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

# Master's Dissertation

In partial fulfillment of the requirements for the master's degree
In Strategic Management and Information Systems

**Design and Modeling of a Risk Management Information System with Integrated Multi-Criteria Risk Assessment**
**Case of Ooredoo Algeria**

**Submitted by:**
Amina MAKOUDA
Hiba Ayat Errahmène MECHLIH

**Supervised by:**
Dr. Soumiya LADJOUZI

Academic year: 2025/2026

## Abstract

In the telecommunications sector, rapid technological disruption and escalating complexity continuously reshape risk exposure, making operational risk management a critical lever for organizational resilience. This study designs and models a Risk Management Information System (RMIS) tailored for Ooredoo Algeria, incorporating a multi-criteria risk assessment framework.

Employing a qualitative methodology, this research integrates semi-structured interviews with risk management professionals, field observations, and institutional document analysis. The findings indicate that while Ooredoo Algeria possesses a well-established risk culture, the lack of a centralized, automated system compromises data reliability and impedes efficient decision-making.

To bridge these gaps, the proposed RMIS model introduces a structured multi-criteria framework to prioritize operational risks and drive proactive mitigation strategies. However, successful implementation hinges on overcoming technical integration barriers and fostering robust cross-functional coordination. Ultimately, this study recommends a phased deployment of the RMIS to seamlessly align digital risk management infrastructure with the organization's overarching strategic objectives.



**Keywords:** RMIS, Enterprise Risk Management (ERM), multicriteria risk assessment, decision support systems, telecommunications strategy.

## Résumé

Dans le secteur des télécommunications, où les mutations technologiques et la complexité redéfinissent continuellement l'exposition aux risques, le management global des risques est devenu un levier stratégique de la résilience organisationnelle. Cette étude porte sur la conception et la modélisation d'un Système d'Information de Management des Risques (SIMR) pour Ooredoo Algérie, en intégrant une approche multicritère aux risques.

L'étude adopte une méthodologie qualitative, combinant des entretiens semi-directifs avec des professionnels du management des risques, une analyse documentaire, et des observations sur le terrain. Les résultats révèlent que, malgré une culture du risque bien établie, l'absence d'un système centralisé et automatisé limite la fiabilité des données ainsi que l'efficacité des processus de prise de décision.

Pour combler ces lacunes, le modèle proposé introduit un cadre multicritère permettant une hiérarchisation structurée des risques de l'entreprise et soutenant des stratégies de mitigation proactives. Toutefois, sa mise en œuvre reste tributaire du dépassement des contraintes d'intégration technique et du renforcement de la coordination transversale. L'étude recommande un déploiement progressif du SIMR, afin d'assurer l'alignement entre les outils digitaux de gestion des risques et les objectifs stratégiques de l'organisation.



**Mots-clés :** SIMR (Système d'Information de Management des Risques), Management des Risques de l'Entreprise (ERM), évaluation multicritère des risques, systèmes d'aide à la décision, stratégie des télécommunications.

## ملخص

تعيد التحولات التكنولوجية والتعقيدات صياغة طبيعة التعرض للمخاطر بشكل مستمر في قطاع الاتصالات، حيث أصبحت إدارة المخاطر الشاملة ركيزة استراتيجية لتعزيز المرونة التنظيمية. تركز هذه الدراسة على تصميم ونمذجة نظام معلومات لإدارة المخاطر لشركة أوريدو الجزائر، مع دمج منهجية متعددة المعايير للمخاطر.

تعتمد الدراسة على منهجية نوعية تدمج بين المقابلات نصف الموجهة مع مختصين في إدارة المخاطر، الملاحظات الميدانية والتحليل الوثائقي. وتكشف النتائج أنه على الرغم من وجود ثقافة راسخة لإدارة المخاطر داخل الشركة، إلا أن غياب نظام مركزي يحد من موثوقية البيانات وكفاءة عمليات اتخاذ القرار.

ولمعالجة هذه الفجوات، يقترح النموذج المقدم إطاراً متعدد المعايير يسمح بترتيب أولويات مخاطر المؤسسة بشكل هيكلي ويدعم استراتيجيات الاستجابة الاستباقية. ومع ذلك، يظل تنفيذ هذا النظام مرهوناً بتجاوز قيود التكامل التقني وتعزيز التنسيق بين مختلف المصالح. وتوصي الدراسة بنشر تدريجي لنظام معلومات إدارة المخاطر، بما يضمن المواءمة بين أدوات إدارة المخاطر الرقمية والأهداف الاستراتيجية للمنظمة.



**الكلمات المفتاحية:** نظام معلومات إدارة المخاطر، إدارة مخاطر المؤسسة، التقييم متعدد المعايير للمخاطر، نظم دعم القرار، استراتيجية قطاع الاتصالات.

## Acknowledgements

*My deepest gratitude ascends to Allah for the gift of this journey that has ended as beautifully as it began.*

*To the one who gave me a name I wear with pride, to the role model who believed in me, trusted me and my vision since day one, to my dad*

*To my successful female model, who supported me along this life path, to the one who covers me with her most silent, whispered prayers, to my beloved Ghalieuse*

*To Abdelhak & Mariem*

*To the source of the positive energy, to my beloved khaltou, to my nearest and dearest*

*To my professors, especially to our supervisor, Ms. Soumiya Ladjouzi, for her kind, inspiring, and empowering mentorship throughout this entire journey*

*to the team at Ooredoo, especially Mr. Adel Krelifa, Mr. Mohamed Riad Faid, and everyone who contributed to this experience. Thank you for the professional guidance and the warm welcome.*

*To the colleagues who shifted my perspectives and expanded my way of thinking*

*to the school that gave me a new lens through which I see the world.*

*A journey as long as this would not be as remarkable as it is without the amazing people I met along the way*

*To the gentle spirits whom Allah brought into my life, the girls with whom I shared the typical dream days and created unforgettable memories, to those kind hearts, "my click"*

*To the one who chose to walk beside me through this experience, my companion at the close of this chapter, my lovely courageous Hiba*

*To my soul's reflection, the sweetest, my Asmaa*

*To my forever favorite, my long-distance light, my home, Aya*

*To all my lifelong friends who have been with me through every season*

*To You, for making this journey a "beautiful" reality, for being the reason it is now forever an indelible part of my heart, my mind, my story*

*To myself, for the battles fought in silence, for simply not giving up,*

*thank you for making what once seemed like a far dream a reality*

*Not forgetting Yarissa, for the endless miles and the shared highs and lows*

*To everyone, each moment, and everything that has been part of this story and also of the victory.*

***Amina***

## Acknowledgements

*This thesis may have my name on it…*

*but it was never a one-person journey. It was built in conversations, carried by support, and held together by people who never let me fall too far behind.*

*To my mother Bentaleb Fahima, you are my constant. Your strength became mine long before I realized it.*

*Every sacrifice you made quietly shaped this moment. I hope this makes you proud—because everything I am started with you.*

*To my sister Mechlih Serine, you are my balance. In the middle of stress, deadlines, and overthinking, you reminded me how to breathe again. You kept me me—and that mattered more than anything.*

*To Tata Hayet, you were my calm voice in the noise,*

*like a gentle light in uncertain moments, you always knew how to guide me without overwhelming me. Your kindness, your patience, and your constant belief in me made this journey feel less heavy.*

*To my tutors, this work grew under your guidance.*

*To Mme Soumiya Ladjouzi —Thank you for your presence, your guidance, and for always pushing me to do better. Your encouragement made all the difference.*

*To Mr. Adel Krelifa, Mr. Mohamed Riad Faid, and the ERM team —thank you for making this real,*

*for trusting me, and for showing me what this work looks like beyond theory.*

*Because of you, this is more than a thesis; it's a step into something bigger.*

*To my binôme, Amina,*

*We really went through it all, didn't we?*

*Deadlines, stress, doubt, small wins that felt huge. Thank you for showing up every time, for pushing through with me, and for proving that teamwork can actually mean something real.*

*We didn't just finish this; we earned it. And finally…*

*To my friends, and to everyone who stood by me—loudly or quietly, in words or simply in presence. In your laughter and your presence, I found balance.*

*You were the pause I didn't know I needed.*

*If this work stands today, it is because I never stood alone.*

***Hiba***

## Table of contents

## List of tables

## List of figures

## List of appendices

## List of abbreviations

- **BPMN:** Business Process Modeling Notation
- **CCO:** Chief Commercial Officer
- **CEO:** Chief Executive Officer
- **CFO:** Chief Financial Officer
- **CHRO:** Chief Human Resources Officer
- **CLRO:** Chief Legal and Regulation Officer
- **CMO:** Chief Marketing Officer
- **COSO:** Committee of Sponsoring Organizations of the Treadway Commission
- **CPO:** Chief Procurement Officer
- **CSO**: Chief Sales Officer
- **CTIO**: Chief Technology and Information Officer
- **ERM:** Enterprise Risk Management
- **IS:** Information System
- **ISO:** International Organization for Standardization
- **IT:** Information Technology
- **KPI:** Key Performance Indicator
- **KRI:** Key Risk Indicator
- **MCDA:** Multi-Criteria Decision Analysis
- **MCDM:** Multi-Criteria Decision Making
- **MERISE:** Méthode d'Étude et de Réalisation Informatique pour les Systèmes d'Entreprise
- **MIS:** Management Information System
- **RMIS:** Risk Management Information System
- **UML:** Unified Modeling Language

## Glossary of key terms

- **Business Unit (BU) Representative:** An operational stakeholder responsible for identifying, reporting, and monitoring risks within a specific department.
- **Decision Support System (DSS):** An information system that assists decision-making through data analysis and modeling tools.
- **Enterprise Risk Management (ERM):** An integrated approach to identifying, assessing, managing, and monitoring risks across the organization.
- **Functional requirements:** Specifications describing the expected functionalities and operations of a system.
- **Governance, Risk, and Compliance (GRC):** A framework that integrates governance, risk management, and regulatory compliance processes.
- **IS architecture:** The structured design of an information system, defining its components and their interactions.
- **Key Performance Indicator (KPI):** A measurable value used to evaluate organizational performance.
- **Key Risk Indicator (KRI):** A metric used to signal potential increases in risk exposure.
- **Multi-Criteria Decision-Making (MCDM):** A method used to evaluate and prioritize alternatives based on multiple criteria.
- **Multi-Criteria Decision Analysis (MCDA):** A structured analytical approach for comparing options using weighted criteria.
- **Risk appetite:** The level of risk an organization is willing to accept in pursuit of its objectives.
- **Risk assessment:** The process of identifying and evaluating risks based on their likelihood and impact.
- **Risk owner:** The individual responsible for managing a specific risk and ensuring appropriate mitigation actions.
- **Risk Register:** A centralized repository that records identified risks, their characteristics, and mitigation actions.
- **Risk mapping (heat map):** A visual representation of risks based on their probability and impact.

- **Risk treatment:** The process of selecting and implementing measures to address risks.
- **Risk champion:** A designated stakeholder within a business unit responsible for promoting risk awareness, coordinating risk management activities, and acting as a liaison between operational teams and the ERM function.
- **System Integration:** The process of connecting different systems into a unified structure.
- **AS-IS process:** A representation of the current state of a business process.
- **TO-BE process:** A representation of the future optimized state of a process after improvement.
- **Workflow automation:** The use of technology to execute processes with minimal human intervention.
- **Risk Management Information System (RMIS):** A centralized system designed to support the identification, assessment, monitoring, and reporting of risks.
- **Multicriteria risk scoring:** A method of evaluating risks using multiple weighted criteria.
- **Composite risk score:** A calculated value representing the overall importance of a risk.
- **Risk lifecycle:** The sequence of activities involved in managing risks, from identification to monitoring.
- **Escalation process:** A mechanism for raising critical risks to higher management levels.
- **Risk dashboard:** A visual interface displaying key risk indicators and performance metrics.

# Introduction

In an increasingly volatile, uncertain, and digitized global environment, organizations are confronted with a growing complexity of risks that threaten their operational continuity and strategic objectives. This is particularly true for the telecommunications sector, where high dependence on information systems makes the management of risks a critical strategic pillar. As firms undergo digital transformation, the ability to identify, track, and mitigate risks becomes a primary lever for organizational resilience and competitive advantage.

In this perspective, Risk Management Information Systems (RMIS) have emerged as an important evolution in governance practices. A risk management information system can be understood as a centralized system that gathers risk-related information, supports process automation, and provides decision-makers with timely and structured insights. While traditional approaches based on standards such as ISO 31000 offer a solid framework, there remains room for improvement. In particular, integrating Multi-Criteria Decision-Making (MCDM) methods allows for a more nuanced prioritization of risks by incorporating additional strategic dimensions into the analysis.

This research focuses on Ooredoo Algeria, a major actor in the national telecommunications sector with over 15 million subscribers nationwide. The company demonstrates a relatively mature approach to risk management, aligned with ISO 31000 guidelines. However, current practices rely on multiple stakeholders and dispersed tools, which can limit efficiency and visibility. This situation highlights the need to move toward a more integrated system. The present study therefore proposes the design of a conceptual RMIS adapted to Ooredoo's context, with the aim of structuring existing processes, centralizing data, and improving traceability in real time.

Based on these elements, the central research question is formulated as follows:

**"How to design a system architecture to structure, centralize, and improve risk management within a complex organization like Ooredoo?"**

To address this central research question, the study is guided by three sub-questions:

- **RQ1:** How is the risk management process currently structured at Ooredoo Algeria, and what are the functional and informational requirements for transitioning toward an integrated system?
- **RQ2:** What functional architecture and conceptual models—encompassing processes, actors, and data flows—are necessary to design a Risk Management Information System (RMIS) specifically tailored to Ooredoo's operational environment?

- **RQ3:** In what ways can the integration of Multi-Criteria Decision-Making (MCDM) improve risk prioritization and enhance risk management practices?

The main objective of this research is to design and model a RMIS that strengthens the structuring, traceability, and strategic management of risks at Ooredoo Algeria. To achieve this, several steps are pursued:

- Organizational analysis: To evaluate Ooredoo's current risk management against international standards and identify the functional gaps that require automation.
- Target architecture: To design a centralized functional and technical framework for the RMIS that meets the specific needs of the organization.
- Process Modeling: To create clear "TO-BE" workflows and conceptual data models using BPMN and UML to ensure better risk traceability.
- Decision-support design: To integrate multi-criteria assessment into a system that provides general management with automated prioritization and strategic dashboards.

To provide a comprehensive answer to the research questions, this thesis is organized into three main chapters:

**Chapter I: Literature review and conceptual framework**

This chapter establishes the theoretical foundations of risk management and information systems. It explores the integration of multi-criteria approaches into risk assessment and constructs a conceptual framework bridging international standards with IS design methodologies.

**Chapter II: Methodological framework and host organization**

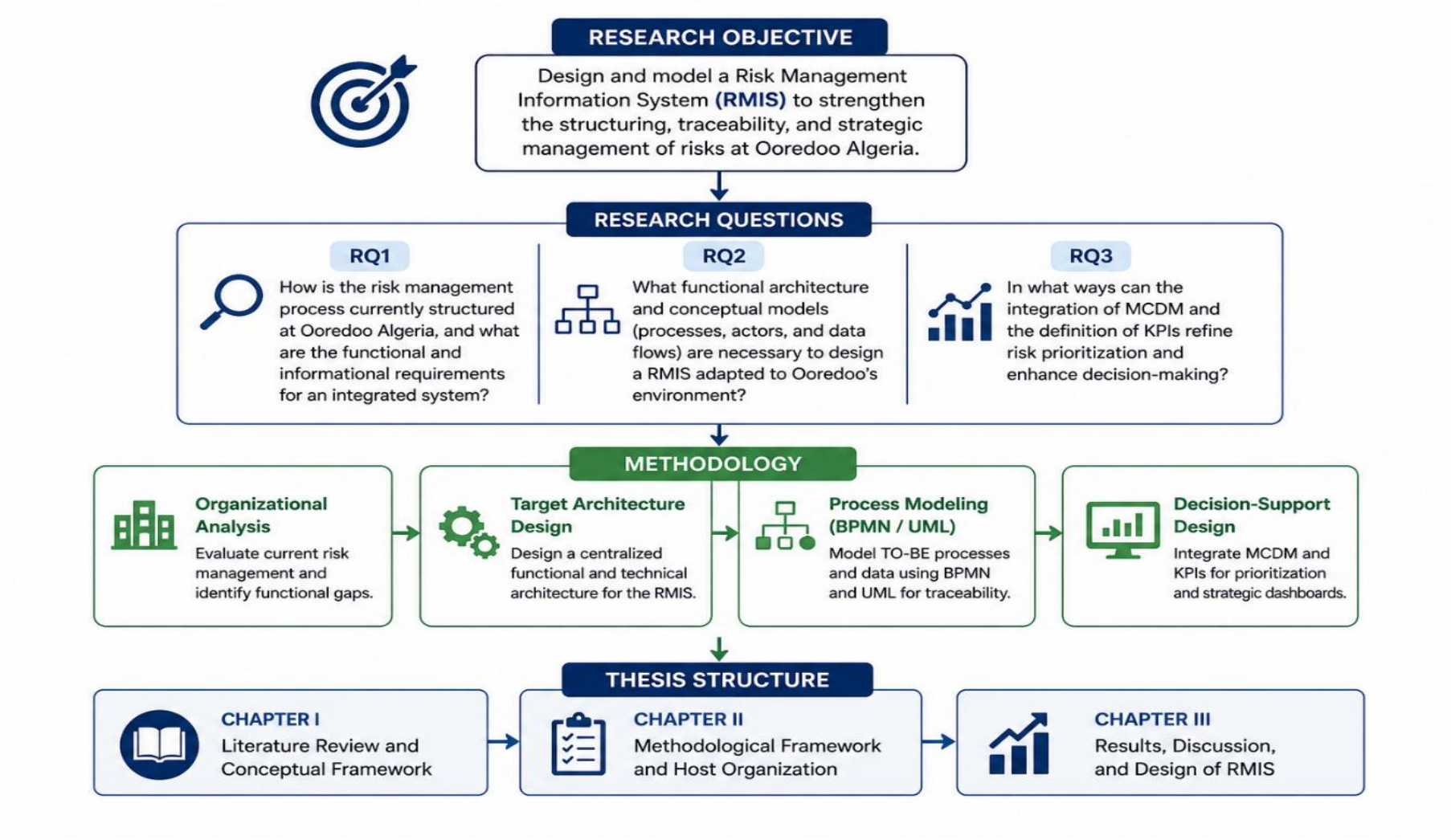
It details the research strategy, data collection tools, and the analytical approach used. This chapter also provides a diagnostic of Ooredoo Algeria, focusing on its organizational structure and the existing risk management processes.

**Chapter III: Results, discussion, and design of a RMIS**

This final chapter presents the results of the qualitative analysis conducted with key organizational actors to define system requirements. It outlines the target functional architecture of the proposed RMIS, details the process modeling through BPMN and UML, and concludes with the integrated multi-criteria framework and strategic recommendations for risk governance.

A synthetic overview of the research structure is presented in the figure below:

*Figure 1: Research overview and conceptual framework*




**Source:** Elaborated by authors.

# Chapter I: Literature review and conceptual framework

Risk management has become a key priority for organizations operating in uncertain and rapidly evolving digital environments. In this context, information systems dedicated to risk management are essential tools for strengthening resilience and supporting informed decision-making, which underpins this research.

This chapter sets out the theoretical and conceptual foundation for designing and modeling a Risk Management Information System (RMIS) at Ooredoo Algeria. It is structured into two sections. The first section provides a literature review following a geographic progression, from the global level to the African and then the Algerian context. The second section focuses on the conceptual framework of the study, outlining the key concepts, models, and relationships that guide the design of the proposed system.

## Section 1: Literature review

This section provides a synthesis of academic works pertaining to organizational risk management and the contributions of information systems in this domain. It allows for the identification of existing theoretical foundations, the positioning of the research problem within the telecommunications sector, and the delineation of the analytical axes necessary for the design of a Risk Management Information System integrating multi-criteria assessment.

## 1. Global trajectories and organizational maturity in risk management

The evolution of risk management is marked by a global transition from informal practices toward structured maturity models that drive strategic resilience.

### 1.1. From informal practices to structured frameworks

Historically, risk management has evolved from a collection of isolated, informal actions into a series of structured, universally recognized frameworks such as COSO-ERM, ISO 31000, and COBIT, which provide organizations with standard guidelines, principles, and repeatable processes to manage uncertainty effectively (Efe, 2023). Modern enterprise risk management (ERM) represents a holistic approach that moves beyond traditional silos to identify and assess potential strategic, financial, and operational threats that could impede organizational goals (Al Lawati et al., 2025). This transition has been accelerated by the arrival of advanced technologies, which have introduced complex new variables that often overwhelm basic analytical capabilities, necessitating more sophisticated, structured frameworks for decision support (Więckowski et al., 2023).

### 1.2. Levels of maturity in risk management: models and indicators

The maturity of risk management within an organization can be assessed through various indicators and models that help leadership implement appropriate security policies and ensure operational processes run smoothly (Metin et al., 2024). Maturity models, such as the Capability Maturity Model Integration (CMMI), allow organizations to align their risk frameworks with operational departments and measure the effectiveness of their IT risk management practices (Al-Dosari & Fetais, 2023). At higher levels of maturity, risk management is not a static obligation but is viewed as an "organic" and dynamic strategic asset that facilitates better risk-taking and provides a source of long-term competitive advantage (Ruiz-Canela López, 2021).

### 1.3. Comparative perspectives: Global trends, African realities, and the Algerian context

The following table synthesizes the comparative perspectives of risk management based on existing literature:

*Table 1: Comparative perspectives of risk management*

| Feature | Global Trends | African Realities | Algerian Context |
|---|---|---|---|
| **Framework adoption** | Widespread use of COSO, ISO 31000, and NIST RMF to address complex, interconnected global risks (Efe, 2023). | Adoption is growing as a response to volatility, though implementation can often be limited to specific business units or sectors (Ruiz-Canela López, 2021). | Localized empirical application of advanced methodologies, such as AHP-TOPSIS, has been observed in specific sectors to optimize quality and priorities (Chaube et al., 2024). |
| **Maturity focus** | Transitioning toward "Cyber-Resilience," prioritizing proactive recovery and adaptation over reactive compliance (Al-Dosari & Fetais, 2023). | Focus is often on benchmarking against industry peers to enhance operational performance and results (Ruiz-Canela López, 2021). | Utilization of multi-criteria decision analysis (MCDA) to bridge the gap between subjective managerial judgments and objective resource allocation (Chaube et al., 2024). |
| **Sectoral focus** | Highly mature in financial services and insurance; rapidly evolving in manufacturing and energy (Ruiz-Canela López, 2021). | Significant interest in the telecommunications and construction sectors to stabilize financial performance under oil price fluctuations and geopolitics (Al Lawati et al., 2025). | Integration of structured decision tools (like AHP) to handle interdependencies and specific criteria in project-based environments (Chaube et al., 2024). |

**Source:** Elaborated by authors based on the analyzed articles.

The comparative reading of this table reveals a structural asymmetry that deserves explicit acknowledgment: while global frameworks are progressively oriented toward proactive cyber-resilience, the African and Algerian contexts remain, according to the available literature, predominantly reactive and sector-fragmented in their approach. This gap is not merely a question of methodological lag, it reflects deeper institutional and resource constraints that condition the pace of risk management formalization.

## 2. Information Systems and digitalization in risk management: Roles, impacts, and limits

While modern information systems are essential for data-driven risk analysis, their effectiveness is often constrained by implementation challenges and the evolving landscape of digital threats.

### 2.1. The role of IS and RMIS in organizational risk management

A Risk Management Information System (RMIS) acts as a centralized, automated repository—centered around a dynamic risk register—that supports the systematic identification, analysis, and treatment of risks throughout an organization's operational lifecycle (Almutairi & Saleh, 2026). By providing data-driven and transparent decision-making power, Management Information Systems (MIS) have evolved from simple cost-reduction tools into strategic enablers that ensure managers have accurate information for both short- and long-term resource management (Madanchian & Taherdoost, 2025).

### 2.2. Impact of digital transformation on risk management practices

Digital transformation has significantly expanded the scope of cyber threats by creating more "digital touchpoints," such as APIs and cloud services, which require innovative and automated risk management solutions to protect sensitive data and ensure business continuity (Metin et al., 2024). Modern digitalization necessitates dynamic IT risk management frameworks that can adapt to rapid technological shifts, such as Industry 4.0 and 5.0, where cyber-physical systems and the Internet of Things (IoT) introduce unprecedented levels of network interconnectivity (Barraza de la Paz et al., 2023).

### 2.3. Current limitations and challenges of existing systems

Existing risk management frameworks often suffer from a high degree of abstractness and vague guidelines, making them difficult and expensive for many organizations to implement effectively (Al-Dosari & Fetais, 2023). Furthermore, many current RMIS tools are criticized for being overly complex and primarily targeted at large enterprises, often

failing to address human factors or the dynamic causal relationships between different security elements (Almutairi & Saleh, 2026) (Al-Dosari & Fetais, 2023).

For an organization like Ooredoo Algeria, operating in a complex regulatory and competitive environment, this critique underscores the importance of designing a RMIS that complements quantitative multi-criteria outputs with interpretive flexibility, a design principle that informs the methodological choices of the present research.

# 3. Multi-criteria methods in risk assessment: Applications, contributions, and boundaries

Multi-Criteria Decision Analysis (MCDA) offers a structured mathematical approach to navigating complex risk landscapes where strategic goals and conflicting priorities must be balanced.

## 3.1. Multi-criteria analysis in organizational decision-making

Multi-Criteria Decision Analysis (MCDA) provides a robust mathematical framework that allows decision-makers to evaluate and rank multiple alternatives based on conflicting criteria, ensuring that final choices are aligned with the company's strategic goals (Madanchian & Taherdoost, 2025). By integrating various technical, economic, and environmental factors, MCDA allows for a more holistic perspective that can accommodate the subjective preferences of stakeholders alongside objective data (Chaube et al., 2024).

