Journal of Organizations, Technology and Entrepreneurship
https://www.acadlore.com/journals/JOTE

Implementing Information Technology Risk Management: A Case Study in the African Airline Industry

Hasnaa Berrada*, Souhaïl El Ghazi El Houssaïni, Jaouad Boutahar

Systems Architectures and Networks Team, EHTP Ecole Hassania des Travaux Publics (Hassania School of Public Works), 8108 Casablanca, Morocco

* Correspondence: Hasnaa Berrada (berrada.hasnaa.cedoc@ehtp.ac.ma)

Received: 08-04-2023 **Revised:** 09-13-2023 **Accepted:** 09-21-2023

Citation: Berrada, H., El Ghazi El Houssaïni, S., & Boutahar, J. (2023). Implementing information technology risk management: A case study in the African airline industry. *J. Organ. Technol. Entrep.*, *1*(1), 58-76. https://doi.org/10.56578/jote010105.

Abstract: Recent financial scandals and crises have underscored the criticality of robust risk management practices, particularly in the realm of information technology (IT). This study explores the implementation of an Information Technology Risk Management (ITRM) system within an African airline, utilizing the RITM 23 methodological approach. RITM 23, a comprehensive framework, integrates standards from enterprise risk management (ISO 31000 and COSO ERM) and ITRM (COBIT 5), guiding organizations through framing the project, data collection, development of the ITRM system, and its subsequent communication and monitoring. The case study demonstrates the effective implementation of the RITM 23 framework, which led to the establishment of a complete environment for ITRM, inclusive of templates, tools, procedures, and governance processes. This implementation significantly enhanced the management of IT risks, mitigating potential catastrophic outcomes associated with unmanaged IT threats in the airline sector. The study concludes with a contemplation of future advancements, particularly the integration of artificial intelligence to further streamline and automate the ITRM process. This case study not only illustrates the successful application of RITM 23 but also sets a precedent for future ITRM implementations in similar sectors.

Keywords: Information Technology Risk Management (ITRM); Roadmap; Enterprise risk management; COBIT 5; ISO 31000; COSO ERM; Airline industry

1. Introduction

In the contemporary, ever-evolving global landscape, risk is a fundamental aspect of organizational operations (IBM, 2008). Various factors such as mergers and acquisitions, partnerships, globalization, and continual technological advancements are identified as key contributors to risk (IBM, 2008). These elements present challenges that organizations must navigate (Amansou, 2019). Consequently, there is an increasing emphasis on risk management within organizations, encompassing a spectrum of risks including human, commercial, economic, and political (Amansou, 2019).

The incorporation of information technology within businesses, while beneficial, necessitates the efficient management of IT-related risks to ensure the achievement of corporate objectives (Saeidi et al., 2019). ITRM is inherently linked to overall enterprise risk management, as IT-related risks can have significant impacts on the enterprise. This underscores the importance of a framework that integrates IT risks into enterprise risk management (Ernawati et al., 2012; Suroso & Rahadi, 2017).

The consequences of unmanaged IT risks on organizations can be severe. For instance, in 2017, an outage at Amazon Web Services disrupted numerous online services and websites, illustrating the risks associated with dependency on a single cloud service provider (Weise, 2017). Similarly, British Airways experienced an IT outage in 2017 due to a power surge, which impacted their aging IT infrastructure, leading to widespread flight cancellations and delays (Hern, 2017). Additionally, in 2016, Delta Air Lines faced significant operational disruptions and financial losses due to a power outage, highlighting the absence of a robust disaster recovery plan (CBS News, 2016).

To address the need for effective ITRM, various standards and guidelines have been established. COSO, renowned for its expertise in internal control, introduced in 2017 a version specifically designed for enterprise risk management (COSO ERM), although it does not directly address ITRM (COSO, 2013; COSO, 2017; Renard, 2012). ISO 31000, established in 2018, offers principles and guidelines for general risk management but also lacks specificity for ITRM (ISO, 2018; Sutra, 2018). Conversely, COBIT, primarily focused on IT management and governance, addresses ITRM in its COBIT 5 framework. COBIT 5 provides best practices for ITRM, yet its implementation can be challenging due to its complexity and lack of a simplified, holistic approach (ISACA, 2012a; ISACA, 2014; ISACA, 2013; Walid & Basil, 2015).

