immediately change Wi-Fi passwords if a breach is suspected. - Identify and isolate compromised devices from the network. - Analyse logs to determine the extent of the breach and the exploited vulnerability. - Block MAC addresses of identified unauthorized devices. - Review and update security configurations following the incident. - Notify relevant parties according to the incident response plan.				
Kaspersky Controller	Antivirus control	Unauthorized access to the console	Gaining access to the antivirus admin panel could allow attackers to disable protection or tamper with settings.	Antivirus fails to detect malicious software	Increased risk of malware and ransomware attacks	4	1	2	8	IT Security Team	Use strong, unique passwords for access to the Kaspersky Security Centre console. - Implement two-factor authentication (2FA) for console access if available. - Restrict network access to the administration console to authorized IP addresses or subnets only. - Regularly audit accounts with console access and their privilege levels. - Regularly update Kaspersky Security Centre software to patch known vulnerabilities. - Monitor console access logs for suspicious login attempts. Corrective - Immediately change all console access passwords if a compromise is suspected. - Identify the source of unauthorized access and block it. - Analyse console logs to determine actions performed by the intruder.	4	1	1	4

											- Verify the integrity of security policies and antivirus configurations. - Restore configuration from a clean backup if necessary.				
Smart PSS	Video surveillance	Misconfiguration of user rights	Incorrect rights assignment could let unauthorized users control or delete footage.	Unauthorized sharing of data	Data exposed to unintended recipients	4	1	2	8	Security Operations	Apply the principle of least privilege for Smart PSS system users. - Define clear user roles with specific permissions (view only, PTZ control, access to recordings, administration). - Regularly audit user rights in Smart PSS. - Implement an approval process for assigning access rights. - Train administrators on secure user rights management. Corrective - Immediately correct improperly assigned rights. - Revoke unnecessary or excessive access. - Analyse if unauthorized actions were performed (deletion of recordings). - Review the rights assignment process to prevent recurrence	4	1	1	4
DLGC	Billing	Financial data leakage	Confidential billing data may be exposed to unauthorized individuals or systems.	Fraudulent actions by insiders or attackers	Data manipulation, theft of assets	4	1	2	8	Data Management Team	Restrict access to billing modules and financial data to authorized users only. - Encrypt sensitive financial data stored in DLGC and during backups. - Secure communication channels when transmitting billing data (encrypted emails, secure portals). - Implement controls to prevent unauthorized export of financial data. - Conduct specific security audits on billing modules. Correction - Identify the source and extent of the financial data leak.	4	1	1	4

											- Take immediate action to stop the leak (revoke access, patch a vulnerability). - Notify affected customers and regulatory authorities, in accordance with legal obligations. - Analyse the impact of the leak and strengthen data protection measures.				
Pccompta	billing	Data alteration	Fraudulent or accidental changes to financial records could disrupt operations or cause compliance issues.	Failure to comply with regulatory requirements	Fines, reputation damage	4	1	2	8	IT Management	Implement data integrity controls in DLGC. - Use audit trails to track all changes to billing data. - Separate duties so that one person cannot perform and validate critical financial changes. - Perform regular reconciliations of financial data. - Frequently back up billing data. Correction - Identify altered data and the source of the alteration. - Restore correct data from backups or audit logs. - Correct the cause of the alteration (human error, security flaw, malicious act). - Implement additional controls to prevent future alterations	4	1	1	4
PCPaie	Payroll management	Lack of encryption	Unencrypted data can be intercepted during transmission or storage, compromising privacy.	Malicious software locks or corrupts files	Data loss, system downtime, financial loss	3	1	2	6	HR Department	Ensure the PCPaie database is encrypted at rest. - Encrypt PCPaie backups. - Use secure communication channels (VPN, HTTPS) if PCPaie is accessed remotely or if data is transferred. - Encrypt sensitive data exports (bank transfer files) if possible. Correction - Implement encryption for unencrypted data and/or communications. - Assess if data was compromised due to lack of encryption.	3	1	1	3

											- Change encryption keys if an old unencrypted system is replaced.				
PCCompta	Accounting	Fraudulent manipulation	Financial records could be deliberately altered to misrepresent accounts or cover up fraud.	Failure to record or track system activities	Unrecoverable data, difficulty in identifying breaches	3	1	2	6	Finance Department	Implement segregation of duties for critical accounting operations. - Require dual validation for important or unusual accounting entries. - Perform regular internal and external accounting audits. - Use PCCompta audit trails to track all modifications. - Implement regular reconciliation controls (bank reconciliation, account analysis). - Train staff on accounting fraud risks. Corrective - Investigate any suspicion of fraudulent manipulation. - Identify the extent of the fraud and the amounts involved. - Take appropriate legal and disciplinary action. - Correct accounting entries and assess the impact on financial statements. - Strengthen internal controls to prevent future fraud.	3	1	1	3
Active Directory	User and session management	Theft of credentials	Usernames and passwords could be intercepted or phished, allowing attackers to impersonate legitimate users.	Incorrect network settings or rights assignment	Service disruption, unauthorized access	3	1	1	3	System Administration	Implement multi-factor authentication (MFA) for all users, especially for remote access and administrative accounts. - Train users to recognize phishing attempts and password management best practices. - Enforce strong password policies (complexity, length, history, no reuse). - Monitor for suspicious logins and unusual access attempts. - Protect domain controllers against Pass-the-Hash and Pass-the-Ticket attacks. - Use Endpoint Detection and Response (EDR) solutions.	3	1	1	3

											- Limit local credential caching (disable domain credential caching on non-critical workstations). Corrective - Immediately reset the password of the account whose credentials were stolen. - Revoke active sessions associated with the compromised account. - Analyse logs to identify malicious actions performed with the stolen credentials. - Identify the source of the credential theft (phishing, malware) and take remedial action. - Notify affected users and provide instructions.				