## 3.2. Applications in risk prioritization: AHP, ELECTRE, TOPSIS, PROMETHEE

- **AHP (Analytic Hierarchy Process):** Widely favored for its versatility and user-friendliness, it allows for the decomposition of complex problems into a hierarchical structure of criteria and sub-criteria for pairwise comparison (Chaube et al., 2024) (Madanchian & Taherdoost, 2025).
- **TOPSIS:** Effective for ranking options according to their geometric proximity to a positive ideal solution and their distance from a negative ideal solution (Madanchian & Taherdoost, 2025).
- **ELECTRE & PROMETHEE:** Often utilized for selecting between discrete actions or managing water and healthcare resources by handling qualitative and quantitative information (Madanchian & Taherdoost, 2025).
- **ANP (Analytic Network Process):** Used to model interdependencies between criteria and stakeholders, providing a more realistic but mathematically demanding evaluation for complicated systems (Madanchian & Taherdoost, 2025).

Among these methods, the AHP-TOPSIS hybrid has received particular scholarly attention as a balanced compromise between structural rigor and computational accessibility.

### 3.3. Empirical contributions and boundaries of applicability

Empirical studies have shown that integrated hybrid models, such as AHP combined with TOPSIS, are more insightful than single-method approaches, particularly in areas like supplier selection and performance evaluation (Chaube et al., 2024) (Hanine et al., 2016). However, the applicability of these methods can be limited by the complexity of weight calculations as the number of criteria increases, often requiring software aid to manage the volume of mathematical operations (Hanine et al., 2016).

This acknowledged limitation merits careful attention in the context of the present research. As the number of risk criteria within a telecommunications operator's environment can be substantial—spanning operational, cybersecurity, regulatory, and reputational dimensions—the risk of weight inconsistency in AHP pairwise comparisons increases proportionally.

## 4. Risk management in the telecommunications sector: Specificities, tools, and identified gaps

The telecommunications industry operates within a high-stakes environment where unique operational threats demand specialized tools and a clear understanding of existing research gaps.

### 4.1. Sector-specific risks in telecommunications

The telecommunications sector faces unique operational risks, including high customer churn, poor quality of service provision, equipment failures, and rapid technological changes that can lead to billions of dollars in losses (Ruiz-Canela López, 2021). These risks are categorized into nine specific types, such as damage to physical assets (networks and facilities), fraud, and non-compliance with legal standards (Ruiz-Canela López, 2021).

In the specific case of the Algerian telecommunications market, these generic sectoral risks are compounded by additional contextual factors, including regulatory fragmentation, infrastructure disparities between urban and rural zones, and the competitive dynamics introduced by the coexistence of public and private operators.

### 4.2. IS and tools mobilized for risk management in the sector

To manage these risks, the sector utilizes frameworks like COBIT 5, which offers specific audit and governance principles for IT risk management (ITRM), and operational risk self-assessment (OpRSA) methods to calculate economic impacts using actuarial techniques (Ruiz-Canela López, 2021) (Berrada et al., 2023). Furthermore, telecommunications companies are increasingly adopting Risk Management Information Systems to consolidate critical information into risk registers, ensuring that risk exposure is transparently reflected in project performance indicators (Almutairi & Saleh, 2026).

### 4.3. Identified gaps in research and practice

There is a notable lack of contrasted references and quantitative evaluation methods specifically tailored for the telecommunications sector compared to the mature models used in the banking and insurance industries (Ruiz-Canela López, 2021). Additionally, many academic solutions lack real-world empirical validation, and existing frameworks often fail to account for the dynamic security ecosystems required for emerging technologies like cloud computing and IoT (Al-Dosari & Fetais, 2023).

## 5. Critical synthesis: Convergences, gaps, and the rationale for an integrated approach

The disconnect between existing risk frameworks and operational reality necessitates a shift toward integrated systems that can handle the complex interdependencies of the telecommunications sector.

### 5.1. Comparative overview and shared limitations of existing approaches

While frameworks like ISO 31000 and COSO-ERM provide essential global standards, they are often perceived as overly theoretical or as "checklists" that lack specific evaluation techniques for non-financial industrial sectors. Many existing approaches also follow a "silo" mentality, analyzing individual environments while neglecting the complex interdependencies within supply chain networks and human behavioral factors.

### 5.2. The missing link: Absence of IS and multi-criteria integration

A significant research gap exists in the absence of an integrated approach that embeds multi-criteria assessment directly within a dedicated Risk Management Information System. While MCDA provides the logic for prioritization and RMIS provides the data repository, their integration is necessary to move from manual, error-prone spreadsheets to a proactive, automated, and dynamic risk management environment.

The absence of this integration is not incidental, it reflects a disciplinary divide between the information systems community, which has historically prioritized system architecture and data management, and the operations research community, which has developed MCDA methods largely independently of IS design considerations.

This research gap constitutes the primary scientific contribution of the present work: bridging the IS design tradition with multi-criteria analytical methodology in a single, coherent, and empirically grounded system.

### 5.3. Justification of the proposed research model

The proposed model, focusing on the design and modeling of a RMIS with multi-criteria risk assessment for Ooredoo Algeria, is justified by the need to operationalize MIS theory through the integration of performance metrics and precise multi-criteria evaluation. By employing established modeling techniques like UML and integrated AHP-TOPSIS methodologies, the research aims to provide a customized, scalable management tool that enhances transparency and decision-making accuracy within the specific dynamic context of an Algerian telecommunications provider.

Taken together, the reviewed literature converges on a shared diagnostic: existing tools are either analytically powerful but contextually blind or contextually relevant but methodologically limited. The present research responds to this dual inadequacy by proposing a system that is simultaneously theoretically grounded—drawing on established MCDA and RMIS scholarship—and contextually situated within the operational realities of Ooredoo Algeria. In doing so, it positions itself not as an incremental contribution to an existing literature but as a deliberate methodological bridge between two scholarly traditions that have, until now, advanced largely in parallel.

### 5.4. Researcher Positioning

This research is positioned at the intersection of Enterprise Risk Management, Management Information Systems, and multi-criteria decision support. The literature shows that risk management frameworks provide strong governance principles, while RMIS solutions support centralization, monitoring, and reporting. However, the integration of multi-criteria assessment within a dedicated risk management information system remains insufficiently addressed, particularly in the telecommunications context.

Based on this gap, the present study adopts a design-oriented perspective. It does not aim to develop a new risk management standard but rather to model an integrated RMIS adapted to Ooredoo Algeria's organizational context. The objective is to combine centralized risk information, structured processes, and multi-criteria prioritization in order to support more coherent, traceable, and decision-oriented risk management practices.

## Section 02: Conceptual framework

This section establishes the conceptual foundations underpinning the present study. Three complementary analytical dimensions are examined in sequence: risk management as an organizational discipline, information systems as strategic infrastructure, and multi-criteria risk assessment as a decision-support methodology. Rather than treating these dimensions in isolation, this framework positions them as mutually reinforcing, each one informing and constraining the design choices made in the proposed approach. The theoretical articulation developed here provides the basis for the empirical and methodological choices presented in subsequent sections.

## 1. Risk management

To build a clear understanding of the subject, this section covers the history, definitions, and integrated processes of modern risk management.

### 1.1. Historical evolution of risk management

Risk has always been an integral part of human activity, long before it was formalized as an academic discipline. Across different periods, individuals and organizations have continuously sought ways to deal with uncertainty and protect their economic and strategic interests. These early practices, although not structured, already reflected a fundamental idea that remains central today: the need to anticipate and manage uncertainty.

A major turning point occurred in the 17th century with the development of probability theory by mathematicians such as Blaise Pascal and Pierre de Fermat. For the first time, uncertainty could be approached in a structured and quantitative manner rather than relying solely on intuition (Bernstein, 1996). This intellectual shift laid the foundations for modern risk analysis and enabled the later development of insurance systems and financial models.
In the 20th century, the nature of risks became more complex due to industrialization and technological progress. Organizations were no longer facing isolated risks but interconnected and sometimes systemic ones (Aven, 2016). This led to the development of more rigorous analytical tools, such as Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA), particularly in high-risk industries (Aven, 2016). At the same time, financial theories introduced new ways of understanding and optimizing risk.

However, one of the most important turning points came from major organizational failures, such as the collapse of Barings Bank and the Enron scandal. These events clearly showed the limits of fragmented approaches to risk management (Power, 2004).

As a result, organizations progressively moved toward more integrated approaches, notably Enterprise Risk Management (ERM), supported by international standards such as ISO 31000. Today, risk management is no longer seen as a secondary function but as a strategic necessity, especially in a context marked by digital transformation and increasing uncertainty (International Organization for Standardization (ISO), 2018).

### 1.2. Definitions and fundamental principles

Risk is a complex concept that varies across disciplines. In management sciences, one of the most widely accepted definitions is provided by ISO 31000:2018, which defines risk as the "effect of uncertainty on objectives." This definition is particularly relevant because it links risk directly to organizational goals and highlights that risk is not always negative, it can also represent opportunities.

In practice, risk is generally analyzed through three main elements: its source, the likelihood of occurrence, and its potential consequences. The combination of these elements allows organizations to assess the level of risk and decide how to manage it. However, ISO 31000:2018 insists on an essential point: risk must always be understood within its context. What is considered a major risk for one organization may be insignificant for another, depending on its objectives and environment (Hopkin, 2017; International Organization for Standardization (ISO), 2018).

Beyond definitions, ISO 31000 also proposes a set of principles that guide effective risk management. These principles emphasize that risk management should be integrated into all organizational activities, rather than treated as a separate function. It should be structured, based on reliable information, and adapted to the organization's context. It must also take into account human and cultural factors, which play a key role in how risks are perceived and managed. Overall, these principles reflect a more modern view of risk management, where it becomes a tool for better decision-making rather than just a control mechanism (International Organization for Standardization (ISO), 2018).

The following figure presents the ISO 31000:2018 risk management framework, emphasizing the central role of leadership and commitment in ensuring the effective integration and continuous improvement of risk management practices.

*Figure 2: Risk management process according to ISO 31000:2018*


**Source:** (International Organization for Standardization (ISO), 2018).

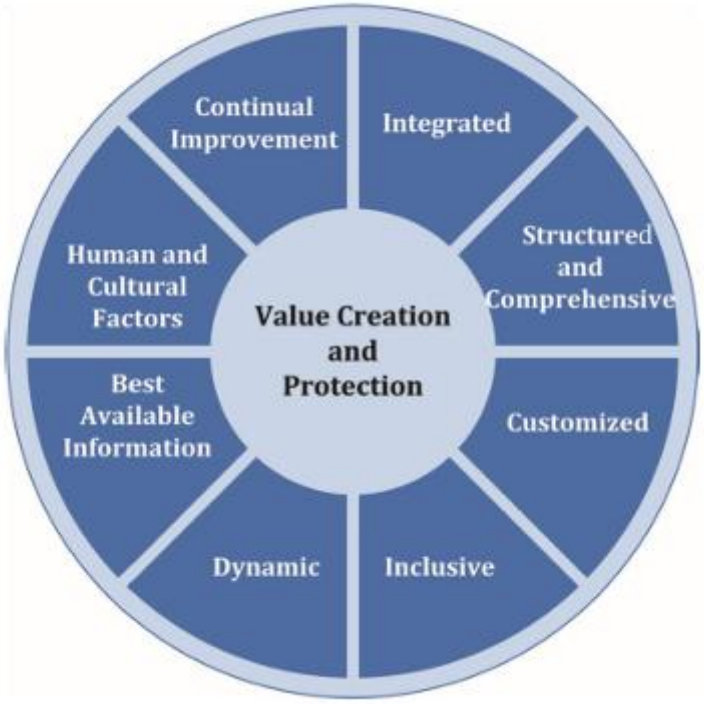
### 1.3. International standards and frameworks

The development of international risk management frameworks reflects the need to standardize practices in an increasingly complex and interconnected environment. As organizations faced diverse and evolving risks, the need for a common and structured approach became essential.

Among these frameworks, ISO 31000 is considered the most universal reference. Developed by the International Organization for Standardization and revised most recently in 2018, it provides principles, a framework, and a process applicable to any organization, regardless of size, sector, or the nature of the risks it faces. It provides a comprehensive approach based on three key elements: principles, a framework, and a process. These components ensure that risk management is integrated into organizational governance, strategy, and operations. The process includes the main steps of risk management, from context definition to risk identification, assessment, treatment, and monitoring. In addition, ISO 31000 emphasizes leadership involvement and the continuous improvement of risk management practices (International Organization for Standardization (ISO), 2018).

The fundamental principles of risk management according to ISO 31000:2018 are illustrated in the following figure, highlighting the key elements that contribute to value creation and organizational protection.

***Figure 3: Risk management framework according to ISO 31000:2018***




**Source:** (International Organization for Standardization (ISO), 2018).

Other frameworks provide complementary perspectives such as COSO ERM Framework that was updated in 2017 by the Committee of Sponsoring Organizations of the Treadway Commission, approaches risk through a governance and performance lens. Where ISO 31000 is process-oriented, COSO is strategy-oriented: it connects risk management directly to value creation, emphasizing the role of organizational culture, board-level accountability, and the alignment between risk appetite and strategic objectives (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017). Similarly, the Federation of European Risk Management Associations framework offers a more practical approach, particularly within the European context (Federation of European Risk Management Associations (FERMA), 2003).

Overall, while these frameworks differ in their orientation, they converge on the importance of a structured, integrated, and proactive approach to risk management.

To better highlight the differences and complementarities between these frameworks, the following table provides a comparative overview:

*Table 2: Comparison between ISO, COSO and FERMA*

| Aspect | ISO 31000:2018 | COSO ERM (2017) | FERMA Risk Management Standard |
|---|---|---|---|
| **Nature** | International standard | Enterprise risk management framework | European professional standard |
| **Objective** | Provide principles and guidelines for risk management | Integrate risk management with strategy and performance | Provide a practical and comprehensive approach to risk management |
| **Approach** | Principles-based, flexible and adaptable to all organizations | Structured and integrated with governance, strategy, and performance | Holistic and operational, focused on practical implementation |
| **Core Components** | Principles, Framework, Process | Governance & Culture, Strategy & Objective-Setting, Performance, Review & Revision, Information & Communication | Risk identification, assessment, response, monitoring, and communication |
| **Focus** | Applicability to any type of organization and context | Value creation, performance improvement, and organizational resilience | Enhancing risk awareness and supporting decision-making |
| **Integration Level** | Can be integrated into any management system | Strong integration with strategic planning and organizational performance | Focus on operational integration within processes |
| **Flexibility** | High flexibility and adaptability | Moderate flexibility with structured guidance | Flexible but less formalized than ISO and COSO |
| **Orientation** | Guidance-oriented (non-prescriptive) | Performance and governance-oriented | Practice-oriented and user-friendly |
| **Publication Year** | 2018 | 2017 | 2002 (updated versions available) |

**Source:** Elaborated by authors based on (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017; Federation of European Risk Management Associations (FERMA), 2003; International Organization for Standardization (ISO), 2018).

### 1.4. Enterprise Risk Management (ERM): an integrated process approach

Traditionally, risk management was carried out in a fragmented way, with each department managing its own risks independently. Financial, operational, and compliance risks were handled separately, which limited the overall visibility of risk exposure at the organizational level. Enterprise Risk Management (ERM) emerged as a response to these limitations, based on the idea that risks are interconnected and cannot be effectively managed in isolation (Basel Committee on Banking Supervision, 2005).

ERM redefines risk management as a global and integrated approach, aligned with the organization's strategic objectives. Instead of focusing on risks within individual functions, it considers all risks that may affect the achievement of organizational goals and analyzes their interdependencies. This approach requires a shared risk language, a consolidated view of risk at the leadership level, and the definition of a clear risk appetite. In this perspective, the Committee of Sponsoring Organizations of the Treadway Commission framework defines ERM as a set of practices integrated into strategy and performance, aimed at managing risk while creating value (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017).

Operationally, ERM is structured as a continuous process that includes risk identification, analysis, evaluation, treatment, and monitoring. Its main contribution lies not in the individual steps, but in their integration across the organization and their alignment with decision-making processes. In this context, the availability of reliable and timely information becomes essential, highlighting the role of information systems in supporting ERM implementation (International Organization for Standardization (ISO), 2018).

***Figure 4: COSO Enterprise Risk Management framework (2017)***


**Source:** (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017).

### 1.5. Risk typology

Effective risk management requires a clear understanding of the different types of risks an organization faces. In practice, the absence of a structured classification often leads to overlaps or gaps in risk identification. A risk typology helps address this issue by organizing risks into categories, facilitating analysis, communication, and decision-making (Hopkin, 2017).

Most frameworks distinguish several main categories of risk (Hopkin, 2017). Strategic risks affect long-term objectives, such as market changes or competitive pressures. Operational risks, defined by the Basel II framework as losses resulting from failures in processes, people, systems, or external events, relate to day-to-day activities. Financial risks involve exposure to market, credit, or liquidity fluctuations, while compliance risks concern legal and regulatory obligations.

In recent years, technological and information risks have become increasingly significant due to digital transformation. These include cybersecurity threats, system failures, and data breaches. Standards such as ISO/IEC 27005 provide specific guidance for managing these risks (International Organization for Standardization (ISO), 2018).

For organizations such as Ooredoo Algeria, technological risks are central to operational continuity and performance. Their growing importance justifies treating them as a distinct category and reinforces the need for dedicated information systems to support risk management.

### 1.6. Strategic importance in organizational governance

Risk management has progressively evolved from a reactive function to a central component of organizational governance. It is now recognized as a key element in supporting strategic decision-making and improving organizational performance (International Organization for Standardization (ISO), 2018).

The governance of risk is commonly structured around the Three Lines Model developed by the Institute of Internal Auditors (2020). In this model, operational management represents the first line, responsible for identifying and managing risks in daily activities. The second line, composed of risk and compliance functions, provides oversight and guidance, while internal audit forms the third line, ensuring independent assurance. This structure highlights that risk management is a shared responsibility across the organization. Its effectiveness largely depends on the quality of information flows between these levels, which reinforces the importance of information systems (Institute of Internal Auditors (IIA), 2020).

At the strategic level, the concept of risk appetite plays a central role. It allows organizations to define the level of risk they are willing to accept in order to achieve their objectives, ensuring alignment between risk-taking and strategic priorities (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017).

***Figure 5: Integration of risk into strategy and performance (COSO, 2017)***


**Source:** (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017).

Overall, risk management is no longer limited to a control function but has become a strategic capability that enhances organizational resilience. In this context, information systems are essential tools for collecting, analyzing, and communicating risk-related information to support informed decision-making.

## 2. Information Systems: Architecture, governance, and design

Modern information systems have evolved from simple administrative tools into complex architectures that serve as the backbone of strategic decision-making.

### 2.1. Origins and evolution of information systems: From data processing to strategic tools

The concept of information systems (IS) has evolved significantly over time, reflecting the transformation of organizational needs and technological capabilities. In the early stages of computing, information systems were primarily designed to automate repetitive administrative tasks such as accounting and payroll processing. These early systems, commonly referred to as data processing systems, were focused on improving operational efficiency, accuracy, and speed, without directly supporting managerial decision-making processes (Zachman, 2009).

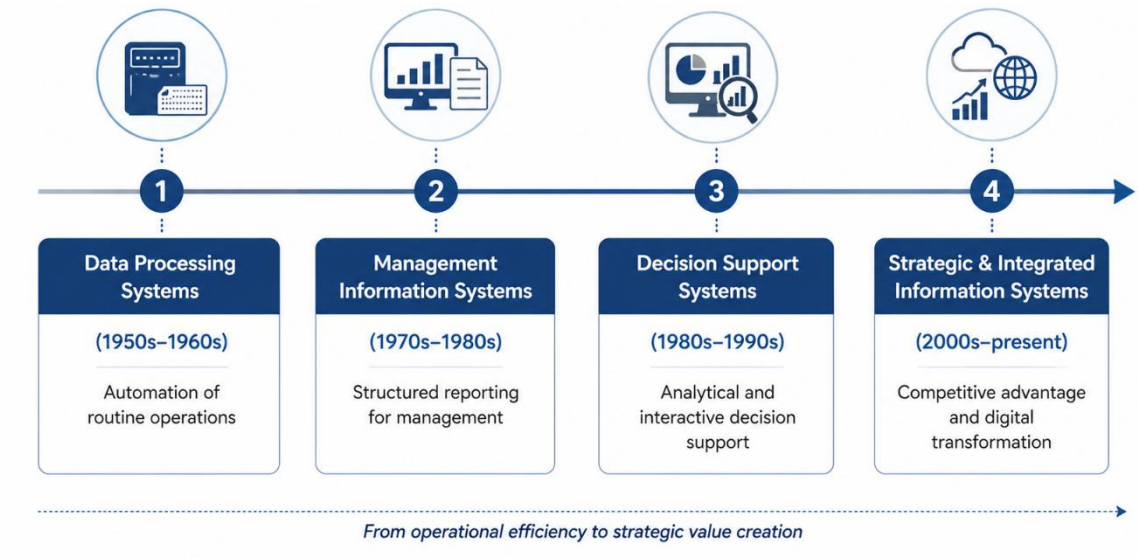
With the development of computing technologies in the 1970s and 1980s, information systems began to support management activities. This period saw the emergence of Management Information Systems (MIS), which provided structured reports to facilitate planning, control, and performance monitoring (Zachman, 2009).

Subsequently, the increasing complexity of decision-making environments led to the development of more advanced systems, such as Decision Support Systems (DSS). These systems introduced analytical models and interactive tools that allowed decision-makers to evaluate different scenarios and alternatives. This evolution reflects a shift from simple information provision to active decision support, where systems assist users in solving semi-structured and complex problems (Eltarabishi et al., 2020).

In recent decades, information systems have become fully integrated into organizational strategy and performance management. Modern IS are no longer limited to supporting operations or decisions; they play a central role in enabling digital transformation, improving organizational agility, and creating competitive advantage. As systems become larger and more complex, the need for structured architectures becomes essential to ensure coherence, integration, and alignment with business objectives (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017).

The following figure illustrates the evolution of information systems from operational tools to strategic decision-support systems.

***Figure 6: Evolution of Information Systems***




**Source:** Elaborated by authors.

### 2.2. Definition, Components, and Architectural Layers of an Information System

An Information System (IS) is an organized set of human, technical, and organizational resources designed to collect, process, store, and disseminate information in order to support operations and decision-making. It combines components such as hardware, software, databases, networks, and users, which interact to transform data into meaningful information (Zachman, 2009).

From a structural perspective, an information system is composed of several interdependent components, including hardware, software, databases, communication networks, and human actors. These elements interact continuously to ensure the circulation, processing, and reliability of information within the organization, thereby enabling efficient coordination of activities and informed decision-making (Zachman, 2009).

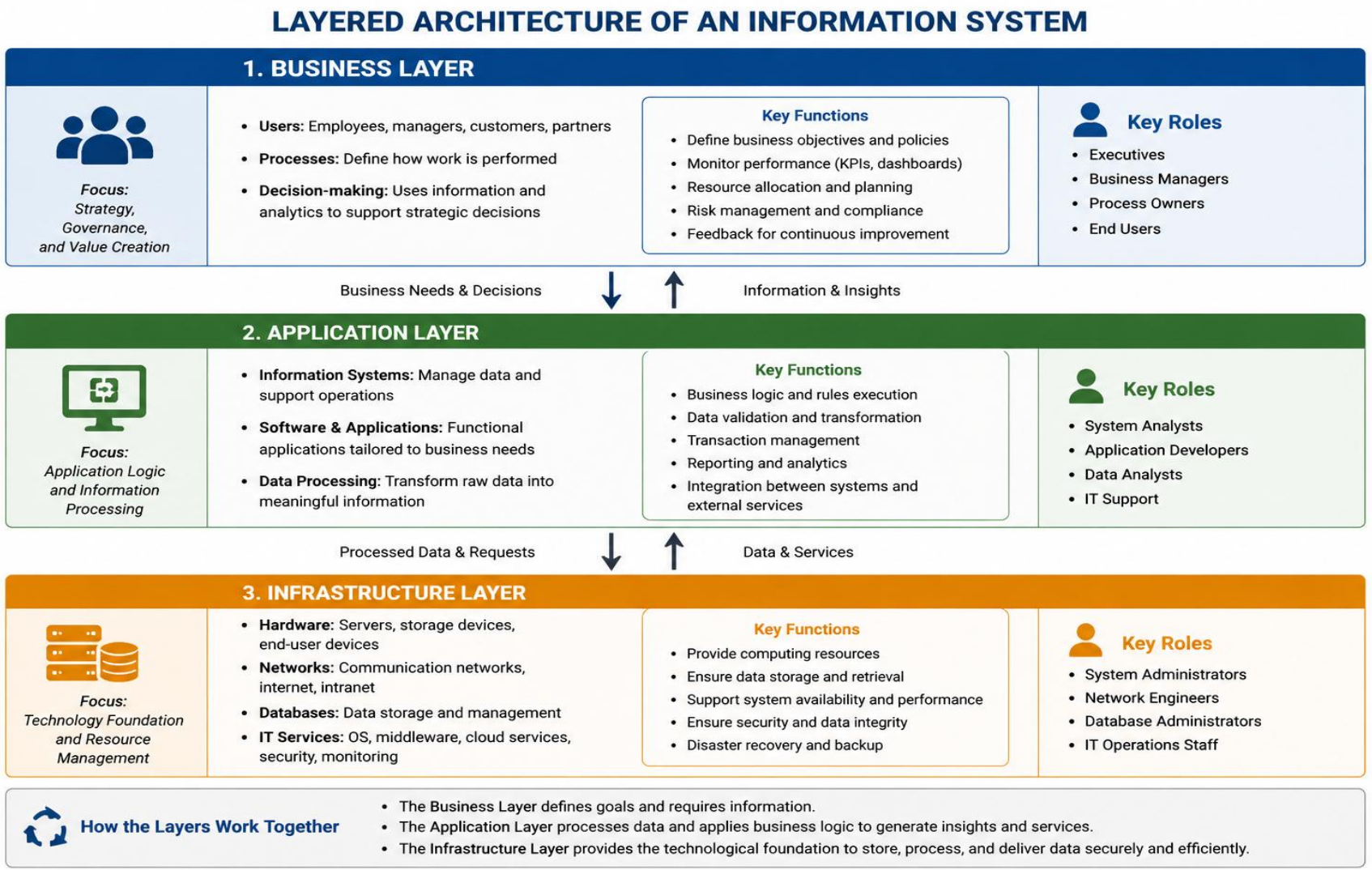
The organization and integration of these components are ensured through the concept of information system architecture, which provides a global and structured representation of the system. This architectural approach defines how different components are organized and interact, serving both as a design framework and as a reference for system evolution over time (Zachman, 2009).