Despite the existing literature on the application of COBIT 5, ISO 31000, and COSO ERM for ITRM, a comprehensive, specialized framework remains elusive. For example, Kozina (2021) in *IT Risk Management in the enterprise using COBIT 5*, proposed a methodology for managing IT risks by integrating COBIT 5 with the Balanced Scorecard. This methodology focuses on identifying potential IT risks, assessing risk acceptance levels, and aligning business and IT objectives, specifically emphasizing risk identification, assessment, and response.

The academic discourse on ITRM has seen notable contributions that apply various frameworks and standards. In *Risk Assessment and Recommendation Strategy Based on COBIT 5 for Risk: Case Study SIKN JIKN Helpdesk Service* (Wulandari et al., 2019), the authors conducted a risk assessment for the SIKN JIKN helpdesk, employing COBIT 5 for risk, COBIT 5 Enabling Process, and COBIT 5 Framework guidelines. Their case study focused on the processes of DSS01 Manage Operations and APO12 Manage Risks. Notably, this method addressed only the risk assessment stage, omitting the EDM03 Ensuring Risk Optimization process, which is crucial for risk governance.

Furthermore, in *Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment* (Nugraha & Istambul, 2019), the authors explored the application of ISO 31000 to manage IT risks in a governmental setting. Their methodology encompassed stages such as Risk Identification, Risk Analysis, Risk Evaluation, and Risk Treatment, focusing on identifying and addressing potential IT threats and risks.

The exploration of ITRM in various sectors continues to be a prominent theme in recent academic research. In *Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework* (Putri & Wijaya, 2023), the focus is on the application of the ISO 31000 framework in Indonesian educational institutions. The methodology outlined in this study encompasses the phases of Risk Identification, Risk Assessment, and Risk Treatment, providing a tailored approach to managing IT risks in an educational context.

Similarly, in *A Study of Information Technology Risk Management of Government and Business Organizations in Thailand using COSO-ERM based on the COBIT 5 Framework* (Tangprasert, 2020), the research evaluates IT security control within Thai government and business organizations. This study integrates COSO ERM with COBIT 5, specifically focusing on the principles of Risk Identification, Risk Assessment, and Risk Response. This approach offers insights into the performance and efficacy of IT security controls in a cross-sectoral context.

The cited research articles, while contributing significantly to the field of ITRM, exhibit common limitations as summarized in Table 1:

Table 1. Comparison of research articles

Research Article	Risk Management Process					
	Governance Process			Management Process		
	Surveillance & Monitoring	Reporting	Communication	Risk Identification	Risk Assessment	Risk Treatment
(Kozina, 2021)	Missing	Missing	Missing	X	X	X
(Wulandari et al., 2019)	Missing	Missing	Missing	X	X	X
(Nugraha & Istambul, 2019)	Missing	Missing	Missing	X	X	X
(Putri & Wijaya, 2023)	Missing	Missing	Missing	X	X	X
(Tangprasert, 2020)	Missing	Missing	Missing	X	X	X

- Partial Coverage in Establishing ITRM: Each of the studies primarily concentrates on the initial stages of ITRM, such as Risk Identification, Risk Analysis, and Risk Treatment. This focus results in an incomplete portrayal of the ITRM process, as they do not fully develop or address the entire spectrum of ITRM and governance processes. This gap highlights the need for a more comprehensive approach that encompasses all stages of ITRM, from initial identification through to ongoing governance and monitoring.

- Absence of a Holistic End-to-End Approach: The studies lack a holistic, end-to-end approach to ITRM. This limitation is significant as it suggests that the research does not fully integrate or consider the interconnectedness of various risk management processes and their cumulative impact on the organization. A holistic approach would provide a more comprehensive understanding of IT risks, their interdependencies, and their overall impact on

organizational objectives.

To address the identified limitations in existing ITRM research, ongoing work by Berrada et al. (2021) aims to develop a holistic and simplified framework for ITRM. This work, encompassing publications such as *Simplified IT Risk Management Maturity Audit System Based on COBIT 5 for Risk*, *RITM 23: A System to an IT Risk Management Implementation* (Berrada et al., 2023), and *Roadmap and System to Implement Information Technology Risk Management: RITM 23 (process of publication in progress*, focuses on a novel approach called RITM 23.

RITM 23 is characterized as an integrated, holistic, and simplified methodological approach, combining standards like ISO 31000, COSO ERM, and COBIT 5. The primary objective of this article is to validate the efficacy of the RITM 23 approach, particularly in high-risk contexts such as the airline industry. The article presents a case study of RITM 23's implementation in an African airline, providing a practical demonstration of its application.

The structure of this article is as follows: The first section offers a concise overview of the RITM 23 methodological approach for establishing ITRM. This is followed by a detailed case study of its deployment in an African airline, with an analysis and comparison of the results against existing frameworks. Subsequent sections discuss the findings and highlight the contributions of the study. The final section concludes the paper and outlines future perspectives.

2. Methodology

The methodology section outlines the process of implementing Information Technology Risk Management (ITRM) in an African airline using the RITM 23 approach. RITM 23 was selected due to its holistic and simplified nature, specifically tailored for ITRM implementation. While other known standards such as COSO ERM, ISO 31000, and COBIT 5 exist for ITRM, they are either too generic or complex for specialized ITRM deployment.

RITM 23 is an integrated approach, constructed by amalgamating three key standards for Enterprise Risk Management (ERM) and ITRM: ISO 31000 (ISO, 2018), COSO ERM (COSO, 2017), and COBIT 5 (ISACA, 2012b; ISACA, 2013). Its holistic nature ensures comprehensive coverage of both management and governance processes essential for establishing ITRM in organizations.

The RITM 23 methodology encompasses five phases (see Figure 1):

(1) Project Scoping: This initial phase involves framing and organizing the project. Key activities include defining stakeholders, scheduling, and selecting methodological tools.

(2) Data Collection and Analysis: The second phase focuses on gathering IT risk data and organizing it by risk category, laying the groundwork for subsequent phases.

(3) Development of the ITRM System: In this phase, the identified IT risks are mapped in relation to the organization, forming the core of the ITRM system.

(4) Change Management, Communication, and Awareness: This phase aims to cultivate a risk-aware culture within the organization. It involves disseminating information about IT risks to enhance their effective management.

(5) Tracking and Monitoring: The final phase entails continuous tracking and monitoring of IT risks, enabling timely and effective responses to limit losses from IT-related events.