Information system architecture is generally structured into multiple layers. The infrastructure layer includes physical and technical resources such as hardware and networks; the application layer encompasses software systems responsible for data processing; and the organizational layer integrates users and business processes. This layered structuring facilitates system coherence, scalability, and alignment with organizational objectives (Vasconcelos et al., 2003).

Furthermore, the increasing complexity of information systems has made the adoption of formal architectural frameworks essential. A structured architecture ensures integration and consistency across system components while preventing fragmentation and inefficiencies that may arise in decentralized environments (Zachman, 1987).

This layered structure is illustrated in the following figure:

*Figure 7: Layered architecture of an Information System*




**Source:** Elaborated by authors based on (Zachman, 1987, 2009).

### 2.3. IS governance, digital transformation, and strategic alignment

Modern Information System (IS) governance has transitioned from a strictly technical discipline into a high-level executive function. This shift is characterized by the role of the Chief Information Officer (CIO), who acts as a senior leader responsible for strategic planning and creating business alliances, rather than merely overseeing hardware operations (Zachman, 2009).

Strategic alignment serves as the primary mechanism for ensuring that technological investments translate into measurable organizational value. Within the context of digital transformation, the Information System Architecture (ISA) must act as a permanent reference point for all developments to prevent "non-alignment," where systems fail to answer the continuous and evolving demands of the business environment (Vasconcelos et al., 2003).

As organizations distribute computing resources across remote locations, the implementation of a formal IS architecture becomes a necessity to maintain order and control. Without such a logical construct to define and govern the interfaces between components, the decentralization brought about by digital transformation risks organizational disintegration and operational chaos (Zachman, 1987).

### 2.4. IS design methodologies: UML and BPMN in complementarity

Information systems design refers to the process of translating organizational requirements into a structured system architecture capable of supporting business processes and decision-making activities. It aims to ensure alignment between organizational objectives, user needs, and technological solutions by defining system functionalities, information flows, and interactions among stakeholders.

Information systems modeling is the process of creating abstract representations of a system in order to analyze, communicate, and specify its structure and behavior. Through graphical models, stakeholders can visualize processes, actors, data, and interactions, thereby facilitating system understanding and reducing design complexity.

Conceptual modeling methodologies provide a vital communication bridge between the technical requirements of system developers and the functional needs of business users. By employing graphical models early in the design process, organizations can minimize

structural design errors and ensure the system remains focused on the real-world domain it was built to support (Recker et al., 2009).

The Unified Modeling Language (UML) is a foundational industry standard that utilizes an object-oriented approach to maintain modeling integrity. It reduces the gap between business strategy and IT implementation by providing a consistent framework for depicting business resources, processes, and goals (Vasconcelos et al., 2003).

While UML is highly effective for structural and behavioral specifications, the Business Process Modeling Notation (BPMN) offers a complementary focus on activity-centric documentation. BPMN includes a specialized vocabulary for messaging and transaction management, allowing for a level of detail in transactional processes that often exceeds the semantic capabilities of standard UML activity diagrams (Recker et al., 2009).

A comparative synthesis of UML and BPMN is presented in the following table to emphasize their respective roles in information system design:

***Table 3: Comparison between UML and BPMN***

| Aspect | UML | BPMN |
|---|---|---|
| **Nature** | Object-oriented modeling language | Business process modeling notation |
| **Objective** | Model system structure and behavior | Model and analyze business processes |
| **Approach** | Object-oriented approach | Activity and process-oriented |
| **Focus** | Structural and behavioral representation | Workflow, interactions, and transactions |
| **Strengths** | Standardized, widely used, versatile | High readability for business users, detailed process flows |
| **Limitations** | Less detailed for business processes | Less focus on data and system structure |
| **Best Use** | System analysis and software design | Process modeling, analysis, and optimization |

**Source:** Elaborated by authors.

## 2.5. Functional and technical architecture of a management IS: quality and performance criteria

To achieve high performance, a management information system must satisfy rigorous quality characteristics, which include functionality, reliability, usability, efficiency, and maintainability, all of which are necessary for a software product to maximize its benefit to the organization (Hanine et al., 2016).

The technical architecture serves as a high-level "blueprint" that integrates the organization's informational needs with its physical hardware and software applications. This construction process is cyclical and must be driven by the business architecture, which describes the long-term vision and objectives of the enterprise (Zachman, 1987).

A robust architectural framework must explicitly differentiate between different descriptive perspectives, such as "what" (data), "how" (process), and "where" (network). This ensures that every stakeholder, from the executive owner to the technical builder, has a precise and actionable view of how the system's components are integrated (Zachman, 1987).

## 2.6. Towards an integrated IS design approach for risk management

An integrated design approach shifts risk management from being an isolated technical exercise to a process embedded directly within organizational strategy and performance monitoring. This alignment allows leaders to identify how shifts in the risk landscape can be managed as strategic opportunities rather than just threats (Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017).

The integration of risk management into the information system is often operationalized through Governance, Risk, and Compliance (GRC) software products. These tools allow for the normalization and aggregation of data from disparate business units into a centralized Cybersecurity Risk Register (CSRR), providing a composite view that enables executives to adjust strategies based on real-time information.

Finally, the design of a Risk Management Information System (RMIS) benefits from the inclusion of Multi-Criteria Decision-Making (MCDM) methods to manage the inherent complexity of risk assessment. These mathematical techniques empower decision-makers to evaluate conflicting variables and uncertainties systematically, leading to prioritized and rational risk treatment plans (Taherdoost & Madanchian, 2023).

# 3. Multi-criteria risk assessment

The evolution of risk assessment relies on multi-dimensional mapping techniques that transform qualitative expert judgment into structured, actionable insights.

## 3.1. Concept and objectives of risk mapping

Risk mapping refers to the structured process of identifying, analyzing, and representing risks in order to support decision-making and prioritization. It is a central component of the risk assessment process defined in ISO 31000, where risk evaluation aims to compare analyzed risks against predefined criteria to determine their significance (International Organization for Standardization (ISO), 2018).

Risk mapping is an analytical process used to identify and communicate the relative priority of various threats. The objective is to produce a consolidated visual summary, such as a heat map, that represents the likelihood and impact of uncertainties on enterprise goals. These maps allow senior leaders to differentiate between "red-hot" risks requiring immediate response and those falling within acceptable tolerance levels. Prioritization within these maps considers each uncertainty not just as a technical loss but as an "effect of uncertainty on objectives" (Quinn et al., 2022).

Traditionally, risk assessment relies on probability-impact matrices; however, such approaches remain limited when risks involve multiple dimensions (financial, operational, strategic, and technological). In this context, multi-criteria approaches extend risk mapping by integrating several evaluation criteria simultaneously, allowing for a more comprehensive representation of risk exposure.

The main objectives of risk assessment are the following:

- To identify and classify risks across the organization
- To evaluate their criticality using consistent criteria
- To support prioritization and decision-making
- To provide a global view of risk exposure

## 3.2. Principles of multi-criteria analysis in decision-making

Multi-Criteria Decision-Making (MCDM) is a branch of operations research designed to resolve complex problems involving conflicting criteria. These principles provide a structured decision aid that empowers organizations to make rational, well-considered choices in environments where human analytical capacity is overwhelmed by data volume (Caylor & Hanratty, 2020). Decisions are made by grouping alternatives into preference sets

and identifying non-dominated solutions, where one criteria cannot be improved without sacrificing another (Taherdoost & Madanchian, 2023).

### 3.3. Multi-criteria methods applied to risk assessment (AHP, ELECTRE, TOPSIS)

Several multi-criteria methods are commonly applied to risk assessment, each offering a specific analytical approach.

The Analytic Hierarchy Process (AHP) is based on a hierarchical structuring of the decision problem, where criteria and sub-criteria are organized into levels. It uses pairwise comparisons to determine the relative importance of criteria and calculate their weights. This method is particularly suitable for incorporating expert judgment in risk evaluation (Hanine et al., 2016).

The ELECTRE method is based on an outranking approach, where alternatives are compared pairwise to determine dominance relationships. It is particularly effective in situations involving conflicting criteria and complex decision environments (Hanine et al., 2016).

The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) ranks alternatives based on their distance from an ideal solution and an anti-ideal solution. The preferred alternative is the one that is closest to the ideal solution while being farthest from the worst-case scenario (Hanine et al., 2016).

In practice, these methods are often combined to form hybrid models, improving the robustness and reliability of the evaluation process. Such hybrid approaches are increasingly used in real-world applications due to their ability to handle complex and multidimensional decision problems (Eltarabishi et al., 2020).

A comparative overview of the main multi-criteria methods is presented below:

*Figure 8: Comparative overview of AHP, ELECTRE, and TOPSIS methods*

| Aspect | AHP (Analytic Hierarchy Process) | ELECTRE (Elimination and Choice Expressing Reality) | TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) |
|---|---|---|---|
| Approach | Hierarchical decomposition of the decision problem | Outranking relations (pairwise comparison) | Distance to ideal solution (best vs worst alternative) |
| Logic | Pairwise comparisons between criteria and alternatives to derive priority weights | Dominance and concordance / discordance analysis to establish outranking relations | Closeness of each alternative to the ideal (best) and anti-ideal (worst) solutions |
| Main Steps (Overview) | 1. Structure the hierarchy → 2. Pairwise comparisons → 3. Compute weights → 4. Rank alternatives | 1. Decision matrix → 2. Concordance / Discordance matrices → 3. Outranking relations → 4. Rank / Classify | 1. Decision matrix → 2. Normalize matrix → 3. Ideal & anti-ideal solutions → 4. Compute closeness → 5. Rank alternatives |
| Output | Criteria weights and priority ranking of alternatives | Partial or complete ranking of alternatives based on dominance relations | Ranking of alternatives based on relative closeness to the ideal solution |
| Advantages | • Easy to understand and implement<br>• Integrates expert judgment<br>• Provides consistency check | • Handles conflicting criteria well<br>• Does not require compensatory trade-offs | • Simple and intuitive<br>• Computationally efficient<br>• Provides clear ranking |
| Limitations | • Subjectivity in judgments<br>• Many comparisons can be time-consuming<br>• Consistency issues possible | • Complex to implement<br>• Requires parameter setting<br>• May produce partial rankings | • Sensitive to normalization method<br>• Compensatory (may hide weak performances) |
| Typical Use in Risk Management | • Structuring risk evaluation<br>• Weighting risk criteria<br>• Prioritizing risks | • Complex risk environments<br>• Conflicting or non-compensatory criteria<br>• Risk classification | • Ranking risks<br>• Selecting critical risks for treatment<br>• Comparing risk scenarios |

**Source:** Elaborated by the authors based on (Eltarabishi et al., 2020; Hanine et al., 2016; Taherdoost & Madanchian, 2023).

### 3.4. Contributions of multi-criteria mapping to risk prioritization

The application of multi-criteria approaches significantly enhances the process of risk prioritization. Unlike traditional methods based solely on probability and impact, multi-criteria assessment incorporates additional dimensions, allowing for a more refined and accurate evaluation of risks.

By integrating multiple criteria, this approach enables a better differentiation between risks with similar characteristics and supports a more objective ranking process. It also improves transparency by providing a structured and traceable evaluation framework.

In complex environments, prioritizing risks requires considering various interdependent factors. Multi-criteria methods facilitate this process by enabling systematic comparisons and supporting consistent decision-making (Caylor & Hanratty, 2020).

Furthermore, structured prioritization mechanisms are essential within enterprise risk management frameworks, as they allow organizations to allocate resources effectively and focus on the most critical risks (Quinn et al., 2022).

### 3.5. Limitations and conditions of application

Despite its advantages, multi-criteria risk mapping presents several limitations. One of the main challenges lies in the subjectivity associated with the weighting of criteria, which may vary depending on expert judgment. In addition, the implementation of MCDM methods can be complex and requires a solid methodological framework.

Another limitation is that different methods may produce different results for the same problem, making the selection of the appropriate method a critical step in the decision-making process (Eltarabishi et al., 2020).

To ensure effective application, several conditions must be met. These include the clear definition of evaluation criteria, the availability of reliable and relevant data, and the involvement of domain experts. Moreover, the chosen method must be adapted to the specific context of the decision problem.

### 3.6. Integration of multi-criteria risk assessment into an information system

The integration of multi-criteria risk assessment into an information system, particularly within a Risk Management Information System (RMIS), represents a key evolution in risk management practices.

Information systems enable the centralization of risk data, facilitate real-time evaluation, and support decision-making through analytical tools and dashboards. By embedding multi-criteria models into these systems, organizations can automate the risk assessment process and improve the consistency and reliability of evaluations.

In addition, decision-support systems increasingly rely on MCDM methods to enhance their analytical capabilities and address complex decision-making problems (Więckowski et al., 2023).

From an architectural perspective, integrating such models into information systems ensures better alignment between business processes and decision-support tools, thereby improving organizational performance and responsiveness (Vasconcelos et al., 2003).

# Chapter II: Methodological framework and host organization

This chapter presents the methodological framework adopted to address the research problem related to the design of a Risk Management Information System within Ooredoo Algeria. It explains the main methodological choices, based on a qualitative approach and an abductive logic, ensuring coherence between the research objectives and the field study.

The first section outlines the epistemological positioning, the research approach, and the methods used for data collection and analysis, including interviews, observation, and documentary review, as well as the selection of participants and the limits of the study.

The second section introduces Ooredoo Algeria, its strategic positioning, organizational structure, and the role of the risk management department. It also presents the existing practices and highlights the gaps that justify the design of the RMIS.

## Section 1: Methodological framework

This section presents the methodological framework of the research. It outlines the epistemological positioning, the abductive approach adopted, and the main stages of designing and validating the RMIS It also describes the data collection methods employed, the criteria governing participant selection, and the techniques used for data analysis. Finally, it highlights the study's limitations and the measures taken to ensure its rigor.

### 1. Epistemological positioning

The epistemological positioning frames the way the research problem is understood and analyzed, providing a coherent foundation for the selection of the research approach and methods.

#### 1.1. Constructivist and pragmatic rooting

Epistemology refers to the theory of knowledge, concerned with how knowledge is constructed, validated, and interpreted. It examines the processes through which individuals understand reality and justify their beliefs. According to research methodology literature, epistemology seeks to answer the question of how we know what we know and how knowledge is generated within a given context (Marín García, 2023).

In research methodology, epistemological positioning is commonly structured around three main paradigms: positivism, interpretivism, and constructivism. Positivism is grounded in an objectivist epistemology, assuming that reality exists independently of the researcher and can be understood through empirical observation, measurement, and the identification of causal relationships. Knowledge is therefore considered valid when it is

based on observable and verifiable evidence, following a deductive logic and aiming at generalization (Ali, 2024).

In contrast, interpretivism is based on a subjectivist perspective, according to which reality is socially constructed and cannot be understood independently of the meanings that individuals attribute to it. This paradigm emphasizes the importance of context, human experience, and interpretation, arguing that knowledge is produced through interaction between the researcher and the studied phenomenon (Pham, 2018; Ryan, 2018).

Finally, constructivism extends the interpretivist perspective by emphasizing that knowledge is co-constructed through social interactions and individual experiences. It rejects the idea of a single objective reality and instead considers multiple realities shaped by actors' perceptions, contexts, and interactions. This approach highlights the active role of the researcher in the construction and interpretation of knowledge (Yong et al., 2021).

The question of scientific knowledge—how knowledge is produced—is at the heart of all research in management sciences. This study falls within a predominantly constructivist epistemological paradigm, complemented by a pragmatic sensitivity, which constitutes a posture particularly suited to the design of an organizational artifact such as a Risk Management Information System (RMIS).

This epistemological choice is primarily justified by the nature of the research subject, namely the design and modeling of a risk management information system, which requires both an interpretative and constructive approach:

- The study is centered on the design of an RMIS, which goes beyond mere observation and requires the construction of a structured and functional solution.
- Risk management does not rely on a fully objective and fixed reality but on perceptions, interpretations, and judgments formulated by organizational actors.
- Risk identification and evaluation are strongly influenced by the organizational context, including roles, practices, and internal dynamics.
- Within a RMIS, information is context-dependent, as it is produced and interpreted within specific organizational processes and governance structures.
- The research aims to develop a concrete and usable artifact (RMIS), which justifies the integration of a pragmatic orientation focused on applicability.

The combination of constructivism and pragmatism is particularly relevant in the context of this research. Constructivism enables a deeper understanding of the complex and subjective nature of risk, shaped by the perceptions and interactions of organizational actors.

On the other hand, pragmatism allows this understanding to be translated into the design of a concrete and operational solution. In this regard, the proposed RMIS is not only grounded in the analysis of organizational realities but is also conceived as a functional tool aimed at supporting risk management practices and decision-making processes. This dual positioning ensures both the analytical relevance of the study and the practical applicability of its outcomes.

### 1.2. Researcher posture in the field

This research adopts a researcher-designer posture, reflecting a dual orientation combining a theoretical dimension, through the mobilization of conceptual frameworks, and a practical dimension, through engagement with the organizational context of Ooredoo Algeria. Within this framework, the study is conducted from a researcher-practitioner perspective.

Access to the organization was organized through a combination of guided on-site interactions, semi-structured interviews, remote exchanges, and documentary consultation. This configuration enabled the collection of diversified data while ensuring a structured understanding of the observed practices.

A structured observation grid was developed to support the observation process and ensure consistency in data collection (see observation grid, appendix B).

The grid includes structured criteria relating to risk identification, reporting practices, stakeholder roles, communication mechanisms, and supporting tools.

This tool made it possible to systematically capture key elements related to risk management practices, including processes, actors, tools, and information flows.

To ensure the rigor of the analysis and limit potential bias, methodological triangulation was applied by cross-referencing data from interviews, direct observation, and documentary sources.

## 2. Adopted research approach

Our approach follows a structured process to ensure the final model meets both academic standards and real-world needs.

### 2.1. Abductive logic: Between exploration and modeling

Our research is based on an abductive logic positioned between deduction and induction. Abduction involves generating provisional explanatory hypotheses from observed empirical

issues, which are then progressively refined through confrontation with theoretical frameworks and field data.

In this study, the abductive logic is particularly relevant as the objective is both to understand current risk management practices within Ooredoo Algeria and to design a Risk Management Information System (RMIS) adapted to the organizational context, particularly ISO 31000:2018. The research is therefore grounded in a pragmatic perspective, which emphasizes the production of useful and actionable knowledge rather than purely theoretical explanations. As highlighted in the literature, pragmatism focuses on generating knowledge that is applicable to real-world problems and supports decision-making processes (Hofmann et al., 2024).

### 2.2. Methodological process: From problem identification to RMIS evaluation

The following steps present the methodological process adopted to design, model, and evaluate the proposed Risk Management Information System.

- **Step 1: Problem identification:** The first stage consists in analyzing existing risk management practices at Ooredoo Algeria in order to identify limitations, gaps, and unmet needs within the current system.
- **Step 2: Field exploration and data collection:** Empirical data is collected through semi-structured interviews and direct observation of stakeholders involved in risk management activities in order to capture practices, expectations, and contextual constraints.
- **Step 3: Requirements elicitation and analysis:** The collected qualitative data is processed through thematic analysis to extract and formalize both functional and organizational requirements for the RMIS.
- **Step 4: Design and modeling:** Based on the identified requirements, the RMIS is designed and structured using UML diagrams including use case, class, and sequence diagrams to represent its conceptual architecture.
- **Step 5: Evaluation against reference framework:** The proposed model is assessed for coherence, completeness, and relevance with respect to ISO 31000:2018 principles and the requirements derived from the field study.
- **Step 6: Communication and formalization:** Research outcomes, design choices, and operational recommendations are synthesized and formalized, constituting the scientific and practical contribution of the study.

## 3. Data collection methods

To ensure the reliability of our findings, this research employs a multi-method approach consisting of interviews, direct observation, and documentary analysis.

### 3.1. Semi-structured interviews

The primary data collection method consists of semi-structured interviews conducted with four participants selected from key organizational functions interacting with Enterprise Risk Management (ERM). Semi-structured interviews were chosen because they combine the consistency of a predefined interview guide with the flexibility necessary to explore emergent themes and unexpected insights specific to each participant's experience.

The interview guide was organized around four axes: current risk management practices, the limits of the existing ERM framework, methods of risk assessment and prioritization, and expectations regarding a future RMIS. It was conducted through semi-structured interviews with risk managers and selected staff involved in these processes. This format ensured a common structure while allowing participants to elaborate on their experience. All interviews were carried out in a confidential setting, with prior consent obtained for recording or note-taking.

The interview guide was specifically developed for this research *(see Appendix A)*. It is intended to structure data collection while ensuring alignment with the research objectives. The guide comprises a total of 20 questions, organized into four main axes:

- **Axis 1: Overview of risk Management Practices (5 questions):** aimed at understanding how risk management is currently organized, including stakeholders involved, types of risks, tools used, and reporting practices.
- **Axis 2: Assessment of the ERM framework's limitations (5 questions):** focused on identifying existing challenges, gaps in information, coordination issues, and inefficiencies in current processes.
- **Axis 3: Risk assessment and prioritization (5 questions):** intended to explore the criteria, methods, and tools used to evaluate, rank, and map risks within the organization.
- **Axis 4: Target vision for a RMIS (5 questions):** aimed at identifying expectations regarding system functionalities, decision-support needs, integration requirements, and potential organizational impacts.

The interviews were conducted following a semi-structured format, ensuring consistency across discussions while allowing participants to elaborate on their experiences. Each

interview began with a presentation of the research objectives and confidentiality assurances, followed by a guided discussion based on the four axes of the interview framework. All interviews were conducted face-to-face.

Data collection was carried out through detailed note-taking or audio recording (when authorized), ensuring the accuracy and completeness of the collected information. Prior consent was systematically obtained from all participants, in accordance with ethical research standards.

A summary of the interview process is presented in the table below:

***Table 4: Summary of interviewees and conditions of semi-structured interviews***

| Interviewee | Function | Years of Experience (ERM) | Duration | Method | Recording |
|---|---|---|---|---|---|
| Interviewee 1 | ERM manager | 9 years | 40 min | Face-to-face | Notes |
| Interviewee 2 | Risk management specialist | 3 years | 50 min | Face-to-face | Notes |
| Interviewee 3 | Risk & compliance procurement | 1.5 year | 70 min | Face-to-face | Audio recording |
| Interviewee 4 | Head of regulatory affairs | 8 years | 35 min | Face-to-face | Notes |

**Source:** Elaborated by the authors.

### 3.2. Direct observation

As a complementary method, direct observation was conducted during guided visits to Ooredoo Algeria's operational environment. This approach aims to capture risk management practices as they are effectively implemented in daily organizational activities, beyond formalized procedures and declared practices. It allows for the identification of potential discrepancies between prescribed processes and actual practices within the organization.

To ensure a structured and consistent observation process, a detailed observation grid was specifically developed for this research. This grid was designed based on key phases of the risk management process, in alignment with the principles of ISO 31000:2018 and internal ERM practices. It is structured around several categories, including risk identification, assessment, mapping, monitoring, reporting and communication, incident

management, documentation and data management, regulatory compliance, and information systems integration.

For each category, the grid includes three main dimensions: observed practices, identified gaps or limitations, and an overall synthesis. This structure enables a systematic analysis of organizational practices, facilitating the identification of strengths, operational constraints, and areas for improvement.

The use of this observation tool contributes to enhancing the reliability of the collected data and supports methodological triangulation when combined with interviews and documentary analysis.

The results of the direct observation are presented in an observation grid (see Appendix B).

### 3.3. Documentary analysis

Documentary analysis is employed as a triangulation method to contextualize and validate the primary data. In a context where internal policy documents and specific ERM protocols are treated as strictly confidential, this analysis relies on accessible administrative artifacts and standardized reporting templates. These elements provide the necessary framework to understand the formal structure and the reporting constraints imposed on the organization’s risk management activities.

With regard to international reference frameworks, the analysis focuses exclusively on the operational application of ISO 31000:2018 within the organizational context. Since detailed internal risk policies are inaccessible for direct citation, the standard serves as the primary evaluative lens to assess the maturity of the existing Enterprise Risk Management (ERM) system. This approach makes it possible to systematically compare observable field practices such as risk identification techniques and monitoring frequencies against the standard's process components (scope, context, criteria; risk assessment; and risk treatment).

This comparison identifies the degree of alignment between current operations and international best practices, highlighting areas where operational implementation remains limited or diverges from the standard’s principles. By focusing on these functional intersections, the documentary analysis contributes to a robust understanding of the organizational environment while providing a credible basis for interpreting data collected during the field study. This approach strengthens the analytical framework of the study and supports the design of the proposed RMIS by linking normative references to observed practices within the organization.

## 4. Sampling and participant selection

The selection of participants is based on a logic of relevance rather than statistical representativeness, consistent with a qualitative approach (Creswell, 2014). A purposive sampling method was used, focusing on individuals directly involved in risk management and working in key areas. This includes Business Unit representatives and risk champions, who offer insights from different departments and contribute to a broader understanding of how risks are managed across the organization.

The sample includes four participants, which is considered sufficient given the specific scope of the study. As future users of the RMIS, their perspectives help identify practical needs, system requirements, and possible constraints. Their diversity also reflects the transversal nature of the system and supports the development of a solution that can be used across the organization.