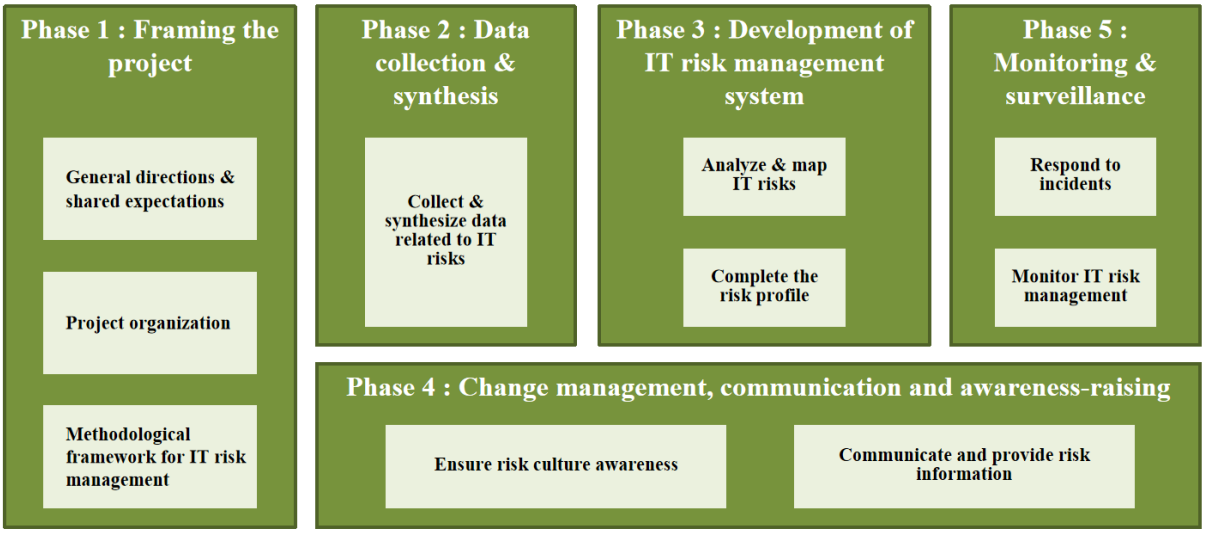

Figure 1. RITM 23 approach to implement ITRM

To assist in the implementation of Information Technology Risk Management, a simplified guide is provided in the appendix.

For comprehensive details on the proposed methodology, readers are encouraged to consult the article *RITM 23: A System to an IT Risk Management Implementation* (Berrada et al., 2023). This publication offers an in-depth exploration of the RITM 23 approach, contributing valuable insights into the field of ITRM.

The case study was undertaken at a prominent African airline, referred to as "Fly Africa" for confidentiality purposes. Fly Africa operates across Africa, Europe, Asia, and America, boasting a medium-sized fleet and employing approximately 2,000 personnel. The airline adopts an enterprise risk management strategy aligned with the COSO framework, which is also instrumental in managing IT-related risks.

The methodology of the study encompassed a blend of internal interviews and analysis of both internal and external documentation. Specifically, data and information were gathered through the following means:

- Qualitative Interviews: A series of 20 interviews were carried out with internal stakeholders at Fly Africa. These interviews included discussions with business line managers, business process owners, the Chief Risk Officer, IT risk leader, and IT process owners. The aim was to obtain qualitative descriptions and insights into the internal risk management processes and perceptions.
- Internal Documentation Analysis: An extensive review of Fly Africa's internal documentation was performed. This included an examination of budget guidance documents, ITRM maturity audit reports, risk management methodological kits, activity reports, IT incident databases, IT risk mappings, process mappings, and dashboards of Key Risk Indicators (KRIs).
- Analysis of Industry Peers' Published Documents: To gain a broader industry perspective, published documents of industry peers were also analyzed. This included reviewing annual reports from Easyjet (2021), Ryanair (2020), International Airlines Group (IAG, 2021), and the Lufthansa Group (2021), as well as universal registration documents from the Air France KLM Group (2020), Air France KLM Group (2021) and Safran (2021).

3. Results

This section details the application of RITM 23 within the context of “Fly Africa.” Extracts from the results and outputs achieved during the deployment are presented below.

3.1 Framing the Project

3.1.1 General directions and shared expectations

Objectives and Expectations: An interview was conducted with Fly Africa's Director of Internal Control & Risk Management. The director emphasized that the primary objective was to deploy the RITM 23 approach for implementing an IT management system within the airline. Although COSO ERM was already in use for enterprise risk management, it did not fully address the specificities of IT-related risks. Hence, RITM 23 was chosen to evaluate its effectiveness compared to the existing framework. The project needed to align with the company's strategic directions, adhering to defined deadlines, quality standards, and budget constraints.

General Directions: According to the Strategic Director of Fly Africa, the airline's development strategy includes key strategic orientations:

- Optimization of the operating model.
- Growth in passenger revenue, particularly in the most profitable segments.
- Expansion of non-passenger and cargo revenues.
- Contribution to sustainable development.

Major Risks: The major risks facing Fly Africa were identified through an interview with the Director of Internal Control & Risk Management and an analysis of the annual risk management report. The airline operates in an environment characterized by:

- Macroeconomic and geopolitical risks.
- Risks specific to the air transport industry.
- Risks related to group processes.
- Legal risks.
- Market risks.

3.1.2 Organization of the project

The Director of Internal Control & Risk Management established the primary objectives and expectations for the project. Operational details were further defined in an interview with the Chief Risk Officer, who identified the project team members, key stakeholders, and the project timeline.

Project Team: The project team is composed of various organizational functions integral to the deployment of the RITM 23 approach, participating in all stages of the project. The team includes:

- Chief Risk Officer: As the head of the risk management entity, the CRO is responsible for steering and coordinating the project and ensuring adherence to the methodological approach.

- IT Risk Leader: Tasked with deploying the proposed methodological approach.
- IT Process Owners: Providing necessary business expertise in IT for the project's deployment.

Stakeholders: Successful deployment of the roadmap requires the involvement of stakeholders beyond the project team, who will offer support and expertise in their respective areas. These include:

- Business Line Managers: Responsible for steering the project, making decisions, and assisting in disseminating the risk culture throughout the organization.
- Business Process Owners: Offering business expertise in their specific fields.

Project Schedule: The RITM 23 deployment involves five consecutive phases, with an exception for phase 4, which starts alongside phase 2 and continues through phase 5. The planning is benchmarked against similar projects, with phase 3 typically requiring more time than phases 1 and 2 to adequately develop the ITRM system. A three-month execution schedule is anticipated for the project (as depicted in Figure 2). However, phases 4 and 5 are expected to continue beyond the project's formal conclusion.

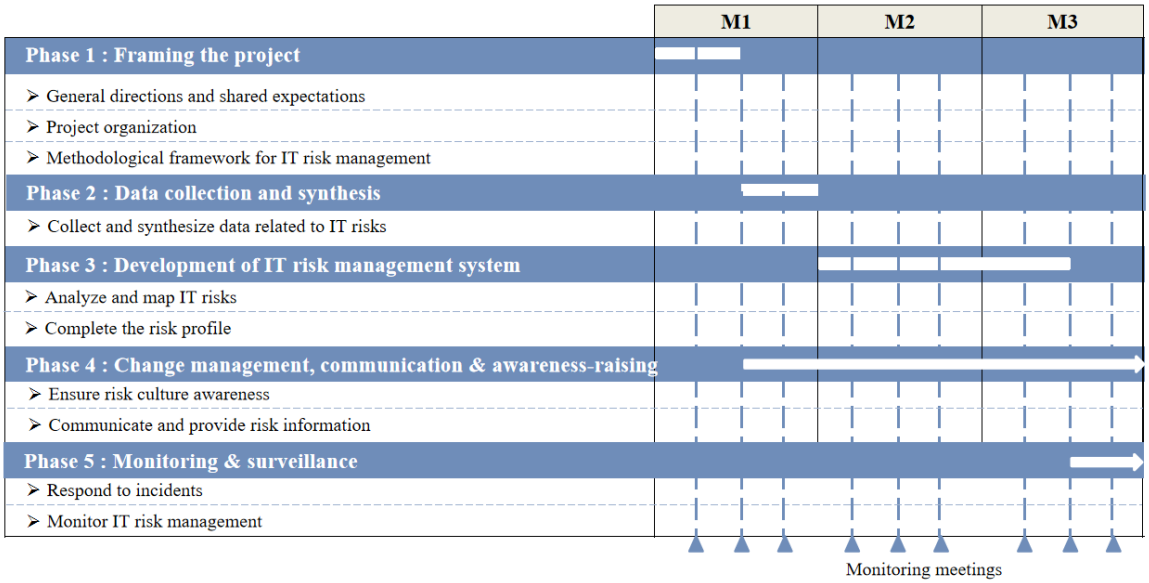

Figure 2. Schedule of the project: deployment of the RITM 23 in the context of Fly Africa

3.1.3 Methodological framework for ITRM

The ITRM methodological framework within the RITM 23 approach is designed to determine the appropriate scales for evaluating risk parameters, such as likelihood, impact, control effectiveness, and criticality. The framework proposes three options for rating scales to cater to the specific needs of each organization: 4-level, 5-level, or 6-level scales.

For Fly Africa, the decision was made to adopt a 5-level scale to align with the existing scales used in the airline's global risk management system, as suggested by the Director of Internal Control & Risk Management and the Chief Risk Officer. This alignment ensures consistency across different risk management domains within the organization.