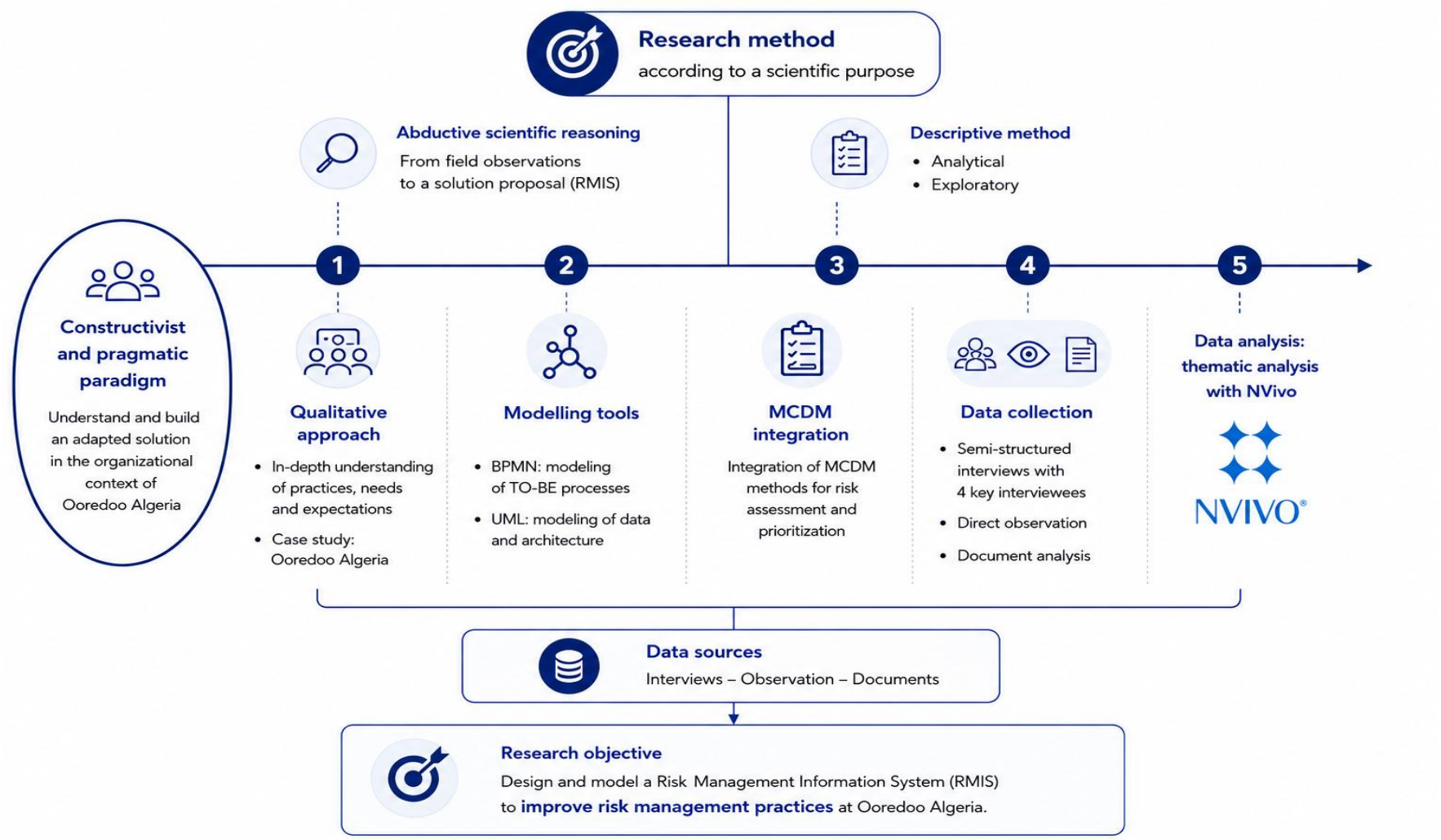
Ethical considerations were respected throughout the process. Participants were informed about the purpose of the study, and their consent was obtained before the interviews.

## 5. Research limits and validity

This study presents certain limitations that should be acknowledged. First, access to data remains constrained due to the confidential nature of the telecommunications sector, which restricts the availability of sensitive strategic information. Second, the research is conducted within the limited timeframe of a master's thesis and therefore reflects a "snapshot" of practices at a given moment rather than their evolution over time. To mitigate these limitations and strengthen the validity of the findings, several measures are adopted, including data triangulation, the use of a reflexive logbook throughout the research process, and member checking, whereby the interpretations are submitted to participants to ensure their accuracy and consistency with the empirical reality.

An overview of the research methodology is presented in the figure below:

*Figure 9: Methodological framework of the study*




**Source:** Elaborated by authors.

## Section 2: Presentation of Ooredoo Algeria

This section describes Ooredoo Algeria's organizational framework and the current processes that justify the transition toward a centralized risk management system.

### 1. History and evolution

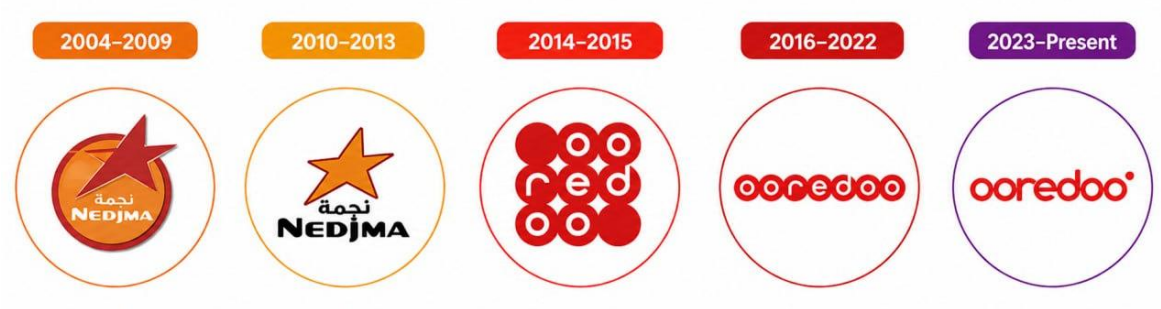
Understanding Ooredoo Algeria's growth and rebranding provides the necessary context for its current digital and risk management strategies.

#### 1.1. Ooredoo Algeria: Market context and rebranding

Ooredoo Algeria is one of the three companies operating in the Algerian mobile telephony market, alongside Algérie Télécom (via its subsidiary Mobilis) and Optimum Telecom Algérie (formerly Djezzy). Its history in Algeria is inseparable from the opening of the telecommunications market to competition, which occurred in the early 2000s as part of the sector's liberalization initiated by Law No. 2000-03 of August 5, 2000, relating to post and telecommunications.

The company was founded in 2003 under the name Wataniya Telecom Algérie (WTA), following the awarding of a GSM mobile telephony license by the Regulatory Authority for Post and Electronic Communications (ARPCE). After operating under the commercial name Nedjma, which established itself as a strong brand in the Algerian market, the company adopted the Ooredoo identity in 2013. This was consistent with the global rebranding strategy of the Ooredoo Group Q.P.S.C., headquartered in Qatar.

***Figure 10: Ooredoo Algeria's visual identity evolution***




**Source:** Elaborated by the authors.

With over thirteen million subscribers recorded in recent years, Ooredoo Algeria holds a significant position in the Algerian telecommunications market, distinguished by its continuous investments in network infrastructure and its positioning in the data and 5G segments. The company maintains a nationwide presence with a commercial network of several hundred branches and authorized points of sale.

### 1.2. Current digital and strategic orientations

Ooredoo Algeria's strategy aligns with the Ooredoo Group’s vision to become a leading digital operator in its emerging markets. In Algeria, this vision translates into several major strategic orientations: accelerating for 5G; developing value-added services (mobile banking, digital content, B2B solutions); internal digital transformation of business processes; and strengthening regulatory compliance and risk management.

This final orientation is particularly structural to our research: intensifying competition, a more complex regulatory environment, and increasing cyber threats have led Ooredoo Algeria to place risk management at the heart of its strategic priorities. This fully justifies the development of an RMIS (Risk Management Information System) tailored to its organizational and sectoral specificities.

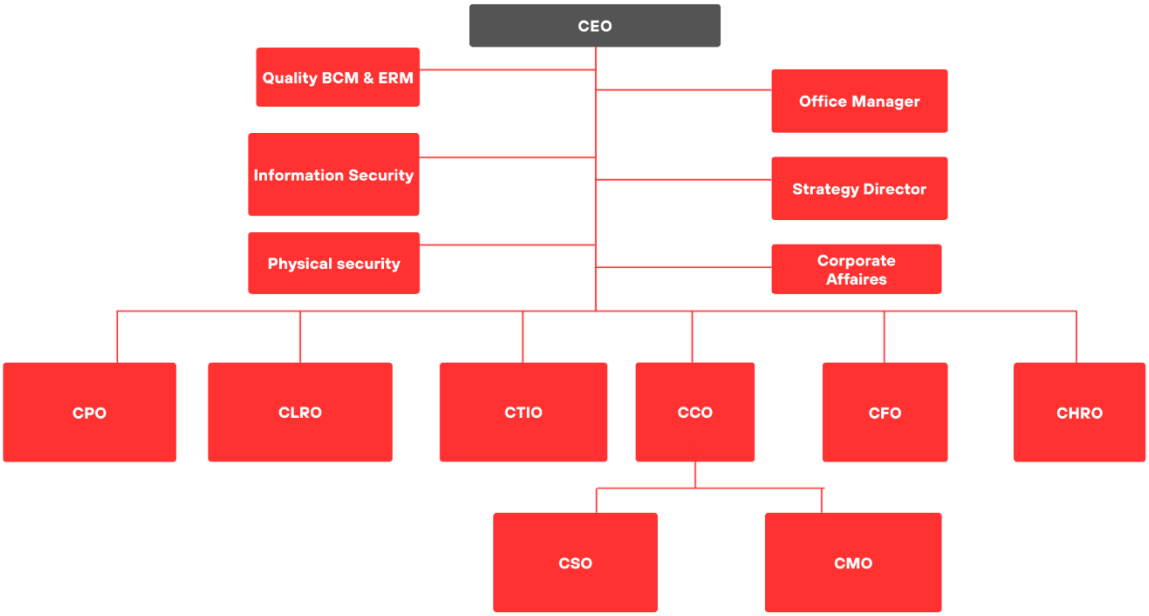
## 2. Organizational structure

The company's internal structure is designed to facilitate coordination between specialized departments and executive leadership.

### 2.1. General company organization

Ooredoo Algeria adopts a functional and organizational structure, typical of large telecommunications companies operating in complex, multidimensional environments. This structure is divided into several main functional departments under the authority of general management.

*Figure 11: The general organizational chart of Ooredoo Algeria*




**Source:** Elaborated by authors based on internal documents.

*Within this organizational structure, the ERM department directly supports the CEO. Risk management activities are primarily embedded within the "Quality, BCM & ERM" function, which operates in close interaction with top management and various operational and support departments. This positioning reflects the transversal nature of risk management, requiring coordination across functions such as Information Systems, Finance, Legal, and Operations. In this context, the proposed Risk Management Information System (RMIS) is intended to support these interactions by facilitating the collection, consolidation, and analysis of risk-related information across all departments, thereby strengthening decision-making processes at the organizational level.*

### 2.2. Reporting line: risk management to general management

A particularly relevant organizational element for our study is the direct reporting line from the Risk Management Department to Top Management. This hierarchical positioning, consistent with international best practices in risk governance (**ISO 31000:2018**), reflects Ooredoo Algeria's commitment to placing risk management at a high strategic level, ensuring functional independence from operational departments.

## 3. The risk management department: Role and missions

The Risk Management Department operates through a series of core missions designed to protect the organization's overall stability.

### 3.1. Scope of intervention and responsibilities

The risk management department at Ooredoo Algeria serves as the central architect of organizational resilience. Its mandate is to design, implement, and steer a global Enterprise Risk Management (ERM) framework that aligns with the ISO 31000:2018 standard.
The department's responsibilities are structured around the core stages of the ISO process:

- **Framework design:** Defining the "risk language," appetite, and tolerance levels to ensure all Business Units align with the company's strategic vision.
- **Risk assessment**: Leading the proactive identification of emerging threats and conducting a multi-criteria analysis to prioritize risks based on their operational and financial impact.
- **Risk treatment:** Collaborating with "Risk Owners" to design mitigation strategies and ensuring that action plans are effectively executed to reduce exposure.
- **Monitoring & communication:** Maintaining continuous oversight through periodic reviews and transforming complex data into consolidated reports for General Management.

By operationalizing these stages, the department ensures that risk management is a dynamic, continuous cycle that directly supports Ooredoo's strategic decision-making.

### 3.2. Coordination with other departments

Effective risk management is inherently transversal and depends on continuous coordination between the Risk Management Department and the organization's key functional and control entities. This coordination ensures a comprehensive identification, assessment, and monitoring of risks across all levels of the company.

First, close interaction with operational business units—namely CTIO, CPO, CCO, HR, and CFO—is essential. These entities represent the primary sources of key risk informations and provide critical operational data required for risk identification and evaluation.

Second, collaboration with specialized control functions, including Internal Control (ICFR), Health, Safety and Environment (HSE), Information Security, Personal Data Protection (DPO), Fraud Management and Business Assurance, and Business Continuity

Management, strengthens the overall control environment. These units contribute to risk mitigation through dedicated frameworks, compliance mechanisms, and monitoring processes.

Finally, coordination with executive management and governance bodies—such as the risk committee, internal audit, group ERM, and the board audit and risk committee—ensures strategic alignment and effective oversight. This interaction supports informed decision-making and reinforces accountability in risk governance.

### 3.3. Decision support for general management

Beyond its operational activities, the risk management department fulfills a strategic decision-support role within the organization. It produces periodic reports—on a quarterly basis or upon request—providing a structured and consolidated view of the organization's risk profile.

These reports incorporate an assessment of risk appetite, defined as the level of risk that Ooredoo Algeria is willing to accept in pursuit of its strategic objectives, in accordance with internal frameworks. This dimension ensures alignment between risk exposure and strategic priorities.

In this perspective, the proposed Risk Management Information System (RMIS) aims to automate the collection and consolidation of risk-related data, while enabling real-time reporting and enhanced visibility for top management. Such a system is expected to strengthen the responsiveness and effectiveness of strategic decision-making.

## 4. Technological environment and risk management practices

A set of clear objectives guides the Risk Management Department in its efforts to protect the organization's strategic goals.

### 4.1. Existing tools and infrastructure

The existing technological environment is characterized by the coexistence of heterogeneous legacy systems and specialized business applications. In the field of risk management, current practices rely primarily on standard office tools—such as Microsoft Excel and Microsoft PowerPoint & Outlook—for risk mapping, monitoring, and reporting activities.

Although this configuration remains operational, it presents several structural limitations. Data are collected across non-integrated systems, which hinders consolidation and reduces overall data reliability. In addition, the absence of real-time visibility limits the capacity for timely decision-making. The strong dependence on manual tools for critical processes increases the risk of errors and reduces efficiency. Finally, the lack of integrated traceability mechanisms makes it difficult to monitor the historical evolution of risks and the effectiveness of implemented treatment actions.

### 4.2. Current reporting and monitoring processes

The current reporting and monitoring processes are structured around periodic data collection cycles, primarily conducted through email exchanges and coordination meetings. These practices enable the circulation of information between stakeholders but remain largely manual and decentralized.

Such an approach presents several limitations. Time lags may arise between the occurrence of risk events and their reporting, reducing the timeliness of managerial responses. In addition, the reliance on informal communication channels complicates the traceability of decisions and follow-up actions. Finally, the aggregation of heterogeneous data from multiple sources remains complex, limiting the ability to produce a consolidated and coherent view of risks at the organizational level.

### 4.3. Identification of gaps justifying the RMIS design

The analysis of current practices reveals limitations in the structuring and accessibility of risk-related information. In particular, the absence of a centralized and shared risk repository leads to data dispersion across multiple tools and departments, affecting consistency and complicating access to reliable and up-to-date information. This fragmentation limits the establishment of a unified view of the organization’s risk exposure.

In addition, the lack of automated alert mechanisms for critical risk thresholds constrains the efficiency and standardization of monitoring processes. Risk tracking relies on manual consolidation and communication practices, which may affect the timeliness of information flows and the consistency of follow-up across risk categories.

These limitations justify the implementation of an integrated RMIS capable of centralizing data and supporting more structured and reliable reporting.

# Chapter III: Results, discussion, and design of the RMIS

This chapter constitutes the empirical core of this research, presenting the results derived from the thematic processing of semi-structured interviews conducted via NVivo 10. These findings are triangulated with field observations and established theoretical frameworks to ensure a rigorous analysis of the risk management ecosystem at Ooredoo Algeria. By moving from a critical assessment of the AS-IS state to a defined TO-BE vision, this chapter establishes the functional requirements and architectural modeling necessary for a digitalized Risk Management Information System (RMIS).

## Section 1: Organizational diagnosis, results and discussion

This section presents the empirical findings of the study, transitioning from a detailed assessment of Ooredoo's current risk management framework to a thematic analysis of stakeholder insights derived through NVivo 10.

### 1. Analytical synthesis of interview results: An NVivo-based qualitative study

The qualitative data collected through semi-structured interviews were analyzed using a thematic approach based on coding and categorization. In this regard, matrix coding query was developed to synthesize and organize the responses of each interviewee according to the predefined analytical axes and nodes. This matrix enables a structured visualization of recurring themes and patterns across participants, while ensuring traceability between raw data and interpreted findings. By grouping responses under common categories, it facilitates a systematic comparison of perceptions related to current risk management practices, identified limitations, assessment methods, and expectations regarding the proposed RMIS. This analytical tool thus contributes to enhancing the rigor, transparency, and reliability of the qualitative analysis process, while supporting the abductive logic adopted in this research *(see Appendix C)*.

While the interviews were initially guided by a four-axis framework, the qualitative analysis allowed for a more granular, inductive categorization based on semantic saturation observed during the coding process. Consequently, the results have been refined into four thematic pillars that more accurately reflect the operational reality and technical expectations of the stakeholders.

**Axis 1: Current risk management landscape**

The analysis reveals a paradox between methodological rigor and the limitations of current tools.

- **Methodological alignment**: The process is strictly aligned with the ISO 31000:2018 standard, utilizing SWOT, PESTEL, and Ishikawa methods.
- **Reliance on manual tools**: Despite this rigor, monitoring is "carried out via Excel spreadsheets," which weakens data reliability and real-time accessibility.

**Axis 2: System limitations and challenges**

This axis identifies the bottlenecks justifying the need for a transition.

- **Reporting inefficiency**: Manual collection, data filtering, and administrative recording are identified as the "most repetitive and time-intensive phases".
- **Disclosure gaps**: "Collection difficulty (disclosure)" is a primary concern, often hindered by a lack of global visibility on underlying risks.

**Axis 3: RMIS functional requirements**

Expectations for the target system are clear, focusing on technical empowerment and automation.

- **Interconnectivity**: Interconnection is considered "fundamental to ensuring data reliability and enabling real-time communication".
- **Dynamic Alerting**: Stakeholders prioritize "clear alerts on regulatory changes" and "pop-up type notifications" for report deadlines.

**Axis 4: adoption factors and strategic impact**

Respondents agree that digitalization, specifically an integrated RMIS, is a lever for cultural and operational transformation.

- **Transversal visibility**: A RMIS is perceived as "crucial for obtaining global and transverse visibility of risks within Ooredoo Algeria".
- **Time optimization**: Automating recurring tasks is seen as a way to "free up time for business functions".

**Summary of trends:**

A word frequency query and frequency analysis validate these qualitative observations:

***Table 5: Summery trends***

| Central theme | Lexical weight | Significance for the study |
|---|---|---|
| **Risk** | 2.34% | The core of the subject, omnipresent in all layers of the organization. |
| **Units** | 1.58% | Indicates the importance of interconnection between different Business Units. |
| **Changes** | 1.33% | Reflects the need for the system to adapt to regulatory and legislative evolutions. |
| **Information** | 1.21% | Highlights that the RMIS must primarily be a tool for reliable data management. |

**Source:** Elaborated by authors based on NVivo 10.

The lexical prominence of 'Units' and 'Changes' confirms that the stakeholders do not just want a storage tool, but a dynamic platform capable of synchronizing different departments and adapting to an evolving regulatory landscape.

The triangulation of the thematic analysis matrix and word frequency query reveals that while Ooredoo possesses a mature risk methodology, its "handcrafted" technical execution (Excel/Email) hinders real-time responsiveness.

Thematic dominance: The terms "Act" (2.66% weighted frequency) and "Risk" (2.34%) are the most prevalent, confirming that operational action and compliance are the primary concerns of the participants.

Organizational friction: High frequencies for "Communication" (1.42%) and "Changes" (1.33%) highlight that the most significant challenges reside in information flow and the need for adaptation.

***Figure 12: Word frequency query***


**Source:** NVivo 10.

## 2. Assessment of Ooredoo Algeria's Existing Risk Management process (AS-IS)

The current risk management landscape at Ooredoo Algeria is characterized by a strong adherence to international standards but hindered by technical limitations.

- **Methodological Framework**: The process is strictly aligned with the ISO 31000:2018 standard, ensuring a structured approach to risk identification and assessment.
- **Organizational Structure**: Risk management is segmented into four pillars: strategic, operational, financial, and compliance/ethics. It relies on a "bottom-up" flow where information is identified at the field level and escalated to the ERM unit.

- **Tooling**: Despite the rigor of the methodology, monitoring is primarily maintained through Excel spreadsheets and stored on SharePoint.
- **Communication**: Coordination involves "Risk Champions" within each directorate, yet the flow of information remains largely asynchronous, relying heavily on emails.

## 3. Identification of system gaps and improvement opportunities

Triangulating the NVivo outputs with field observations reveals critical gaps between the theoretical framework and operational reality:

- **The "Manual Bottleneck"**: Manual data collection and administrative recording are identified as the most resource-intensive and repetitive tasks, leading to a lack of real-time reactivity.
- **Disclosure gaps**: There is a notable "difficulty of collection" regarding critical information, often due to confidentiality constraints or a lack of global visibility on underlying risks.
- **Inconsistent risk culture**: While formal processes exist, there is a perceived "lack of risk culture at the individual level," which limits the organization's ability to anticipate potential threats proactively.
- **Environmental complexity**: The complex and shifting regulatory environment in Algeria makes it difficult to distinguish between known and emerging risks using current tools.

## 4. Functional specifications of the RMIS

To bridge the gap identified in the cross-diagnosis, the RMIS must satisfy five core functional pillars:

- **Automated workflow**: The system must prioritize the automation of collection and the generation of periodic reporting templates to free up operational time.
- **Real-Time alerting**: A critical requirement is the integration of "pop-up" notifications and alerts for regulatory changes and reporting deadlines.
- **Collaborative interface**: The RMIS must provide a "simple, intuitive interface" with a digital sharing space accessible to Business Units, featuring differentiated access rights (Viewer/Editor).
- **Interconnectivity**: The system must be capable of interconnecting with existing data sources to ensure data integrity and permanent accessibility across the organization.

- **Dynamic visualization**: The system should move beyond static files to provide real-time data visualization through dashboards, facilitating better risk management by each stakeholder.

**Comparison of management states: AS-IS vs. TO-BE**

The proposed RMIS aims to bridge the gap between current limitations and target efficiency:

***Table 6: Current limitations and target RMIS***

| Process step | AS-IS (Current state) | TO-BE (Target RMIS state) |
|---|---|---|
| **Data Collection** | Manual, Excel-based, time-consuming | Automated collection and digital sharing |
| **Reactivity** | Delayed, periodic reporting | Real-time alerts and dynamic dashboards |
| **Traceability** | Dispersed in emails and files | Unified, standardized, and immutable |

**Source:** Elaborated by authors.

The analytical results demonstrate that for Ooredoo, the transition to an RMIS is not merely a technological choice, but an operational necessity to guarantee data reliability and strategic responsiveness in an increasingly complex regulatory environment.

## Section 2: Process and the system modeling of the RMIS

The diagnostic conducted in the first section provided a clear understanding of risk management practices at Ooredoo Algeria. Although the process is aligned with ISO 31000, it remains largely manual, relying on interviews, Excel-based registers, and email communication, which leads to fragmented information, limited traceability, and delays in reporting. These findings form the basis for the system proposed in this section. Building on both the theoretical foundations developed in chapter 1 and the insights gathered from the field, this section presents the design and modeling of a Risk Management Information System (RMIS) tailored to the organization's needs. The approach is structured around five complementary dimensions: the definition of the system's architecture and design principles, the modeling of target business processes using BPMN, the conceptual modeling of the system through UML, the design of a multi-criteria risk assessment model, and finally, the evaluation of the proposed solution and its implementation within the organizational context.

### 1. Global architecture and design principles of the RMIS

The RMIS is built on a set of core principles that align digital functionality with the organization's established risk management standards.

#### 1.1. System identity and design intent

The proposed Risk Management Information System is a desktop application designed to digitalize, enrich, and partially automate Ooredoo Algeria's existing risk management process. It does not reinvent the organization's risk management methodology—which is already ISO 31000-aligned and organizationally embedded—but provides the digital infrastructure that makes it faster, more consistent, more visible, and more traceable.

The system is built around three core contributions: the digitalization of manual processes currently conducted through Excel and email, the enrichment of risk evaluation through a weighted multicriteria scoring model, and the extension of current capabilities through structured corporate-level risk tracking and a formalized multi-step report validation workflow.