Likelihood Rating Scale: The adopted likelihood rating scale (illustrated in Figure 3) consists of 5 levels of qualitative assessment. These levels range from level 1, indicating the lowest likelihood, to level 5, signifying the highest likelihood of risk occurrence.

Scale	Description
1	Very low / rare
2	Low / Unlikely
3	Medium / Possible
4	High / Likely
5	Very high / Almost certain

Figure 3. Likelihood rating scale (Fly Africa)

Impact Rating Scale: Similarly, the impact rating scale (shown in Figure 4) also features 5 levels of qualitative assessment. This scale ranges from level 1, representing the lowest level of impact, to level 5, indicating the most significant impact.

Scale	Description
1	Very low/not significant
2	Low/Minor
3	Medium/Moderate
4	High/Significant
5	Very high/Very significant

Figure 4. Impact rating scale (Fly Africa)

Scale of Control Effectiveness: The scale for rating the effectiveness of controls (depicted in Figure 5) includes 5 levels of qualitative assessment. These levels vary from level 1, which denotes the least effective controls, to level 5, which represents the most effective controls in mitigating risks.

Scale	Description
5	Excellent
4	Good
3	Medium
2	Insufficient
1	Very insufficient

Figure 5. Scale of control effectiveness (Fly Africa)

Criticality Level: In the context of the RITM 23 approach, criticality is a measure directly linked to risk exposure, which is determined by the product of the risk's probability of occurrence and its impact. The criticality scale used at Fly Africa (illustrated in Figure 6) includes four distinct levels, regardless of the rating scales utilized for assessing probability of occurrence, impact, or control effectiveness. These levels are:

- Minor Risk: Represents the lowest level of criticality.
- Moderate Risk: Indicates a moderate level of criticality.
- Major Risk: Denotes a high level of risk but not the utmost severity.
- Critical Risk: Signifies the highest level of risk criticality.

These criticality levels are represented in the risk matrix as different colored zones, often referred to as temperature zones. They play a crucial role in defining the levels of risk acceptance and the corresponding risk treatment strategies. In Fly Africa's case, risks categorized as minor and moderate are deemed acceptable, whereas major and critical risks are considered unacceptable and necessitate mitigation.

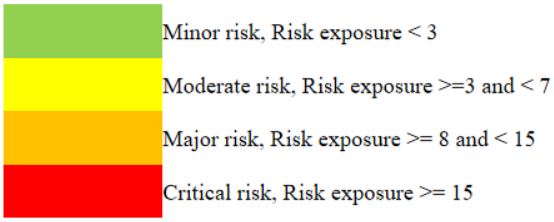

Figure 6. Criticality level (Fly Africa)

Risk Matrix: The risk matrix (shown in Figure 7) serves as a graphical representation of the organization's mapped risks. Each risk is plotted within the matrix based on its probability of occurrence and impact. The matrix is divided into several color-coded zones corresponding to the selected criticality levels:

- Red Zone: Indicates critical risks requiring immediate attention and action.
- Orange Zone: Represents major risks that are of significant concern but less urgent than critical risks.
- Yellow Zone: Encompasses moderate risks that are manageable within normal risk management processes.
- Green Zone: Includes minor risks, which are generally acceptable and require minimal intervention.

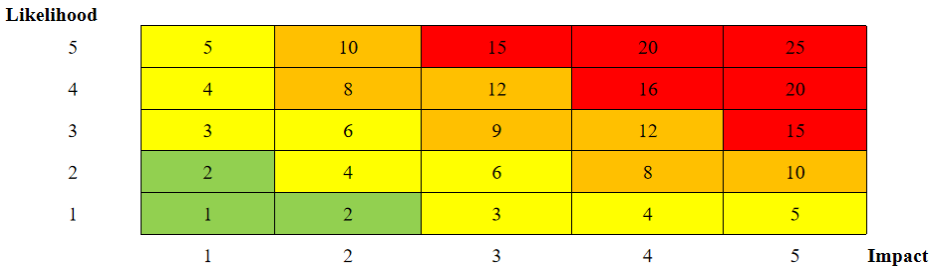

Figure 7. Template of risk matrix (Fly Africa)

3.2 Data Collection and Synthesis

Data for this study were meticulously gathered from a variety of sources, as illustrated in Figure 8. These sources included universal registration documents and annual reports of industry competitors, a range of internal documents from Fly Africa, and interviews with key stakeholders within the airline.