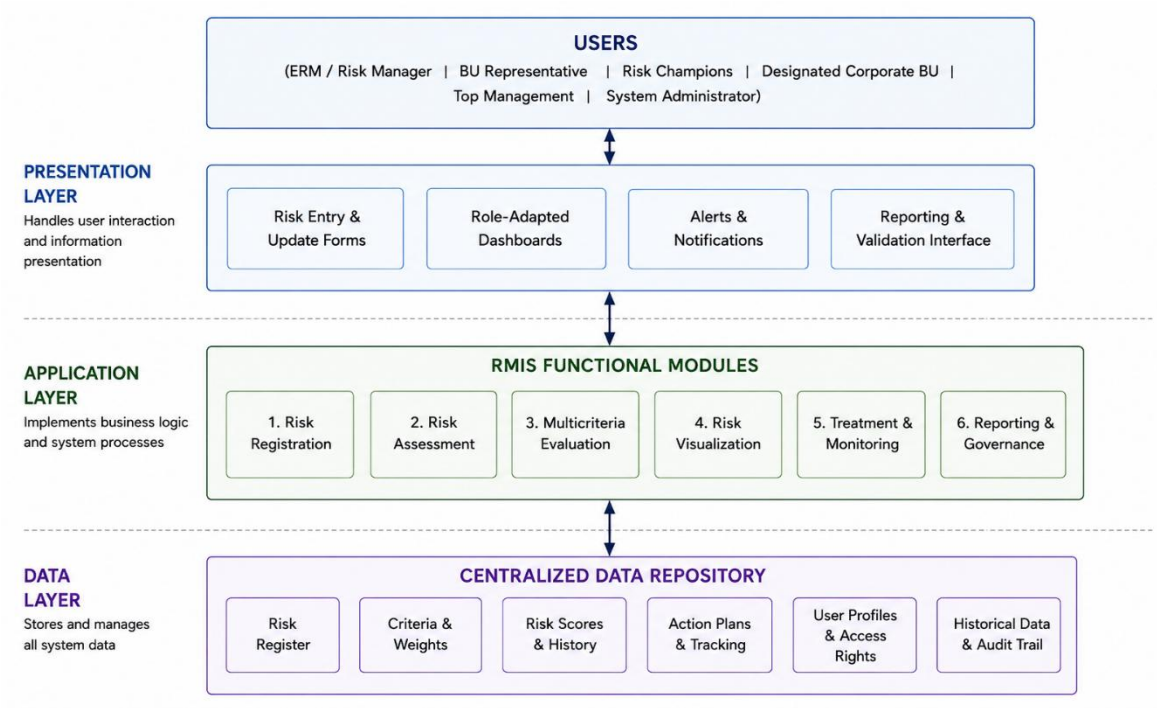
Three design principles governed every architectural and functional decision made in this section. The first is ISO 31000 alignment: Every module and every workflow maps onto a defined phase of the ISO 31000 risk management process, ensuring that the system reinforces rather than disrupts the framework Ooredoo already operates within. The second

is role-based design: The system adapts its interface, its data perimeter, and its available functions to each user profile, ensuring both confidentiality and usability across a diverse organizational user base. The third is progressive implementation: The architecture is modular by design, allowing the system to be deployed in phases without requiring a complete organizational transformation before value is delivered.

### 1.2. Three-layer logical architecture

The system is organized according to a three-layer logical architecture—a recognized IS design pattern that separates user interaction, system logic, and data management into distinct, interdependent layers (Kenneth C & Jane P, 2018). This separation ensures modularity, maintainability, and security — each layer can evolve independently without disrupting the others. The overall architecture is illustrated in Figure 13.

***Figure 13: Three-layer logical architecture of the proposed RMIS***




**Source:** Elaborated by authors, inspired by three-layer IS architecture principles (Kenneth C & Jane P, 2018).

### 1.3. User integration: role-based model

Access to the system is governed by a strict role-based model in which each user profile has a clearly defined scope of action and a precisely bounded data perimeter. Five profiles structure the system's user model:

- **ERM / Risk manager**: full access to all risks, all modules, and all organizational perimeters. Responsible for validation, treatment assignment, report generation, and overall risk governance.
- **Business unit's (BU) representative**: one designated person per department. Enters and updates their department's risks, confirms data during reporting cycles, verifies their section of consolidated reports, and executes assigned action plans. Sees only their own perimeter.
- **Designated corporate BU / top management/ risk champion**: Validates the final consolidated report and receives the general report. Has access to the executive dashboard.
- **System administrator**: configures user profiles, access rights, multicriteria weights, and system parameters. Has no access to risk content.

This role-based structure ensures both confidentiality — sensitive risk data remains within appropriate organizational boundaries — and accountability — every action in the system is traceable to a specific user, role, and timestamp through the audit trail.

## 2. BPMN-based modeling of target business processes (TO-BE)

The process models presented in this section are based on the BPMN 2.0 standard, which provides a clear graphical language for representing business processes through elements such as swimlanes, tasks, gateways, and message flows. This notation is particularly suitable in this context as it captures both human and system interactions, making it possible to identify responsibilities and understand how information flows between actors. The models developed are TO-BE representations, describing the target state of risk management processes as supported by the proposed RMIS rather than the current manual practices. Two main processes are modeled: the risk lifecycle and the reporting workflow.

### 2.1. BPMN: Risk lifecycle

The first process model represents the complete risk lifecycle, covering all stages from identification to closure. It is structured across three swimlanes: the BU Representative, the ERM / Risk Manager, and the System. The model reflects the target (TO-BE) operation of risk management within the RMIS.

The process begins with two possible entry points:

- The BU representative identifies a risk or opportunity and submits it through a structured form

- The ERM / risk manager directly registers a risk and assigns it to the responsible business unit

These two paths converge at the system level, where the following automated actions are performed:

- Generation of a unique Risk ID and timestamp
- Storage of the risk in a centralized database
- Notification sent to ERM

Once notified, the process continues as follows:

- ERM reviews the risk and defines a treatment and action plan
- The system notifies the BU Representative
- The BU executes the action plan and updates the risk status

The system ensures continuous monitoring by:

- Tracking progress in real time
- Triggering alerts in case of delays

At this stage, ERM evaluates the situation and makes a key decision:

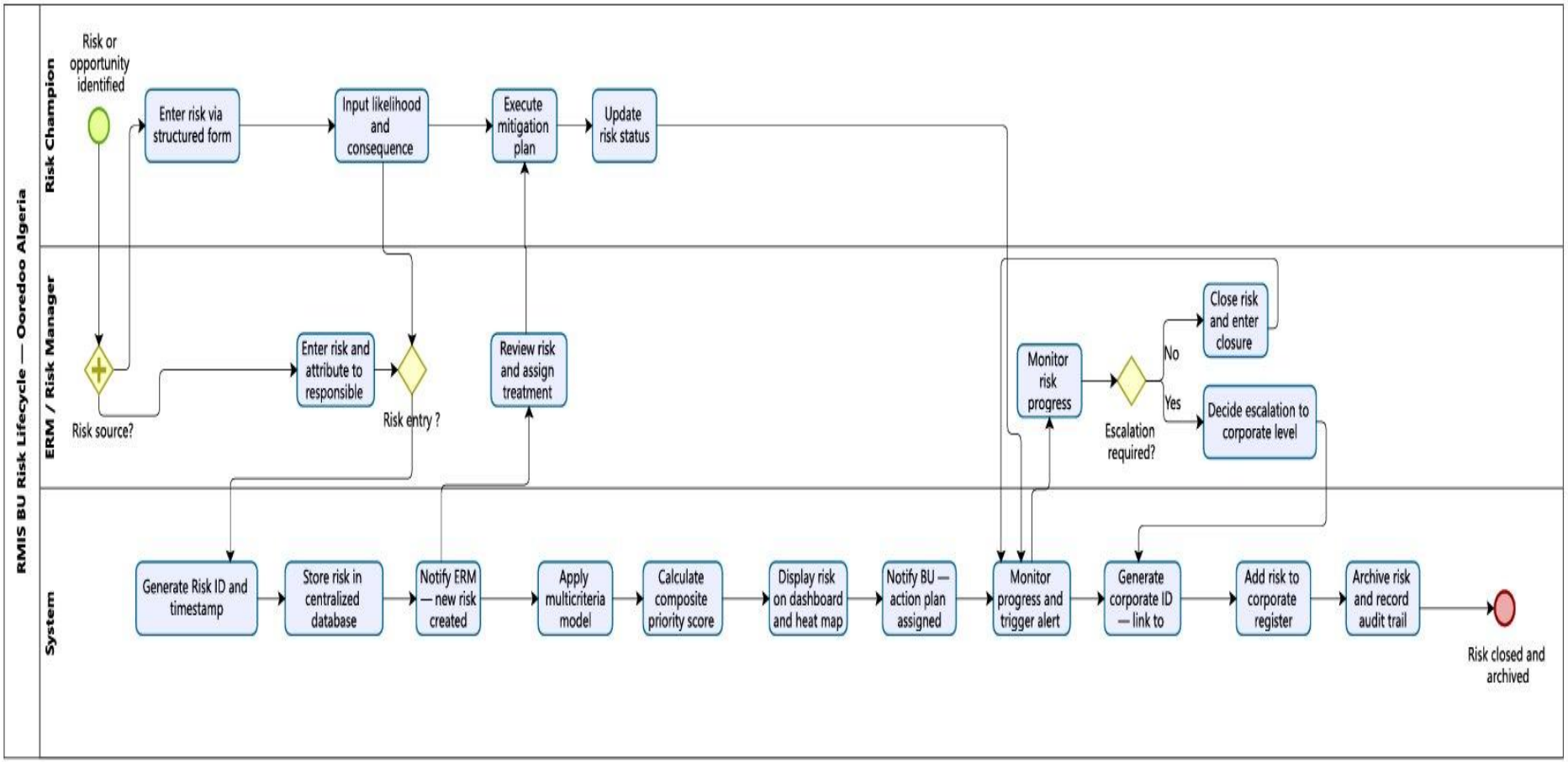
- **Escalation required** → the system generates a corporate ID, links it to the original risk, and integrates it into the corporate register while maintaining monitoring at both levels
- **No escalation** → ERM proceeds to closure

In the closure phase:

- ERM provides a closure justification
- The system archives the risk and records a full audit trail

This process is illustrated in Figure 14.

*Figure 14: Risk lifecycle of the RMIS*




**Source:** Elaborated by authors.

### 2.2. BPMN: Reporting workflow

The second process model describes the complete reporting cycle, from its initiation to the delivery of the final report to top management. It involves four main actors: the system, BU representatives, the ERM / risk manager, and the designated corporate BU / top management.

The process is organized into four main phases:

#### 2.2.1. Trigger and data confirmation

The reporting cycle is initiated in one of two ways:

- Automatically through a quarterly system trigger
- Manually, following an on-demand request from Top Management

The system then:

- Sends a data confirmation request to all BU Representatives
- Tracks confirmations in real time

BU Representatives:

- Review and update their risk data
- Confirm accuracy

Once all confirmations are completed:

- The system notifies ERM

#### 2.2.2. Data validation and report generation

ERM:

- Reviews the consolidated data
- Validates its consistency
- Triggers report generation

The system automatically produces a consolidated report including:

- Risk heat map
- Top 10 prioritized risks
- Risk category breakdown
- Treatment status
- KPI / KRI indicators

The report is then sent to BU representatives for verification.

If a discrepancy is identified:

- The BU sends a correction request
- ERM adjusts the data and regenerates the report

This loop continues until all BUs validate their respective sections.

### 2.2.3. Final validation

Once verification is complete:

- The system sends the report to the Designated Corporate BU / Top Management

Two outcomes are possible:

- **Correction requested** → ERM revises and resubmits
- **Approved** → the system locks the report, preventing further modifications

### 2.2.4. Finalization and distribution

In the final phase:

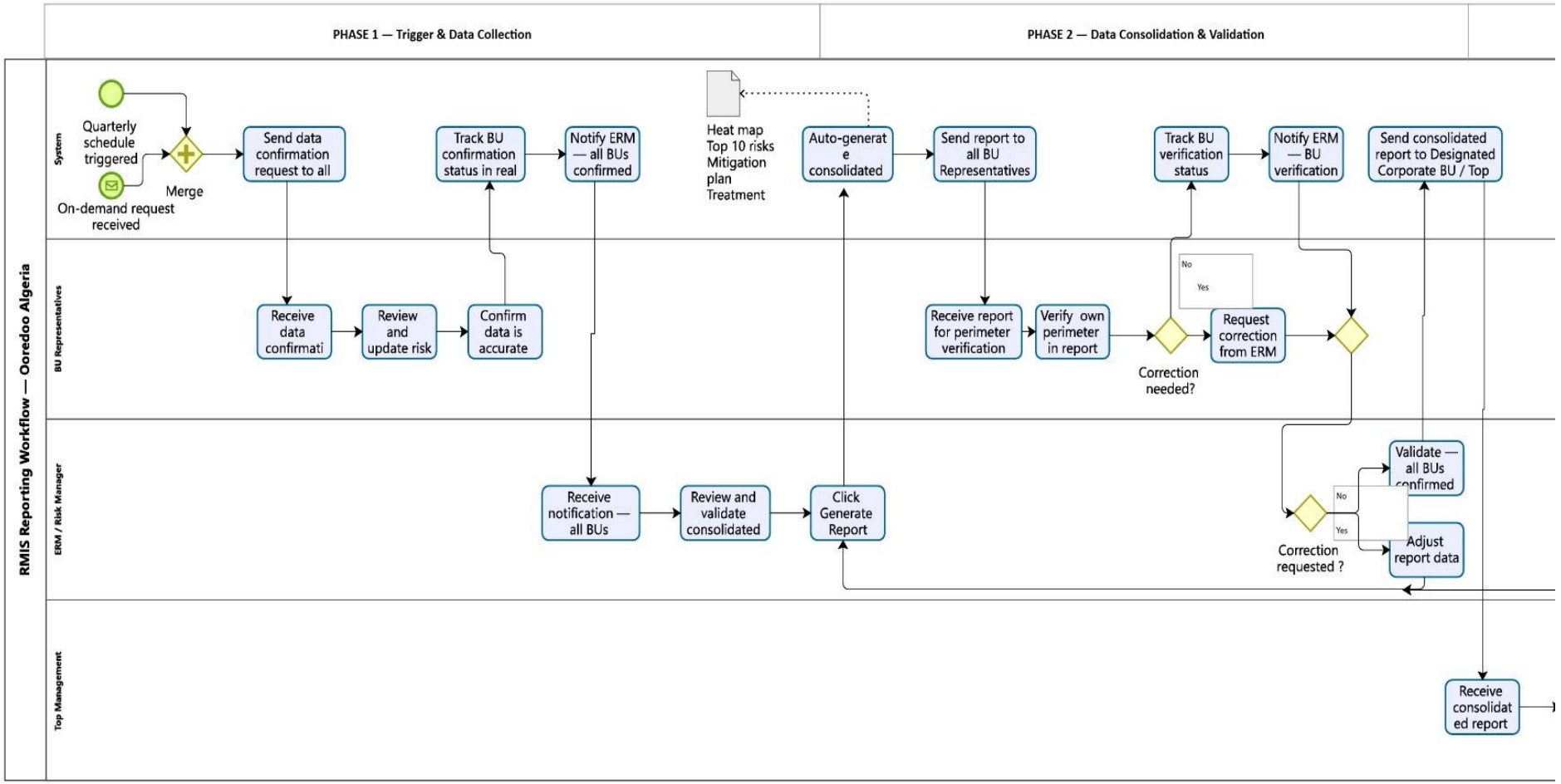
- The system generates the operational report, with each BU accessing only its own data
- ERM prepares the executive report, adding:
  - KRI analysis
  - Trend interpretation
  - Risk appetite alignment
  - Cost-benefit insights

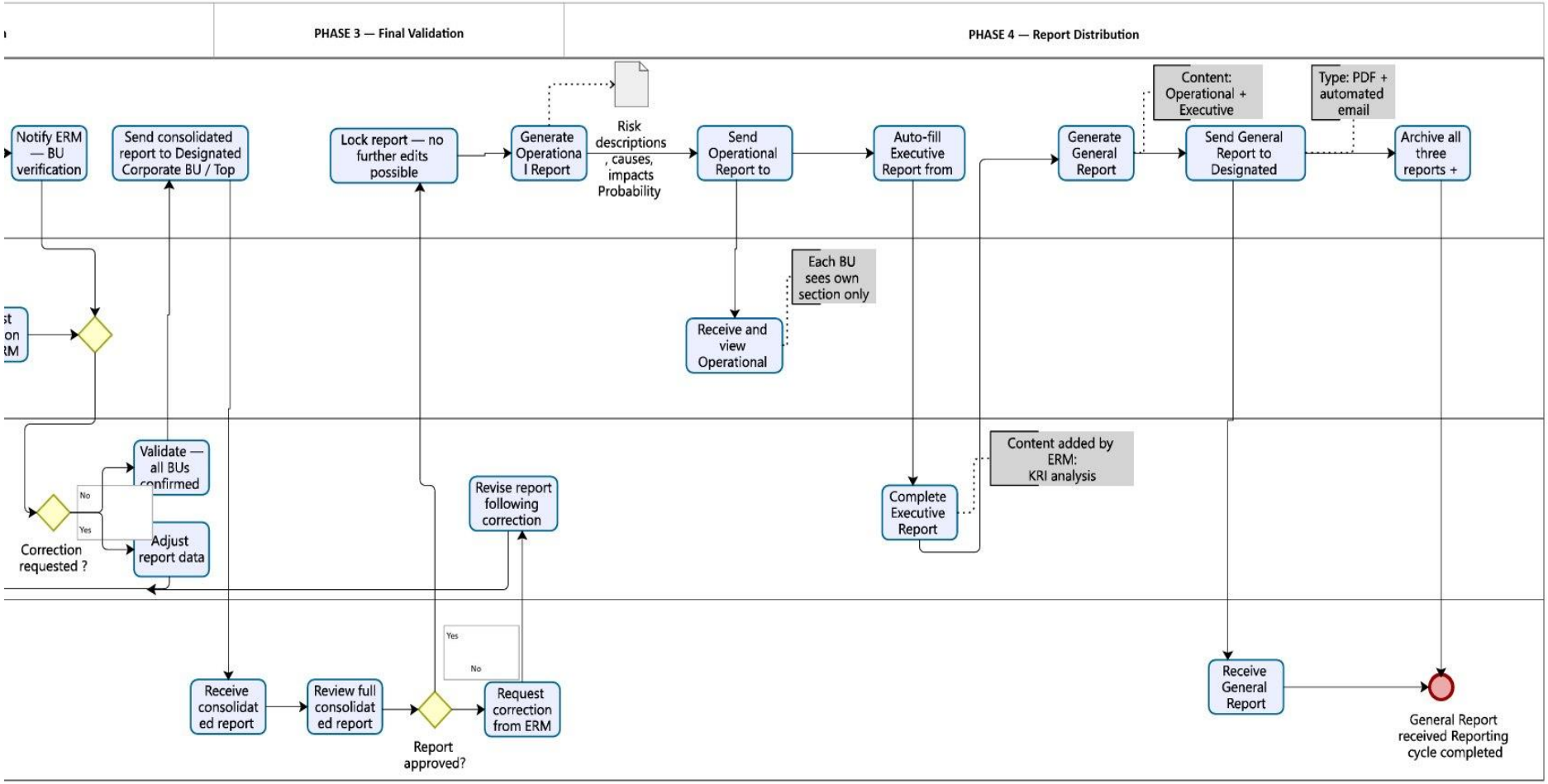
The system then:

- Generates the general report (operational + executive)
- Sends it to top management (PDF + email)
- Archives all reports and records a complete audit trail

This process is illustrated in Figure 15.

*Figure 15: BPMN : Report generation and validation workflow of the RMIS*






**Source:** Elaborated by authors.

## 3. UML-based conceptual modeling of the RMIS

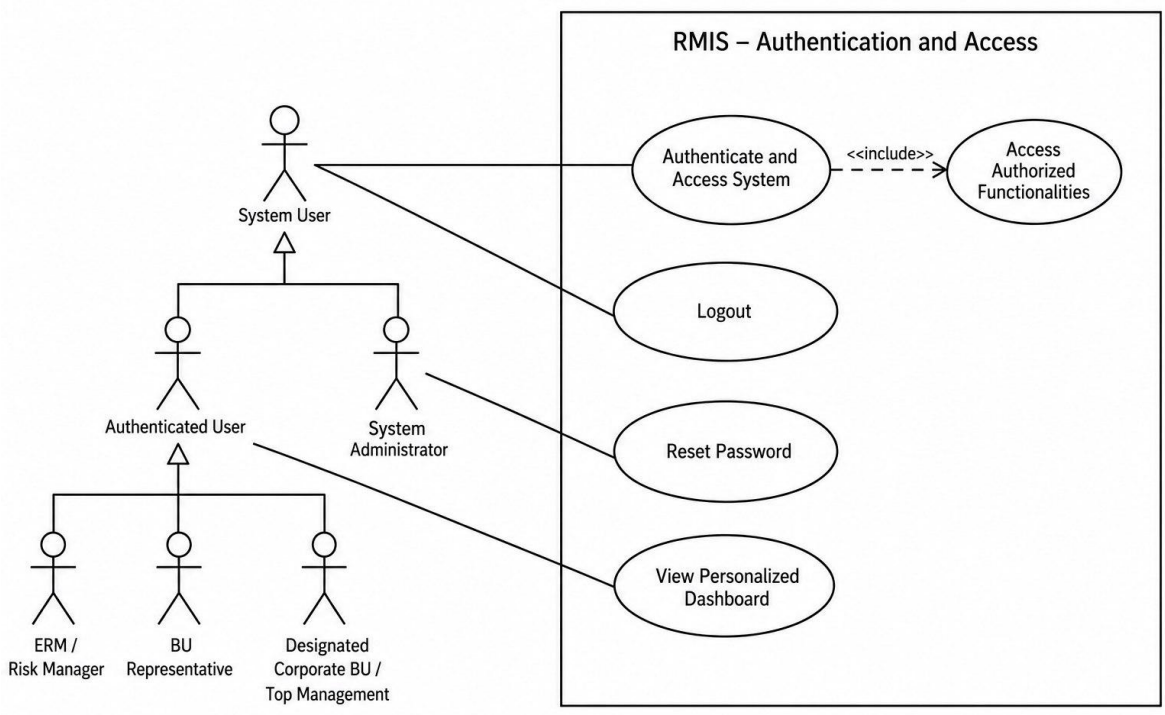
While the BPMN models presented in Section 2.2 describe the dynamic behavior of risk management processes, UML modeling provides a complementary perspective by focusing on the internal structure of the system. It clarifies how the RMIS is organized, how data is structured, and how different actors interact with system functionalities.

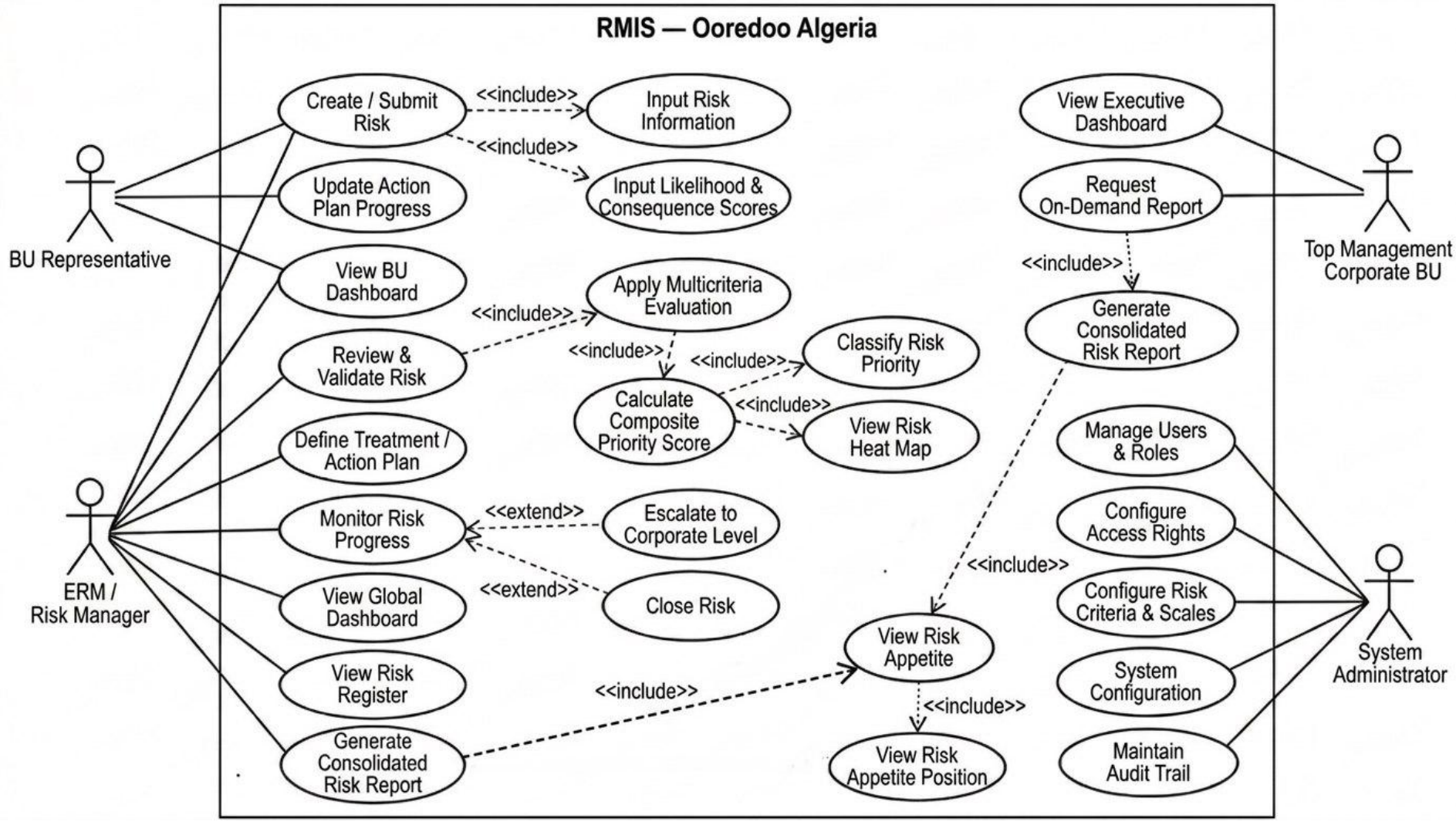
Three UML diagrams are developed, each addressing a specific dimension of the system.

### 3.1. Use case diagram

The use case diagram defines the functional scope of the RMIS by identifying the main actors and their interactions. It highlights the roles of the ERM / risk manager, BU representative, designated corporate BU / top management, and system administrator, each associated with specific functionalities. It provides a clear view of user involvement in key processes such as risk registration, assessment, monitoring, and reporting while also illustrating relationships between use cases. This representation clarifies system boundaries and ensures that all functional requirements are consistently captured.

***Figure 16: Global use case diagram of the RMIS with authentication use case***






**Source:** Elaborated by authors.

### 3.2. Class diagram

The class diagram represents the static structure of the RMIS by defining its core entities, their attributes, and the relationships that connect them. It provides a structured view of how risk data is organized, processed, and maintained within the system.

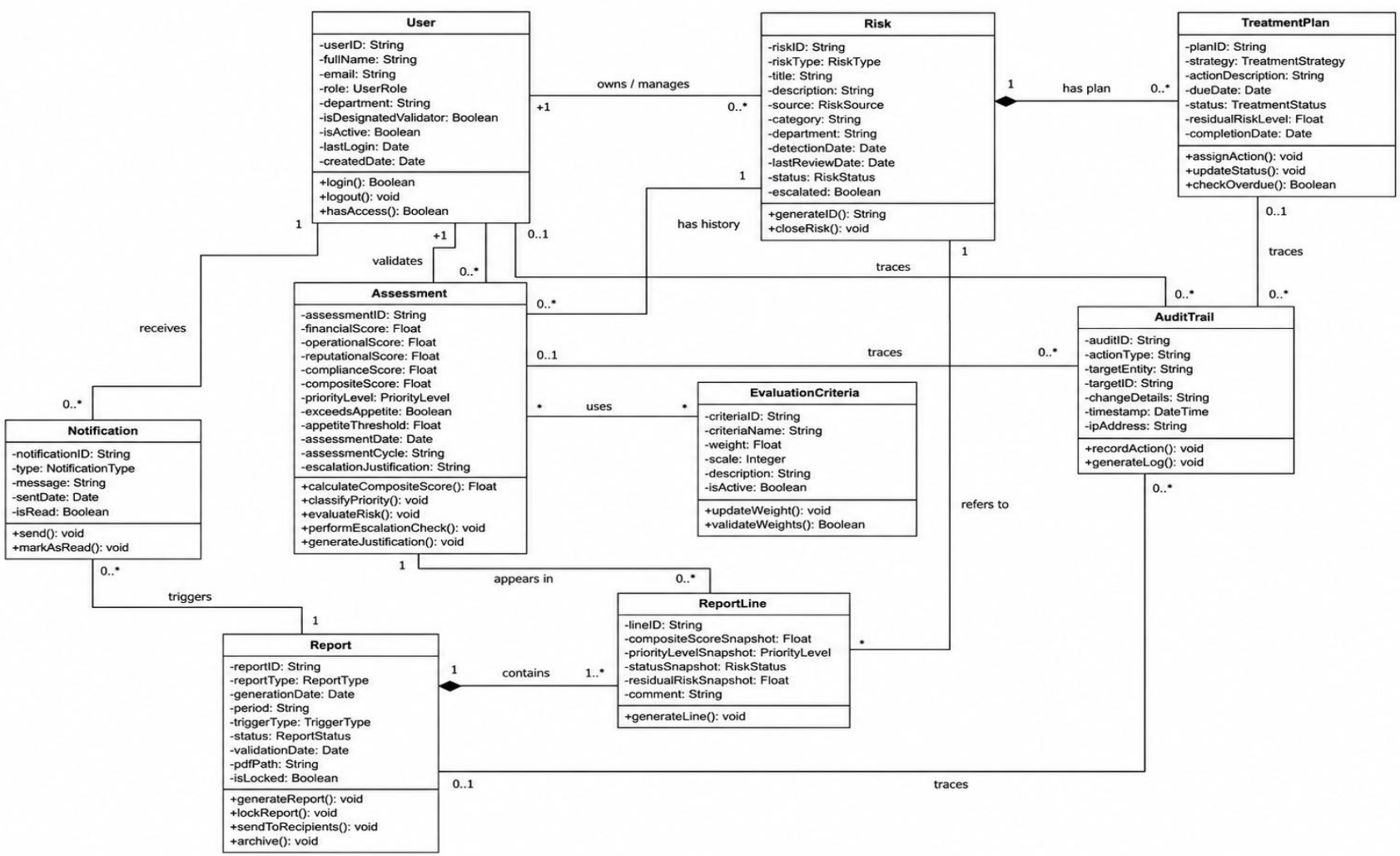
**Core entities:**

- **Risk**
  - Central entity of the system
  - Stores identification and contextual data
- **Assessment**
  - Stores evaluation results
  - Allows multiple evaluations of the same risk over time
- **Evaluation criteria**
  - Contains criteria and weights
  - Configured by the administrator
- **Treatment plan**
  - Defines mitigation actions:
    - Strategy
    - Owner
    - Deadline
    - Residual risk

**Supporting entities:**

- **Report**
  - Represents generated reports
- **ReportLine**
  - Association between Report and Risk
  - Stores a snapshot of risk data at report time
  - Ensures historical consistency
- **User**
  - Manages access control and responsibilities
- **Notification**
  - Supports communication between actors
- **AuditTrail**
  - Records all system actions for traceability

*Figure 17: Class diagram of the RMIS*




**Source:** Elaborated by authors.

### 3.3. Sequence diagram

The sequence diagram models the dynamic interactions between system actors during the report generation cycle, which represents the most complex operational scenario of the RMIS. It illustrates the chronological exchange of messages between participants and highlights how the system coordinates actions, processes data, and ensures consistency throughout the workflow.

**Participants**

- ERM / Risk Manager
- RMIS System
- BU Representatives
- Designated Corporate BU / Top Management

**Main phases**

- **Trigger phase**
  - Report generation initiated
- **Data confirmation**
  - BU validates and confirms data
  - Loop until completion
- **Report generation**
  - System generates consolidated report
- **Verification phase**
  - BU reviews its perimeter
- **Validation phase**
  - Final approval or correction
- **Finalization**
  - Reports generated and distributed
  - Archive + audit trail

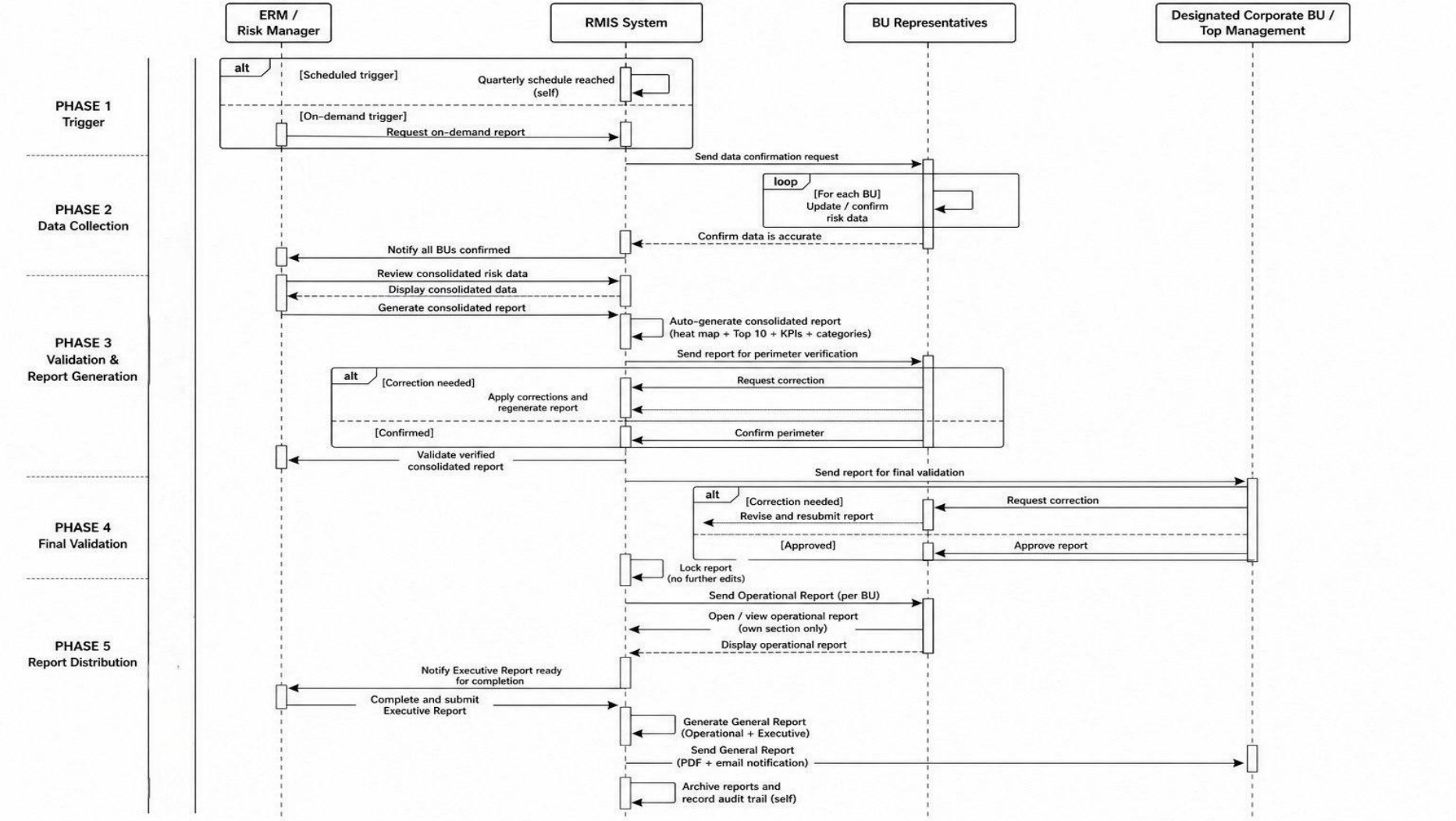
**Control structures**

- **Loop fragment**
  - Repeated BU confirmation process
- **Alt fragments**
  - Correction vs validation decisions:
    - BU verification
    - Final approval

**Final output**

- Operational Report → BU (restricted access)
- Executive Report → completed by ERM
- General Report → top management
- Full audit trail recorded

*Figure 18: UML sequence diagram: report generation cycle*




**Source**: Elaborated by authors.

## 4. Design of a multi-criteria risk assessment model

The effectiveness of a Risk Management Information System depends on its ability to evaluate and prioritize risks in a consistent and meaningful way. Traditional approaches generally rely on a simple combination of likelihood and impact. While practical, this method remains limited, as it reduces impact to a single dimension and does not reflect the complexity of real organizational risks. In the case of Ooredoo Algeria, the field study showed that risks may simultaneously affect financial performance, operational continuity, and strategic positioning, making a single impact value insufficient.

To address this limitation, the proposed RMIS integrates a multi-criteria assessment model that evaluates risks across multiple dimensions rather than relying on a single aggregated impact. This approach is aligned with ISO 31000, which emphasizes the importance of context-based and adaptable risk evaluation.

The model is structured around three main consequence dimensions. The financial dimension captures direct monetary effects such as losses, cost increases, or revenue impact. The operational dimension reflects the impact on service delivery, process efficiency, and system performance. The qualitative and strategic dimension addresses less tangible but critical aspects such as reputation, customer satisfaction, and regulatory exposure. A key characteristic of the model is that a single risk can be evaluated across several of these dimensions simultaneously, providing a more complete representation of its potential impact.

A central feature of the model is the introduction of a consequence library, which allows the ERM function to configure evaluation criteria, scoring scales, and the relative importance of each dimension. This ensures that the assessment model remains flexible and can evolve with the organization’s risk environment. It also enables the integration of expert knowledge directly into the system, reducing reliance on purely subjective judgment.

For each risk, the relevant consequence dimensions are selected based on its nature. Some dimensions are systematically applied to specific types of risks, while others are activated when considered relevant. This selective approach avoids rigid evaluation and ensures that the assessment remains proportionate and meaningful.

The assessment model relies on two categories of Key Risk Indicators to ensure that evaluations remain grounded in Ooredoo Algeria's operational reality. Constant KRIs represent stable data inputs provided periodically by BU Representatives — including Service Revenue, Active Base, and Network Availability — which serve as baseline

reference values for consequence scoring, particularly for operational and financial dimensions. Dynamic KRIs are system-calculated indicators derived from assessment outputs — including composite risk scores, severity trend evolution across assessment cycles, and risk appetite breach status — which enable real-time monitoring and forward-looking prioritization. Together, these two KRI categories ensure that the model produces not only a static risk classification but a continuously updated risk intelligence layer that supports informed governance decision-making at every level of the organization.

Based on the overall evaluation, risks are then classified into priority levels (critical, high, medium, and low). This classification supports decision-making by guiding treatment priorities, facilitating dashboard visualization, and structuring reporting outputs within the RMIS.

# 5. Design of the RMIS solution and evaluation of the proposed system

A comprehensive look at the system's architecture and performance metrics shows how the RMIS addresses the company's specific risk management needs.

## 5.1. The RMIS as an integrated solution

The proposed Risk Management Information System is designed as an integrated organizational solution rather than a standalone tool. It brings together the architecture, processes, data structure, and multi-criteria assessment model developed in the previous sections into a unified system. Its objective is to support the entire risk management lifecycle, from identification and evaluation to monitoring, reporting, and governance.

The system reflects the specific organizational context of Ooredoo Algeria. Several design choices directly result from field observations:

- Dual risk entry (BU and ERM) reflects actual practice
- The consequence library addresses the diversity of risk types
- The reporting workflow mirrors the existing governance structure
- Role-based access ensures confidentiality across departments
- Progressive implementation supports organizational adoption

Rather than introducing a new methodology, the RMIS operationalizes existing practices by improving their efficiency, consistency, and visibility.

## 5.2. System outputs and functional value

The system delivers several key outputs that address the limitations identified in the diagnostic phase:

- **Real-time dashboards:** Provide immediate visibility of risk exposure for all actors
- **Dynamic heat maps:** Improve risk prioritization using the multi-criteria model
- **Automated notifications:** Replace email-based coordination
- **Action plan tracking:** Monitor progress and trigger alerts in case of delays
- **Standardized reports:** Generate Operational, Executive, and General reports
- **Audit trail:** Ensure full traceability of all system activities

### 5.3. Evaluation of the proposed system

The RMIS is evaluated based on four key information system quality criteria.

**Reliability:** The system ensures consistency and data integrity through:

- Centralized data storage
- Automatic ID generation and timestamping
- Report locking after validation
- Full audit trail

**Scalability:** The system is designed to evolve with the organization:

- Modular architecture allows gradual expansion
- New users and departments can be added easily
- The consequence library can be extended over time

**Usability:** Usability is ensured through:

- Role-based interfaces adapted to each user
- Structured forms guiding data entry
- Integrated notifications
- Clear dashboards for quick decision-making

**Security:** Security is addressed through:

- Role-based access control
- Strict data isolation between business units
- Audit tracking of all actions
- Controlled report validation process

### 5.4. Implementation considerations

The transition to a digital system represents a significant organizational change. To reduce adoption risks, the RMIS is designed for progressive deployment:

- **Phase 1:** Digital risk register and notifications
- **Phase 2:** Multi-criteria scoring and heat maps
- **Phase 3:** Reporting automation
- **Phase 4:** Corporate-level risk management

This phased approach allows gradual adoption, supports organizational learning, and ensures that value is delivered from early stages.

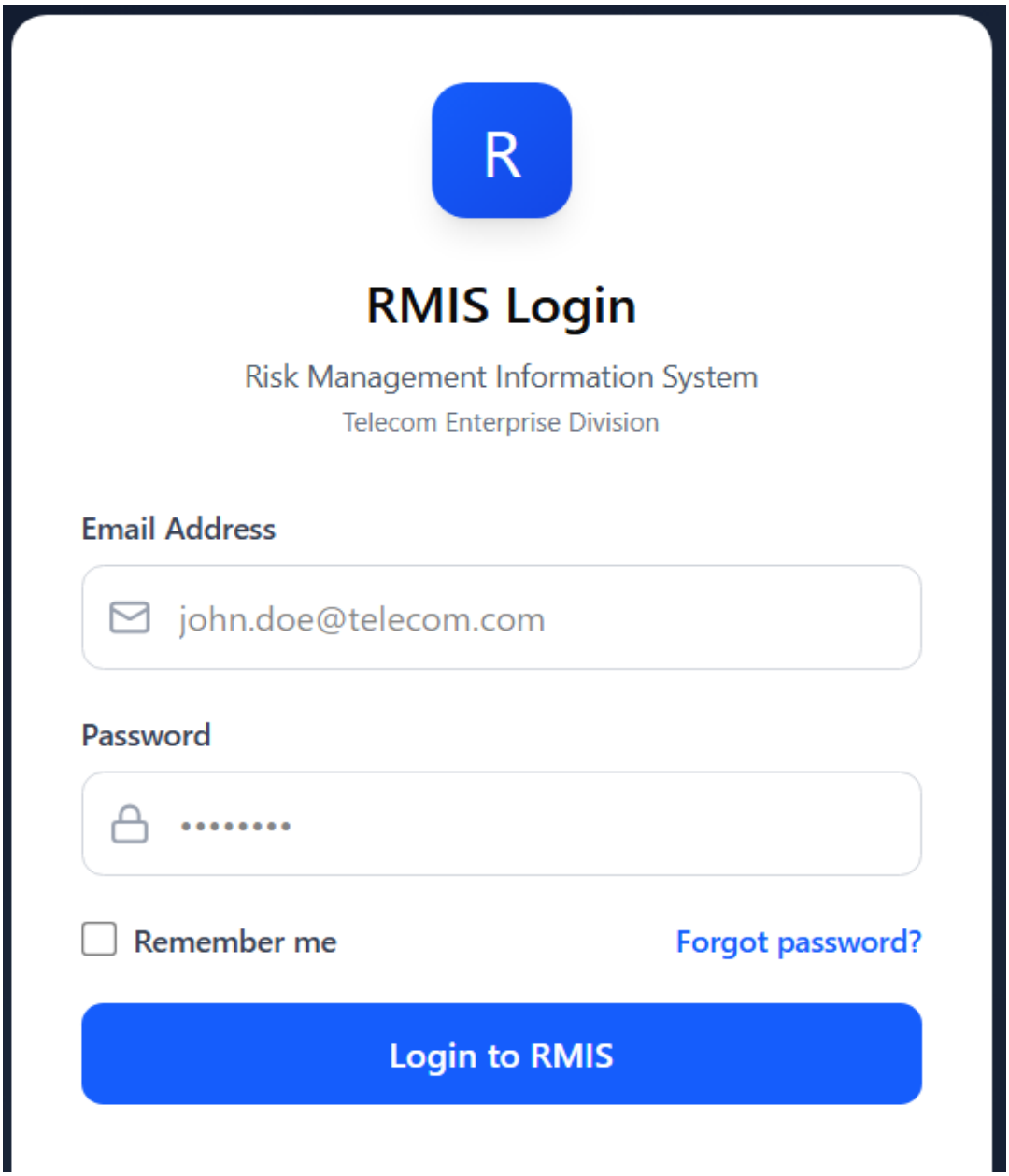
### 5.5. User interface design of the RMIS

The user interface of the RMIS was designed to support usability, role-based access, and real-time decision-making. The interfaces were prototyped using Figma and reflect the functional requirements identified during the field study.

**Login interface**

Figure 19 provides authenticated access—upon login, the system identifies the user's role and automatically loads their adapted interface and data perimeter.

*Figure 19: Risk register interface*

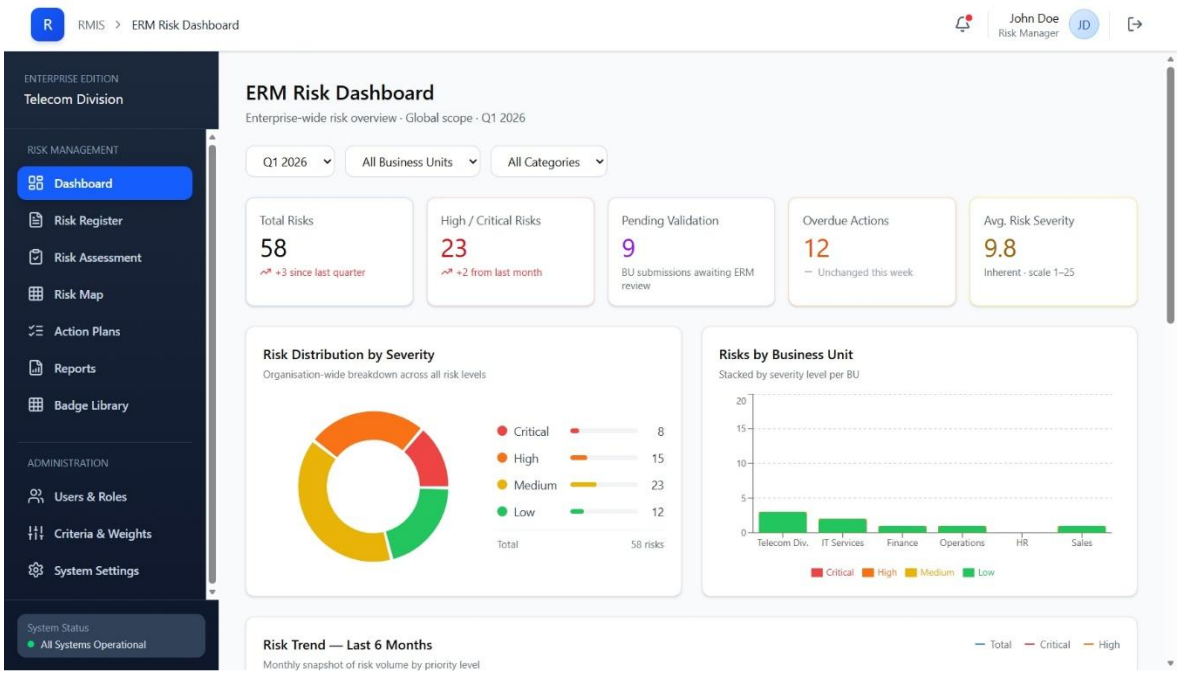


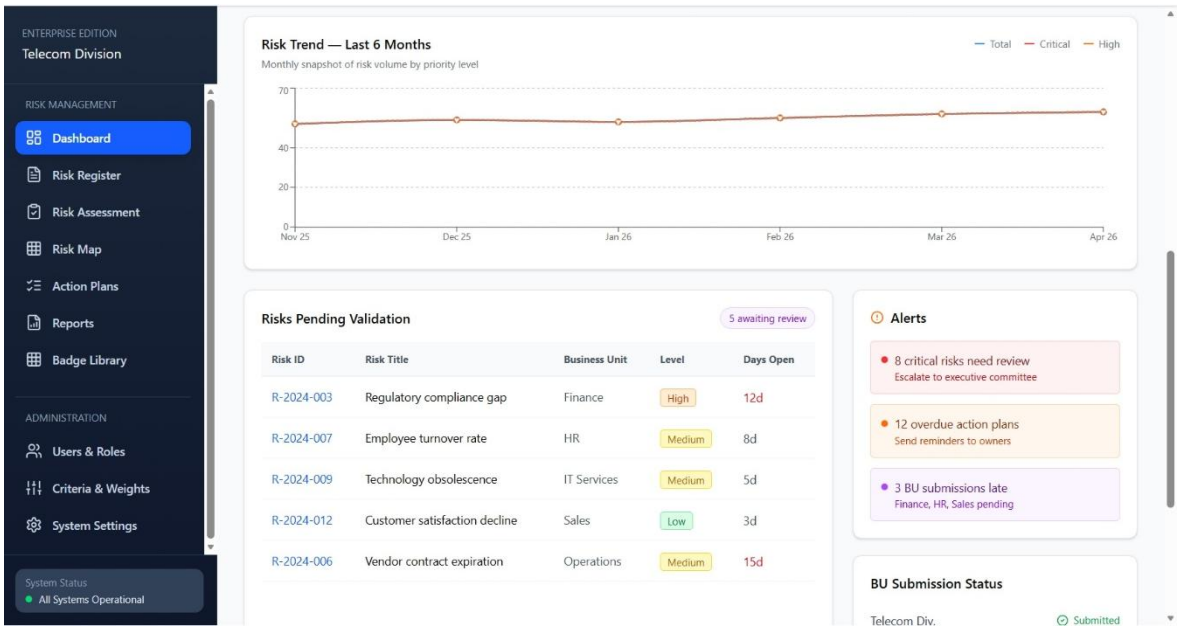

**Source:** Elaborated by authors (Figma prototype).

## The ERM global dashboard

Figure 20 consolidates real-time risk exposure across all business units, displaying key indicators, critical risk alerts, and overdue action counters to support strategic decision-making.