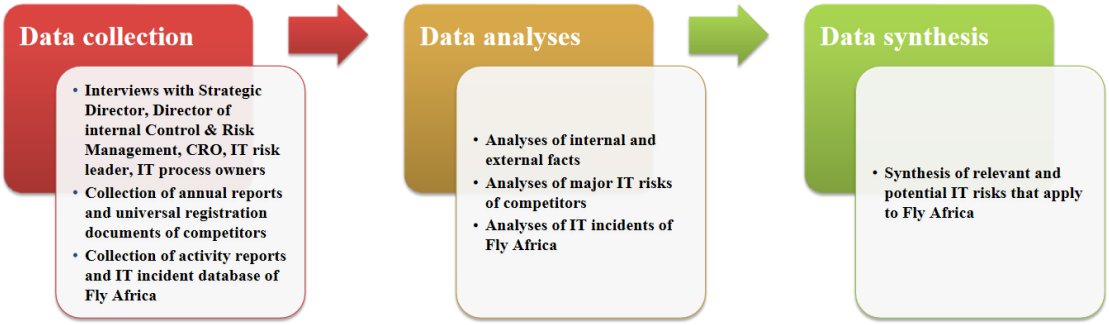

Figure 8. Process for data collection and synthesis

The comprehensive analysis of the collected data led to the development of a summary table (Table 2). This table methodically categorizes the risks and includes critical details such as the description of each identified risk, its specific category, the underlying risk factors, and assessments of both the likelihood and impact of each risk according to the predefined scales.

Table 2. Extract from the summary table of IT risks to be included in Fly Africa's IT risk mapping

Risk	Category	Risk Factor	Likelihood	Impact
Business continuity compromised	Infrastructure / Software	Various origins: internal or external to the Group: cyber-attacks, failure of equipment, infrastructures and IT services, failure of suppliers	4	5
Data security breach	Information (data breach, data leakage and access)	Lack of management of personal data collected from customers and employees. Frequent changes in applications and processes.	5	5
Cybercrime	Malware	Intensive reliance on information and communication technologies	5	5

3.3 Development of ITRM System

3.3.1 Analyze and map IT risks

The process of risk mapping for Fly Africa encapsulated a comprehensive identification and specification of various IT risk attributes. These included factors such as risk sources, potential consequences, existing control activities, associated macro and specific processes, risk categories, KRIs, control effectiveness, likelihood and

impact of each risk, and potential risk response options.

To construct the IT risk map for Fly Africa, a multifaceted approach was adopted. This approach involved utilizing standard IT risk scenarios as defined in COBIT 5, conducting detailed interviews with the project team members, analyzing pre-existing IT risk mappings at Fly Africa, and integrating potential IT risks identified in phase 2. Additionally, the steps outlined in the RITM 23 approach were meticulously followed (as illustrated in Figure 9), ensuring a systematic and thorough development of the ITRM system.