***Figure 20: ERM global dashboard***



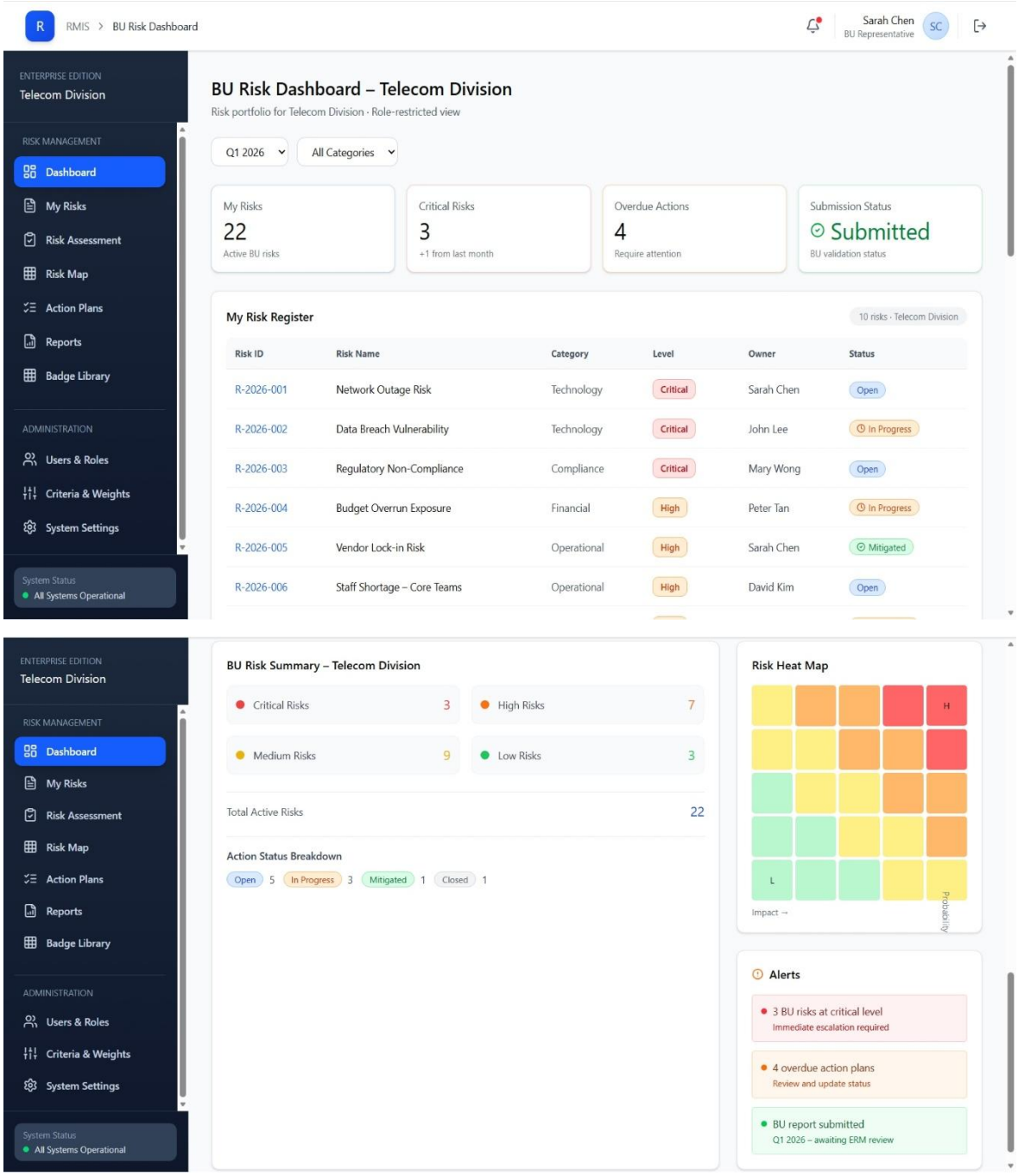




**Source:** Elaborated by authors (Figma prototype).

## The BU restricted dashboard

Figure 21 limits visibility strictly to the business unit's own perimeter, enforcing data isolation while providing local risk status, action plan progress, and reporting cycle submission tracking.

***Figure 21: Restricted dashboard***

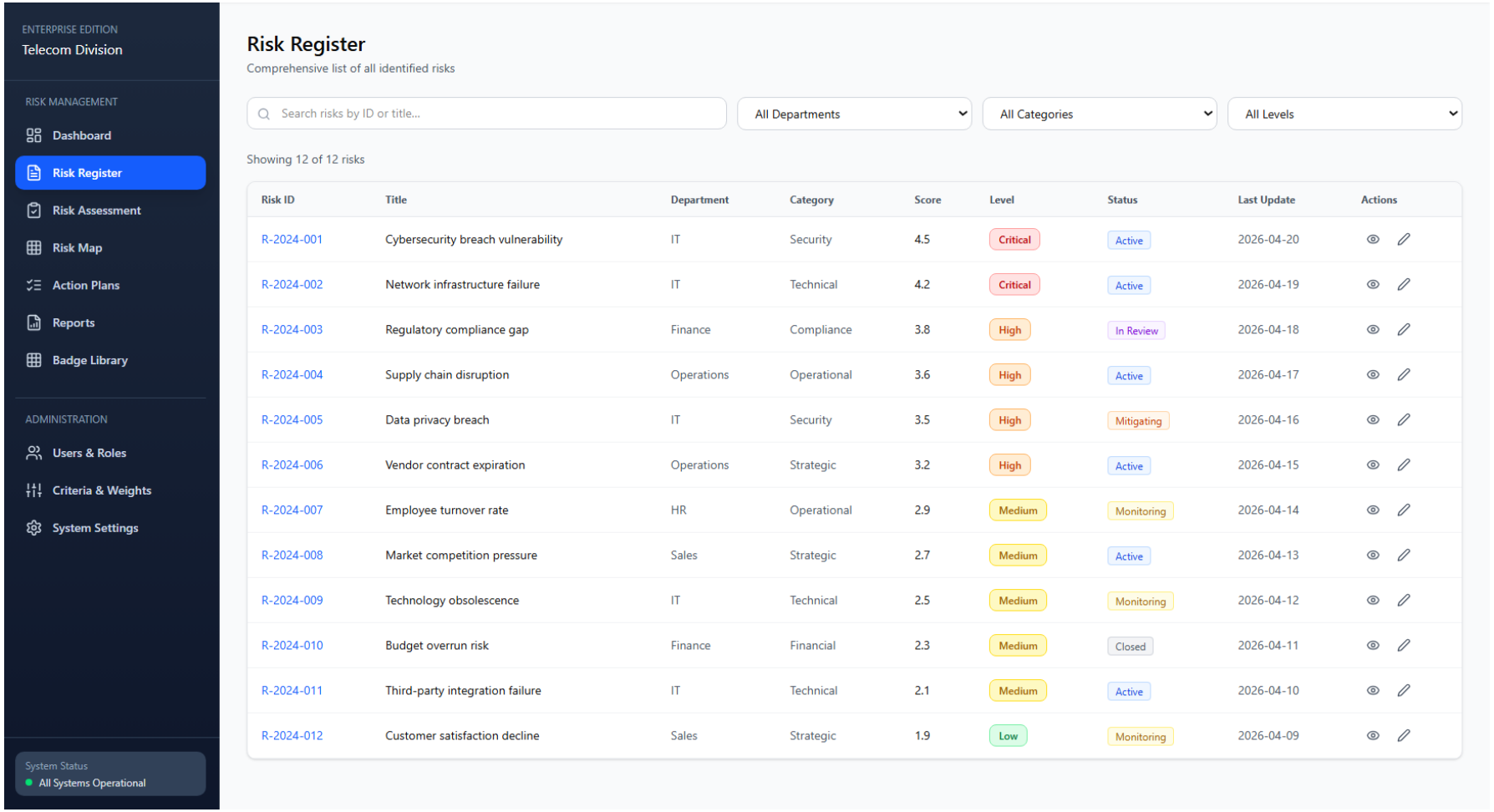



**Source:** Elaborated by authors (Figma prototype).

**The risk register**

Figure 22 centralizes all identified risks in a structured, searchable format displaying multicriteria scores, priority classifications, and treatment status.

*Figure 22: Risk register*

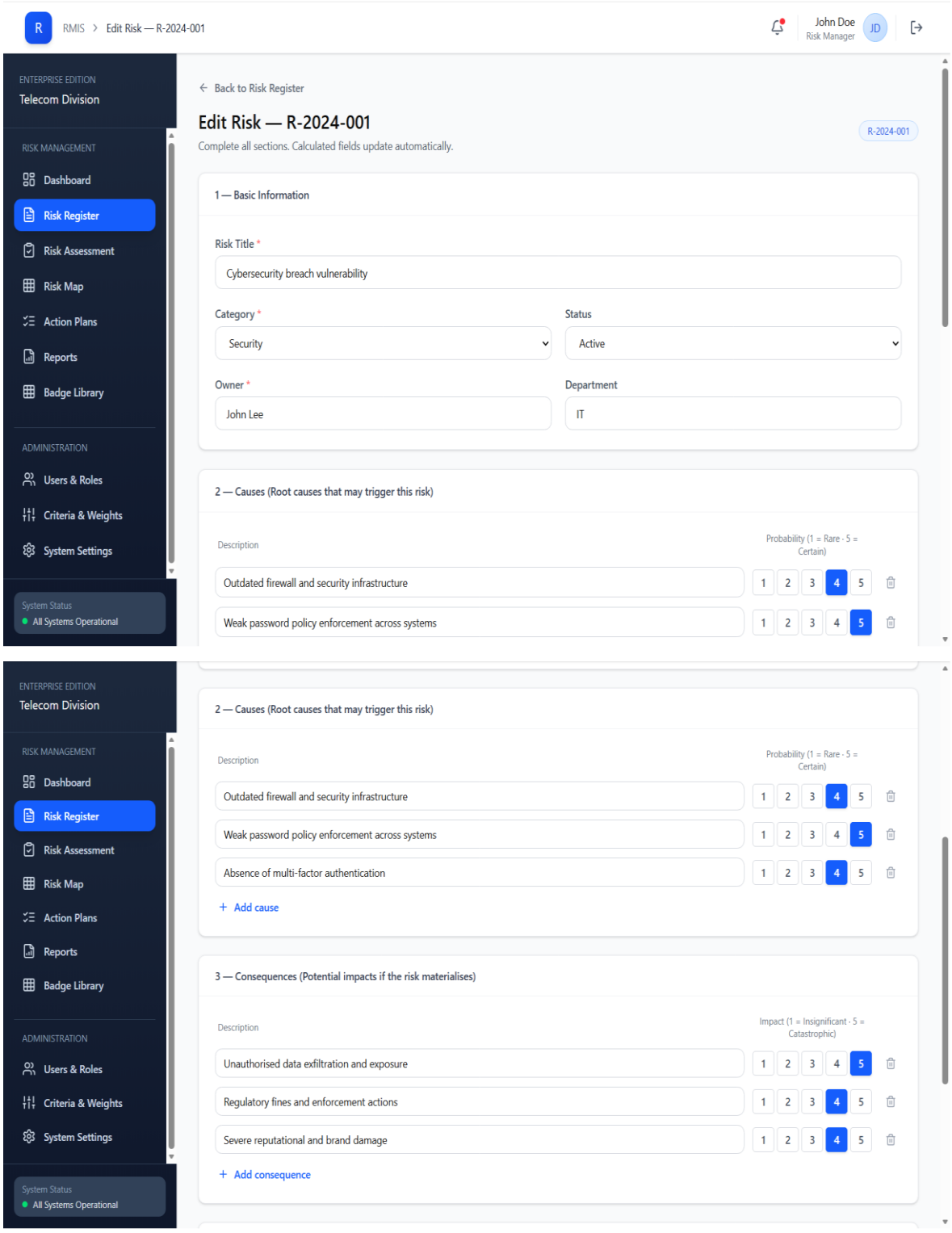


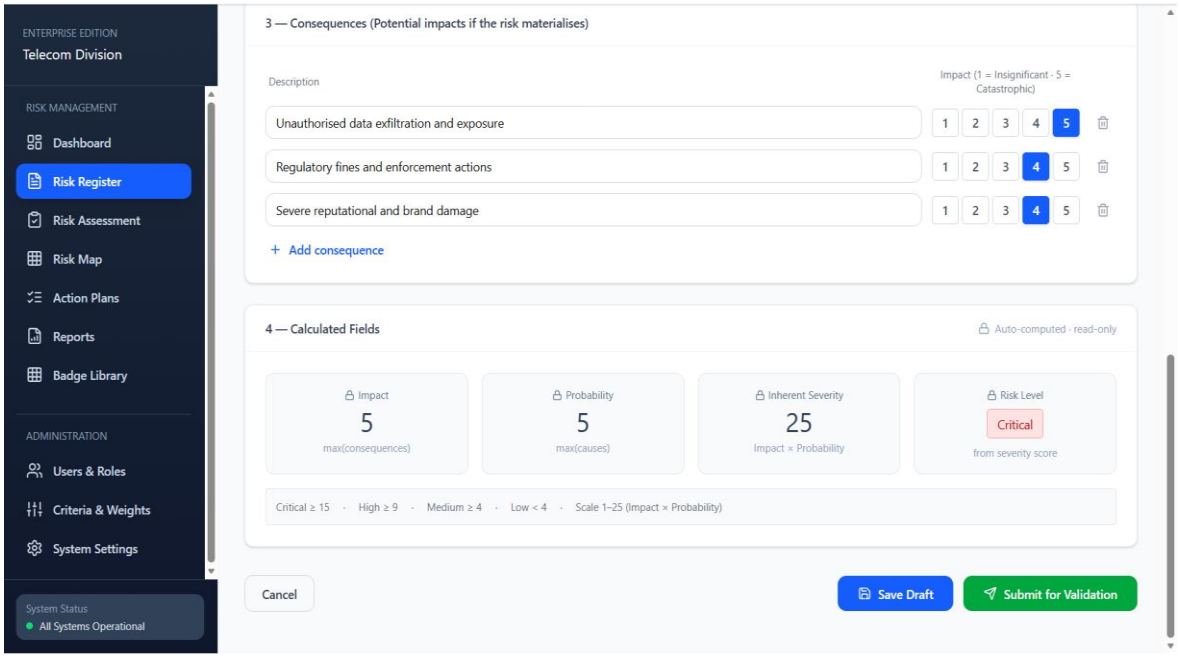

**Source:** Elaborated by authors (Figma prototype).

**The risk entry and assessment form**

Figure 23 guides users through structured risk registration and consequence evaluation, feeding directly into the multicriteria model.

***Figure 23: Risk entry & assessment***



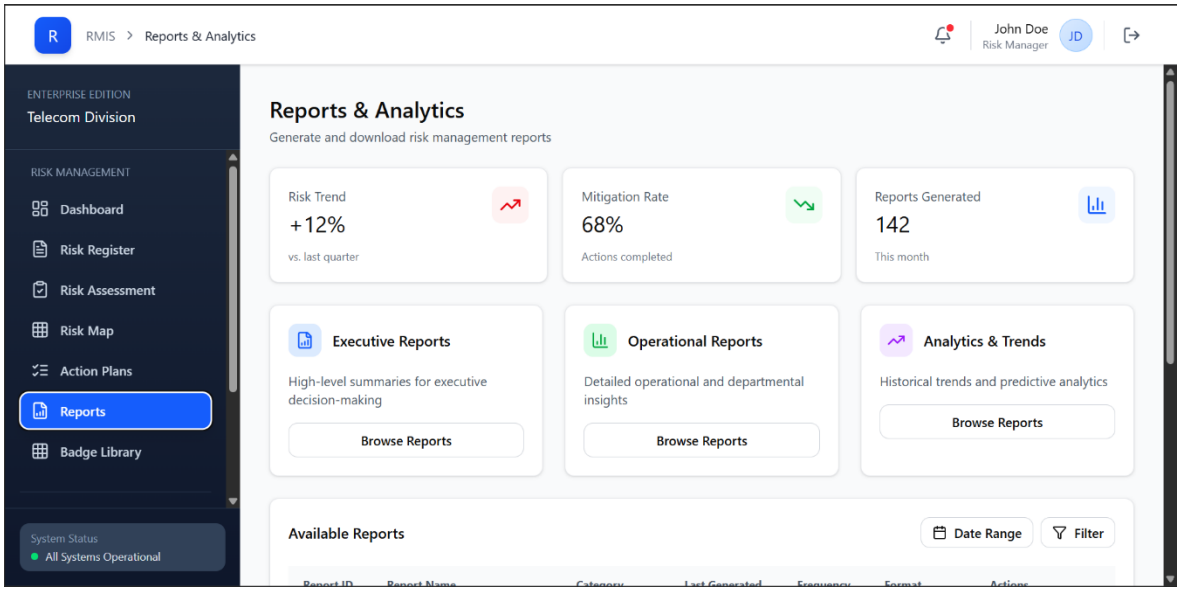


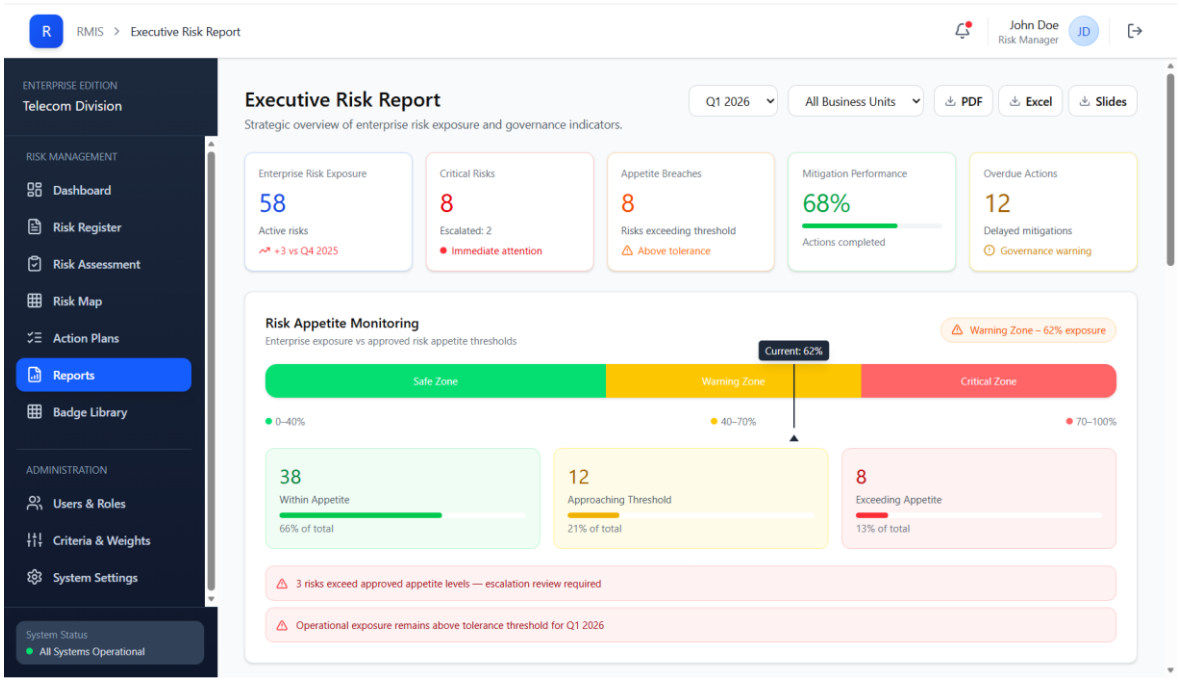

**Source:** Elaborated by authors (Figma prototype).

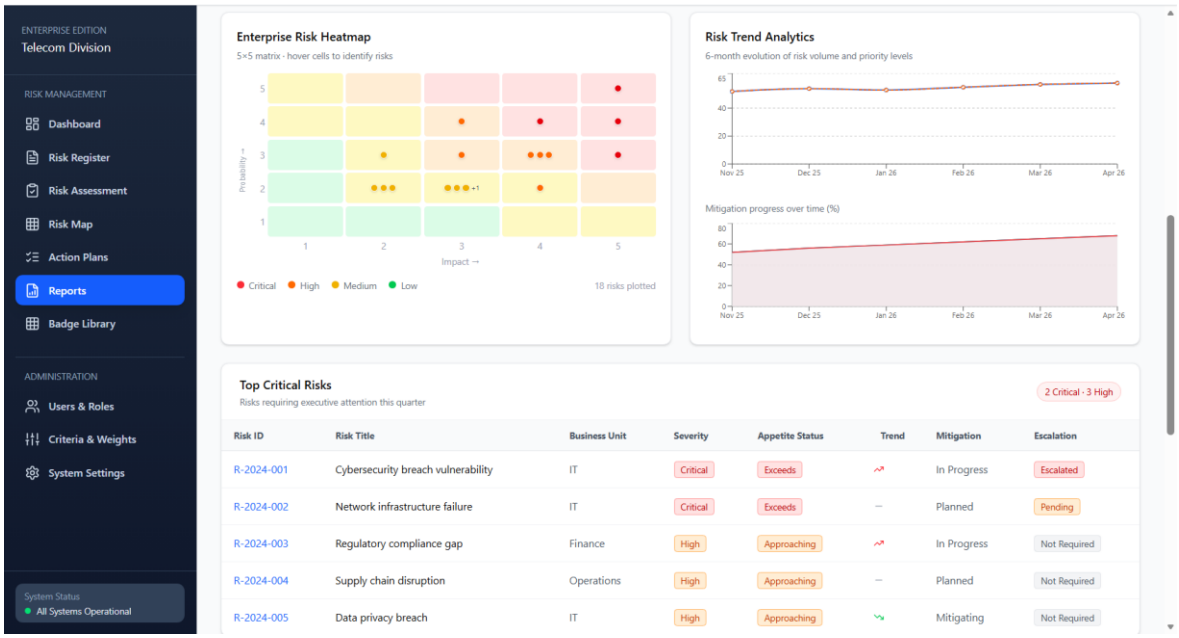
## The reports and analytics interface

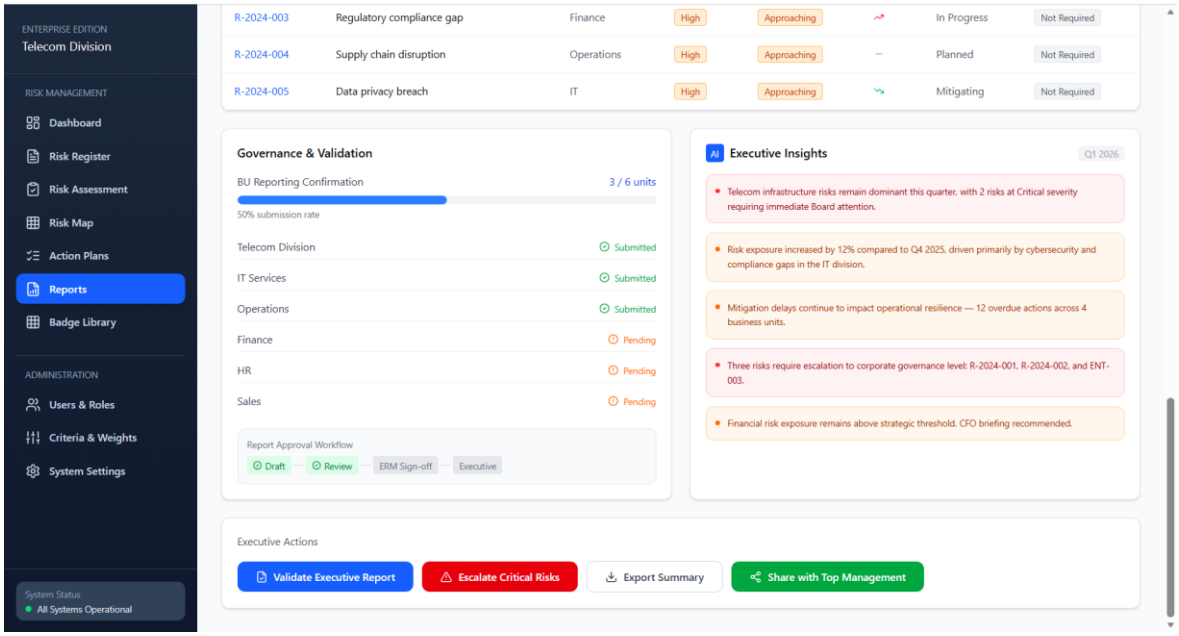
Figure 24 provides access to operational, executive, and general reports alongside trend analysis, risk appetite indicators, and the multi-step validation workflow.

***Figure 24: Reports and analytics interfaces***




RMIS > Executive Risk Report
John Doe
Risk Manager
ENTERPRISE EDITION
Telecom Division
RISK MANAGEMENT
Dashboard
Risk Register
Risk Assessment
Risk Map
Action Plans
Reports
Badge Library
ADMINISTRATION
Users & Roles
Criteria & Weights
System Settings
System Status
All Systems Operational
Executive Risk Report
Strategic overview of enterprise risk exposure and governance indicators.
Q1 2026
All Business Units
PDF
Excel
Slides
Enterprise Risk Exposure
58
Active risks
+3 vs Q4 2025
Critical Risks
8
Escalated: 2
Immediate attention
Appetite Breaches
8
Risks exceeding threshold
Above tolerance
Mitigation Performance
68%
Actions completed
Overdue Actions
12
Delayed mitigations
Governance warning
Risk Appetite Monitoring
Enterprise exposure vs approved risk appetite thresholds
Warning Zone – 62% exposure
Current: 62%
Safe Zone
Warning Zone
Critical Zone
0–40%
40–70%
70–100%
38
Within Appetite
66% of total
12
Approaching Threshold
21% of total
8
Exceeding Appetite
13% of total
3 risks exceed approved appetite levels — escalation review required
Operational exposure remains above tolerance threshold for Q1 2026

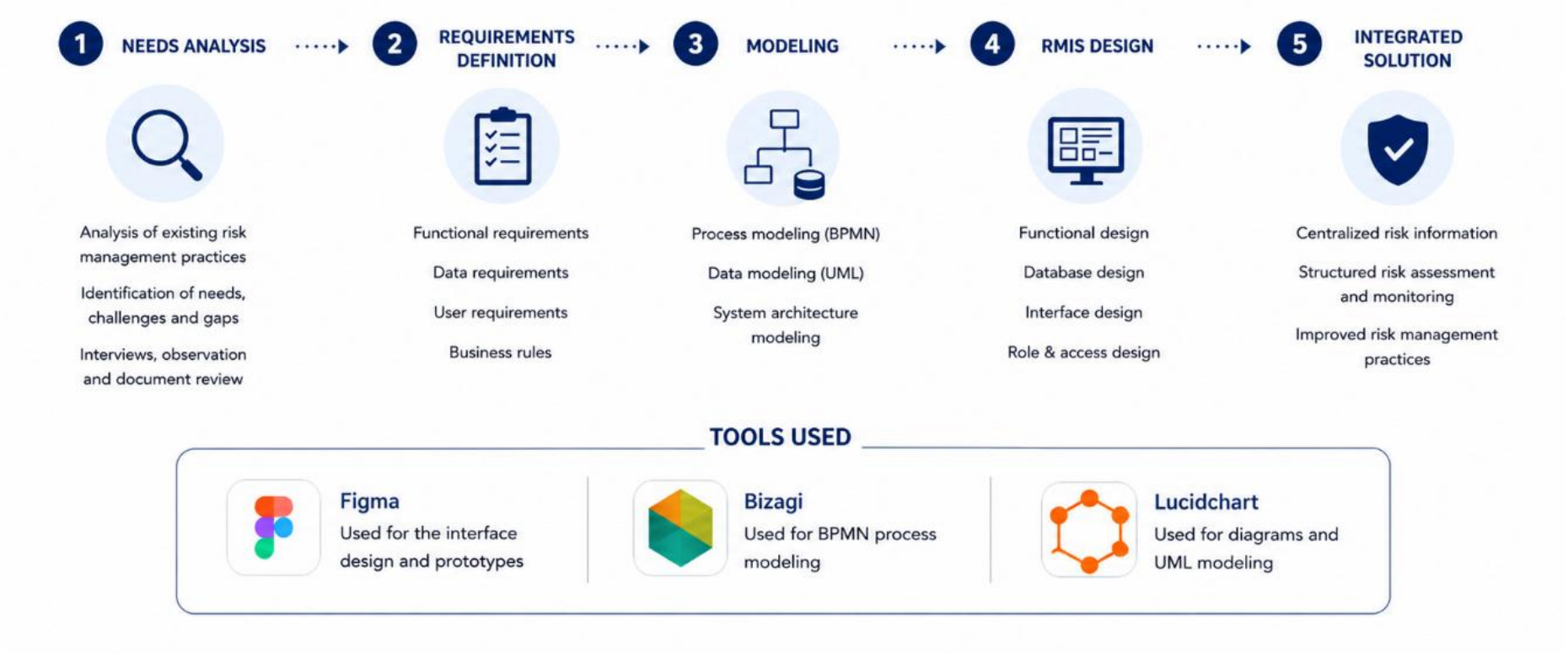

ENTERPRISE EDITION
Telecom Division
RISK MANAGEMENT
Dashboard
Risk Register
Risk Assessment
Risk Map
Action Plans
Reports
Badge Library
ADMINISTRATION
Users & Roles
Criteria & Weights
System Settings
System Status
All Systems Operational
Enterprise Risk Heatmap
5×5 matrix - hover cells to identify risks
Probability →
Impact →
Critical
High
Medium
Low
18 risks plotted
Risk Trend Analytics
6-month evolution of risk volume and priority levels
Nov 25
Dec 25
Jan 26
Feb 26
Mar 26
Apr 26
Mitigation progress over time (%)
Top Critical Risks
Risks requiring executive attention this quarter
2 Critical · 3 High
Risk ID
Risk Title
Business Unit
Severity
Appetite Status
Trend
Mitigation
Escalation
R-2024-001
Cybersecurity breach vulnerability
IT
Critical
Exceeds
In Progress
Escalated
R-2024-002
Network infrastructure failure
IT
Critical
Exceeds
Planned
Pending
R-2024-003
Regulatory compliance gap
Finance
High
Approaching
In Progress
Not Required
R-2024-004
Supply chain disruption
Operations
High
Approaching
Planned
Not Required
R-2024-005
Data privacy breach
IT
High
Approaching
Mitigating
Not Required




**Source:** Elaborated by authors (Figma prototype).

The RMIS design process is illustrated in the figure below:

*Figure 25: RMIS design workflow and modeling tools*




**Source** : Elaborated by authors.

# Conclusion

**Synthesis of findings**

This research is conducted within the broader context of digital transformation, where organizations are increasingly required to adapt their management practices to more complex, dynamic, and data-driven environments. In such a context, risk management has become a strategic function, particularly in sectors highly dependent on information systems, such as telecommunications. However, traditional approaches remain largely fragmented and insufficiently integrated, limiting their effectiveness and their contribution to organizational performance.

Accordingly, this study addresses the following central research question: "*How to design a system architecture to structure, centralize, and improve risk management within a complex organization like Ooredoo?"* This question reflects the need to move beyond conventional tools and to develop an integrated, system-based approach capable of supporting both operational and strategic risk management.

The study conducted within Ooredoo Algeria, based on semi-structured interviews, direct observation, and documentary review, has highlighted several key findings regarding current risk management practices. On the one hand, the organization demonstrates a relatively mature Enterprise Risk Management (ERM) framework aligned with international standards, particularly ISO 31000:2018. This maturity is reflected in structured processes, the existence of a risk register, and the involvement of multiple stakeholders across business units.

On the other hand, the study reveals that these practices remain highly dependent on fragmented tools and manual processes, such as Excel-based tracking and email-based communication. This fragmentation limits data centralization, reduces real-time visibility, and weakens the overall traceability of risk-related information. It also generates operational inefficiencies, particularly in data collection, reporting, and coordination between actors.
Three major insights emerge from this analysis:

- First, the current risk management system, although structured, lacks integration and automation, which constrains its ability to support timely and informed decision-making.
- Second, the absence of a centralized and shared information system limits transversal visibility and complicates the monitoring of risks across the organization.
- Third, stakeholders express a strong need for a digital solution capable of automating recurring tasks, improving communication, and ensuring reliable and real-time access to risk information.

**Answers to the research questions**

This study addressed the three sub-questions guiding the research.

- **Regarding RQ1**, the findings showed that risk management at Ooredoo Algeria is structured and aligned with international standards, but remains limited by fragmented tools and manual processes. This highlights the need for a centralized system ensuring better data integration, traceability, and coordination.
- **Regarding RQ2**, the research led to the design of a coherent RMIS architecture integrating processes, actors, and data flows. The use of BPMN and UML enabled the modeling of a structured system supporting the entire risk management lifecycle.
- **Regarding RQ3**, the integration of Multi-Criteria Decision-Making (MCDM) contributes to improving risk prioritization by incorporating multiple dimensions of risk evaluation, thereby enhancing the structuring and effectiveness of risk management practices.

Overall, the proposed RMIS provides a structured and integrated response to the identified needs and effectively addresses the three research sub-questions.

In this context, the proposed Risk Management Information System (RMIS), enriched by the integration of Multi-Criteria Decision-Making (MCDM) methods, appears as a relevant response to these identified limitations. It enables a more structured, coherent, and scalable approach to risk management.

**Contributions of the research**

This research contributes both to academic literature and managerial practices.

From a theoretical perspective, it enriches existing work at the intersection of risk management and information systems by proposing an integrated framework that combines ERM principles, information system design methodologies, and multi-criteria analysis. It highlights the importance of addressing both organizational and technological dimensions in the design of a Risk Management Information System.

From a methodological perspective, the research adopts a qualitative and abductive approach, enabling a comprehensive understanding of organizational practices while supporting the conception of a concrete and operational artifact. The use of thematic analysis, supported by NVivo, reinforces the rigor and transparency of the findings.

From a practical perspective, this work proposes the design and modeling of a Risk Management Information System (RMIS) tailored to the specific context of Ooredoo Algeria. It is grounded in an in-depth field analysis based on interviews, direct observation, and documentary review, which enabled the identification of concrete organizational needs and existing process limitations.

Building on these empirical insights, the identified requirements are translated into a coherent system design through the modeling of processes, actors, and data flows. Business processes were represented using BPMN with Bizagi Modeler, while UML diagrams were created using Lucidchart to structure system interactions and data elements. In addition, the user interface and system functionalities were conceptualized through interactive prototypes developed with Figma, providing a clear and realistic visualization of the system's operation and role-based access.

The proposed architecture supports the entire risk management lifecycle, while improving data centralization, traceability, and coordination between stakeholders. Furthermore, the integration of a multi-criteria approach contributes to a more structured and consistent evaluation of risks within the system.

Overall, this work goes beyond a purely conceptual contribution by offering a concrete, visualized, and operational design approach that can effectively support the future implementation of an integrated RMIS. More broadly, the findings demonstrate that while Ooredoo Algeria possesses a structured and standard-compliant risk management framework, its effectiveness remains constrained by the lack of integration and digitalization. In this sense, the proposed RMIS should not be viewed merely as a technological upgrade, but rather as a strategic transformation tool aimed at enhancing coordination, traceability, and the overall efficiency of risk management practices.

The integration of information systems and multi-criteria analysis into risk management processes offers a promising pathway toward more structured, transparent, and proactive risk governance. However, the success of such an initiative depends not only on technological choices but also on organizational readiness, stakeholder engagement, and the progressive alignment of practices with digital capabilities. Ultimately, the RMIS should be understood as a lever for continuous improvement, supporting the evolution of risk management from a compliance-oriented function toward a more integrated and value-creating component of organizational strategy.

**Recommendations**

Based on the findings, several recommendations can be formulated for Ooredoo Algeria:

- **Short-term actions**: Initiate the digitalization of risk management processes by standardizing data collection formats and introducing simple automation mechanisms (e.g., reporting templates, reminders, alerts). Strengthening awareness and training on risk culture among stakeholders is also essential.
- **Medium-term actions**: Develop a progressive roadmap for the implementation of the RMIS, starting with pilot functionalities such as the centralized risk register and automated reporting. Ensure strong involvement of business units and risk champions in the design and testing phases.
- **Key prerequisites**: Ensure interoperability with existing information systems, define a clear governance structure for the RMIS, and establish data management standards to guarantee consistency and reliability. Particular attention should also be given to access control and data security.

These recommendations should be implemented gradually, prioritizing actions with high added value and manageable complexity.

**Limitations and future research**

This research presents certain limitations that should be acknowledged. First, the study is conducted within the timeframe of a master's dissertation, which implies a cross-sectional perspective and does not capture the evolution of risk management practices over time. Second, the research focuses on a single organizational case, namely Ooredoo Algeria, which may limit the transferability of the findings to other contexts or sectors. Finally, the proposed RMIS remains at a conceptual and modeling stage, without empirical implementation or real-world testing, which does not allow for a full assessment of its operational performance.

Future research could extend this work by conducting empirical validation through the implementation of a pilot RMIS within Ooredoo or similar organizations. Comparative studies across different sectors could also provide broader insights into RMIS design and adoption. Additionally, further exploration of advanced analytics, artificial intelligence, or predictive risk models could enhance the system's capabilities.

Overall, this research demonstrates that while Ooredoo Algeria possesses a structured and standard-compliant risk management framework, its effectiveness remains constrained by the lack of integration and digitalization. The proposed RMIS does not represent merely a technological upgrade, but rather a strategic transformation tool aimed at enhancing coordination, traceability, and the overall efficiency of risk management practices.

The integration of information systems and multi-criteria analysis into risk management processes offers a promising pathway toward more structured, transparent, and proactive risk governance. However, the success of such an initiative depends not only on technological choices but also on organizational readiness, stakeholder engagement, and the progressive alignment of practices with digital capabilities.

Ultimately, the RMIS should be understood as a lever for continuous improvement, supporting the evolution of risk management from a compliance-oriented function toward a more integrated and value-creating component of organizational strategy.

## Bibliography


Al Lawati, A., Hussin, B. M., Abdul Kadir, M. R., & Khudari, M. (2025). The Relationship Between Enterprise Risk Management, Competitive Advantage, and Firm Performance. *Journal of Information Systems Engineering and Management*, *10*, 50s.

Al-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629

Ali, I. M. (2024). *A Guide for Positivist Research Paradigm: From Philosophy to Methodology*. *9*(2), 187–196. https://doi.org/https://doi.org/10.24191/idealogy.v9i2.596

Almutairi, A. T., & Saleh, K. (2026). *RiskMIS: A Web-Based Risk Management Information System*. *17*(2).

Aven, T. (2016). *Risk assessment and risk management: Review of recent advances on their foundation*. *253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems*, *11*(5), 218. https://doi.org/10.3390/systems11050218

Basel Committee on Banking Supervision. (2005). *International Convergence of Capital Measurement and Capital Standards: A Revised Framework* (p. 284). Bank for International Settlements (BIS). https://www.bis.org/

Bernstein, P. L. (1996). *Against the Gods: The Remarkable Story of Risk*. John Wiley & Sons.

Berrada, H., Boutahar, J., & El Ghazi El Houssaini, S. E. G. (2023). *Roadmap and Information System to Implement Information Technology Risk Management*. https://doi.org/10.18280/ijsse.130602

Caylor, J. P., & Hanratty, T. P. (2020). *Survey of Multi-Criteria Decision-Making Methods for Complex Environments* (Technical Report ARL-TR-9054; p. 41). U.S. Army Research Laboratory (DEVCOM Army Research Laboratory).

Chaube, S., Pant, S., Kumar, A., Uniyal, S., Singh, M. K., Kotecha, K., & Kumar, A. (2024). An Overview of Multi-Criteria Decision Analysis and the Applications of AHP and TOPSIS Methods. *International Journal of Mathematical, Engineering and Management Sciences*, *9*(3), 581–615.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise Risk Management: Integrating with Strategy and Performance*. COSO.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications. https://www.google.dz/books/edition/Research_Design/4uB76IC_pOQC

Efe, A. (2023). A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31000, COBIT. *Journal of Auditing and Assurance Services*, *3*(2), 185–205.

Eltarabishi, F., Omar, O. H., Alsyouf, I., & Bettayeb, M. (2020). *Multi-Criteria Decision Making Methods And Their Applications – A Literature Review*. 2654–2663.

Federation of European Risk Management Associations (FERMA). (2003). *Cadre de référence de la gestion des risques* (p. 16). FERMA. https://www.ferma.eu/

Hanine, M., Boutkhoum, O., Tikniouine, A., & Agouti, T. (2016). Application of an integrated multi-criteria decision making AHP-TOPSIS methodology for ETL software selection. *SpringerPlus*, *5*, 263.

Hofmann, R., Paavola, S., & Rainio, A. P. (2024). Abductive methodology: Opening the mystery of generating theory through qualitative inquiry in practice settings. *Participation, Collaboration and Co-Creation: Qualitative Inquiry across and beyond Divides*, 74–83. https://tinyurl.com/HofmannPaavolaRainio2024

Hopkin, P. (2017). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management* (4th ed.). Kogan Page.

Institute of Internal Auditors (IIA). (2020). *The IIA's Three Lines Model: An Update of the Three Lines of Defense*. IIA.

International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Risk Management – Guidelines* (ISO 31000:2018). ISO.

Kenneth C, L., & Jane P, L. (2018). *Management Information Systems: Managing the Digital Firm* (15th edition). Pearson Education Limited.

Leung, A. C. Y., Liu, D. Y. W., Luo, X., & Au, M. H. (2024). A constructivist and pragmatic training framework for blockchain education for IT practitioners. *Education and Information Technologies*, *29*, 15813–15854. https://doi.org/https://doi.org/10.1007/s10639-024-12505-5

Madanchian, M., & Taherdoost, H. (2025). Applications of Multi-Criteria Decision Making in Information Systems for Strategic and Operational Decisions. *Computers*, *14*(6), 208. https://doi.org/10.3390/computers14060208

Marín García, Á. (2023). Epistemological positions. In *The Routledge Handbook of Translation Theory and Concepts* (pp. 13–27). Routledge.

Metin, B., Duran, S., Telli, E., Mutlutürk, M., & Wynn, M. (2024). IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. *Information*, *15*, 55. https://doi.org/10.3390/info15010055

Pham, L. T. M. (2018). *Qualitative Approach to Research: A Review of Advantages and Disadvantages of Three Paradigms: Positivism, Interpretivism and Critical Inquiry* [Research Paper / Master Level Paper]. University of Adelaide.

Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Demos.

Quinn, S., Ivy, N., Barrett, matthew, Witte, G., & Gardner, R. K. (2022). *Prioritizing Cybersecurity Risk for Enterprise Risk Management* (NISTIR 8286B; p. 45). National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8286B

Recker, J., zur Muehlen, M., Siau, K., Erickson, J., & Indulska, M. (2009). *Measuring Method Complexity: UML versus BPMN*. Americas Conference on Information Systems (AMCIS). https://aisel.aisnet.org/amcis2009/541

Ruiz-Canela López, J. (2021). How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company? *Journal of Risk and Financial Management*, *14*, 139. https://doi.org/10.3390/jrfm14030139

Ryan, G. (2018). *Introduction to Positivism, Interpretivism and Critical Theory*. *25*(4), 41–49. https://doi.org/10.7748/nr.2018.e1466

Taherdoost, H., & Madanchian, M. (2023). *Multi-Criteria Decision Making (MCDM) Methods and Concepts*. *3*(1), 77–87. https://doi.org/https://doi.org/10.3390/encyclopedia3010006

Vasconcelos, A., Sousa, P., & Tribolet, J. (2003). *Information System Architectures: Representation, Planning and Evaluation*. *1*(6), 78–84.

Więckowski, J., Sałabun, W., Kizielewicz, B., Bączkiewicz, A., Shekhovtsov, A., Paradowski, B., & Wątróbski, J. (2023). Recent advances in multi-criteria decision analysis: A comprehensive review of applications and trends. *International Journal*

*of Knowledge-Based and Intelligent Engineering Systems*, *27*, 367–393. https://doi.org/10.3233/KES-230487

Yong, W. K., Husin, M. M., & Kamarudin, S. (2021). *Understanding Research Paradigms: A Scientific Guide*. *27*(2), 5857–5865. https://doi.org/10.47750/cibg.2021.27.02.588

Zachman, J. A. (1987). *A Framework for Information Systems Architecture*. *26*(3), 276–292. https://doi.org/https://doi.org/10.1147/sj.263.0276

Zachman, J. A. (2009). *Information Systems Infrastructure and Architecture*. https://doi.org/https://doi.org/10.3233/KES-230487

# Appendices

# Appendix A – Semi-structured interview guide

**Interview Guide**

**Analysis of practices and expectations regarding risk management information systems**

This interview is intended for risk management managers within the relevant departments at Ooredoo, as well as a few selected employees from other departments involved in these activities, in order to identify current practices, organizational needs, and expectations regarding the design of a risk management information system.

---

**Purpose of the study:**

As part of our master's thesis titled "Design and Modeling of a Risk Management Information System: A Multi-Criteria Mapping Approach—The Case of Ooredoo Algeria," conducted at the National Higher School of Management (ENSM), we are seeking your valuable input.

The study aims to identify current practices, understand organizational mechanisms, and gather stakeholder needs in order to contribute to the design of an information system dedicated to risk management.

Your responses will remain strictly confidential and will be used solely for academic research purposes. There are no right or wrong answers; we value your professional experience and

your authentic perspective.

We sincerely thank you for the time you are dedicating to this project.

---

**Interviewee profile**

- **Position:**
- **Department:**
- **Years of experience in risk management:**
- **Date and duration of the interview:**

---

**Questions**:

**Axis 1: Overview of risk management practices**

**Q1** — How is risk management currently organized within your department (stakeholders involved, responsibilities, and key steps in the process)?

**Q2** — What are the main types of risks identified in your department? Can you rank them in order of importance?

**Q3** — What tools and methods do you currently use to identify, assess, and monitor risks?

**Q4** — How is risk-related information recorded, tracked, and updated (media used, update frequency, responsible parties, etc.)?

**Q5** — How are risk reports produced and communicated to senior management (format, frequency, indicators used, etc.)?

**Axis 2: Assessment of the risk management framework's limitations and opportunities for improvement**

**Q1** — In your opinion, what are the main limitations or challenges of the current Enterprise Risk Management (ERM) process at Ooredoo Algeria?

**Q2** — What information do you believe is insufficient, missing, or difficult to access to support risk management decision-making?

**Q3** — How do you currently collaborate with other departments (IT, Finance, etc.) in the context of risk management?

**Q4** — What are the most time-consuming or repetitive tasks in your current ERM workflow?

**Q5** — If you could improve one aspect of the collection, processing, and sharing of risk information within the ERM framework, which would you prioritize?

**Axis 3: Risk assessment, prioritization, and mapping**

**Q1** — How are risks currently prioritized within the department, and what criteria are used to determine this prioritization?

**Q2** — What criteria do you generally use to assess the severity or criticality of a risk?

**Q3** — Do you currently use a visual tool or matrix to represent and communicate risks within the organization?

**Q4** — Do you believe that the current risk ranking method provides an objective and reliable picture of your risk portfolio?

**Q5** — What challenges do you face when attempting to compare or prioritize risks from different departments or categories?

**Axis 4: Target vision for an RMIS : Expectations, adoption, and organizational impacts**

**Q1** — What features do you consider essential in a Risk Management Information System (RMIS) to effectively support your department?

**Q2** — What types of information or indicators would you expect from such a system to support decision-making at the executive level?

**Q3** — To what extent is it important for this system to be integrated with other departments, such as IT and Finance…etc?

**Q4** — In your opinion, what are the necessary conditions for the successful adoption of a RMIS at Ooredoo Algeria?

**Q5** — In your opinion, what would be the impact of a well-designed RMIS on Ooredoo Algeria's organizational practices?

---

Thank you sincerely for your time and your valuable contribution to this research. Your insights will play a key role in shaping our work.

# Appendix B – Field observation grid of the risk management process

| Process | Risk Management Process (Observation Grid) | Date 20/04/2026 | Synthesis |
|---|---|---|---|
| **Category** | **Observations** | **Gaps / Remarks** | |
| **1. Risk Identification** | Risks are identified through disclosure by operational units during workshops, meetings, and feedback sessions. People are encouraged to share and talk about the risks they face in their activities and processes. This collection of inputs is essential to build a comprehensive risk inventory. | No process gap. Reliance on manual tools (Excel, Word, emails). Data collection depends heavily on people's engagement. | The observation of risk management practices at Ooredoo Algeria shows a high level of maturity and full alignment with ISO 31000:2018 and internal regulatory requirements. All key phases of the risk management process are implemented in a structured and proactive manner.<br><br>However, these practices rely heavily on manual tools (Excel, Word, Outlook), which results in time-consuming activities, data fragmentation, limited real-time visibility, increased operational workload, and a significant lack of risk culture within the organization.<br><br>The main limitation is therefore not related to the processes themselves, but to the lack of automation, system integration, and the absence of a strong risk culture.<br><br>An integrated Risk Management Information System (RMIS) is needed to automate workflows, centralize data, enhance traceability, support real-time monitoring, and improve reporting and communication efficiency.<br><br>***Note: There is a huge lack of risk culture within the organization. This makes the data collection phase the most complicated one, as the identification of risks requires the active collaboration of all departments with ERM.*** |
| **2. Risk Assessment** | Assessment based on impact/probability matrices in line with ISO 31000 and internal methodology. Use of scoring scales. | No methodological gap. Manual calculations and updates are time-consuming. | |
| **3. Risk Mapping** | Risk maps produced using standard templates (heat maps) and presented in periodic committees. | Static maps. No real-time updates or automatic consolidation. | |
| **4. Risk Monitoring** | Periodic monitoring through dedicated meetings and Excel-based tracking of KRIs and action plans. | No real-time tracking. Absence of alerts for threshold exceedances. | |
| **5. Risk Reporting & Communication** | Reports prepared manually using standardized templates. Dissemination mainly via Outlook (emails). | Manual reporting is time-consuming. Communication is fragmented and not integrated. | |
| **6. Incident Management** | Incidents are anticipated, recorded and followed up through structured procedures and risk registers. | No process gap. Lack of automation for tracking and escalation. | |
| **7. Documentation & Data Management** | Use of Office tools (Excel, Word, PowerPoint) for documentation and data storage. | Data is decentralized. Version control and traceability are limited. | |
| **8. Compliance & Regulatory Alignment** | Processes comply with ISO 31000:2018, internal policies, and group reporting requirements. | No compliance gap. Different internal vs. group reporting formats create duplication. | |
| **9. Information Systems Integration** | Limited integration between risk management and other corporate information systems. The ERM department lacks a centralized system to track risks, aggregate information, and collect data from risk owners across all departments. | Lack of interoperability and data consolidation. The ERM department lacks a centralized platform to track, gather, and consolidate risks from all risk owners. | |

# Appendix C – Matrix coding query

| Interviewee | A: Adoption Factors & Strategic Impact | B: Current Risk Management Landscape | C: RMIS Functional Requirements | D: System Limitations & Challenges |
|---|---|---|---|---|
| **Interviewee 4** | Automation of recurring tasks to free up time. Need for global and transversal risk visibility. Facilitation of periodic reporting processes. | No formalized internal process. Focus on compliance risk. Strong collaboration with ERM. Excel-based tracking and reporting. Alignment with ISO 31000:2018. | Automation of data collection and real-time alerts. Legal deadline alerts and regulatory change notifications. Prioritization of urgent risks. Simple and intuitive interface with reminders. | Regulatory complexity (external constraint). Need for better transparency and access to information. Manual data entry and reporting. Time-consuming reporting processes. |
| **Interviewee 1** | Integration into existing processes. Cultural transformation (real-time updates, collaboration). Significant time savings. | Strong collaboration (C-Level, BUs, Audit). ISO 31000-based structured process. Four risk categories (strategic, operational, financial, compliance). Mixed qualitative & quantitative methods. Use of Office tools and SharePoint. | Workflow automation. Dynamic data management and reporting automation. Integration into a single interface. Real-time communication. Customizable and secure system. | Lack of real-time information flow. Data collection difficulties (disclosure). Manual and time-intensive processes. Difficulty distinguishing emerging vs known risks. |
| **Interviewee 2** | Adoption depends on integration with existing | Risk identification based on context and ownership. Dual | Collaborative platform with notifications. Automated data | Weak risk culture. Decision-making inconsistencies with top management. |

| Interviewee | A: Adoption Factors & Strategic Impact | B: Current Risk Management Landscape | C: RMIS Functional Requirements | D: System Limitations & Challenges |
|---|---|---|---|---|
| | matrices. Emphasis on transparency and collaboration. | assessment (qualitative + quantitative). Use of tools (SWOT, PESTEL, Ishikawa, 5 Whys). Risk Register and quarterly reviews. Objective evaluation based on financial indicators. | collection and reporting. Error-free data entry and automated mapping. Visibility on risk assessment and mitigation progress. Strong system interconnection. | Heavy reporting workload. Governance complexity. Need for consistency across departments. |
| **Interviewee 3** | Stakeholder empowerment. Transparency toward ERM. Strengthening risk culture. | Intermediary role with ERM. Bottom-up risk identification process. Focus on operational risks (procurement, supply chain). Excel-based tracking and standardized reporting. | Shared digital platform for BUs. Role-based access (Viewer/Editor). Automated reporting templates. Support for collaboration and engagement cycles. | Lack of global risk visibility. Alignment challenges across departments. Limited access to strategic information. Repetitive reporting tasks. Need for real-time data instead of email-based communication. |