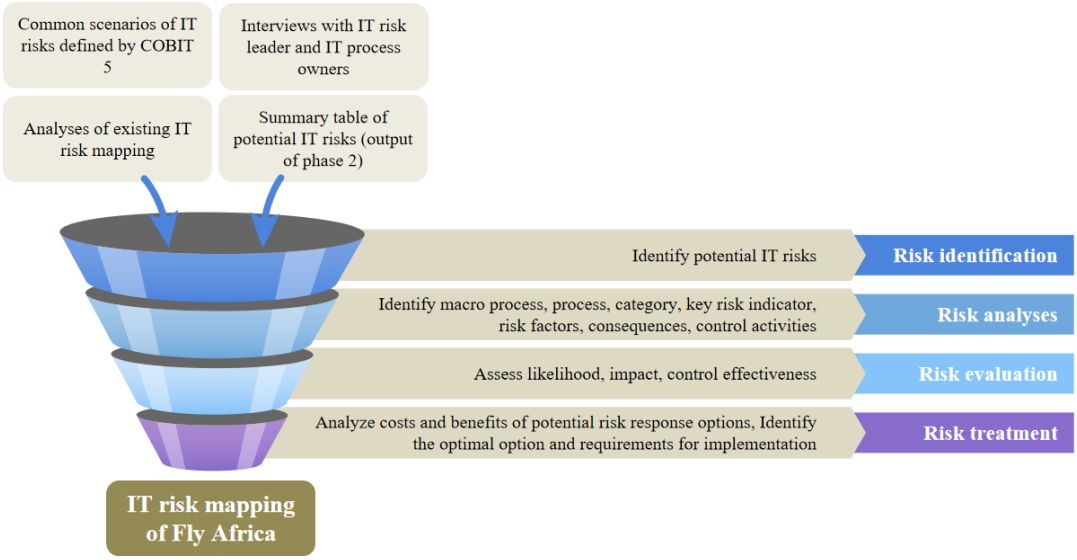

Figure 9. Process of production of IT risk mapping of Fly Africa

Some examples of IT risks identified by Fly Africa are described in Table 3.

Table 3. Some examples of IT risks identified by Fly Africa

Macro-Process	Process	Category	Risk
Information systems operations	Information systems security management	Malware	Company data is stolen following unauthorized access obtained through a phishing attack.
Information systems operations	IT development management	Portfolio setup and management	Inappropriate programs are selected for implementation and are not aligned with the company's strategy and priorities.
Information systems operations	IT development management	Program/ project lifecycle management	An IT project's budget has been exceeded.
Information systems management	IT budget management	IT investment decision-making	Company managers or representatives are not involved in important decisions concerning IT investments (e.g., new applications, prioritization, new technological opportunities).
Information systems management	IT human resources management	Expertise and skills in IT	There is a lack of inadequacy of IT-related skills within IT, for example due to new technologies.
Information systems management	IT human resources management	Staff operations	IT equipment is accidentally damaged by staff.
Information systems operations	Information systems security management	Information	Hardware components are damaged, leading to (partial) data destruction by in-house staff.
Information systems operations	Hardware and software management	Architecture	The company's architecture is complex and inflexible, hampering its evolution and expansion, and missing out on business opportunities.
Information systems operations	Hardware and software management	Infrastructure	As new (innovative) infrastructures are installed, systems become unstable, leading to operational incidents.
Information systems operations	Hardware and software management	Software	Inability to use the software to achieve the desired results (e.g., inability to make the required changes to the business model or organization).

The following illustrates a detailed example of a risk, encompassing all the attributes that have been integrated into the IT risk mapping for Fly Africa. This example is comprehensively documented in Tables 4, 5, 6, and 7.

Table 4. Extract from Fly Africa's risk mapping - part 1

Macro-Process	Process	Category	Risk	KRI
Information systems operations	Information systems security management	Malware	Company data is stolen following unauthorized access obtained through a phishing attack.	No. of attacks

Part 1 of the risk mapping extract illustrates the relationship of the identified risk to specific processes and macro-processes within Fly Africa. It also details how the risk is categorized, including a precise risk indicator for a comprehensive understanding of its context and relevance.

Table 5. Extract from Fly Africa's risk mapping - part 2

Risk Factor	Consequences	Control Activities
- Cyber attack - User error / lack of awareness - Misconfigured systems	- Operational disruption - Regulatory fines/sanctions - Loss of colleague/customer confidence	The IT infrastructure will be adequately protected by firewalls and continuous network monitoring to ensure day-to-day operations.

Part 2 of the risk mapping extract delineates the risk factors and the potential consequences of the identified risk, along with a description of the existing control activities in place.

Table 6. Extract from Fly Africa's risk mapping - part 3

Control Effectiveness	Likelihood	Impact	Exposition	Criticality Level
3	4	5	20	Critical

Part 3 of the risk mapping extract focuses on evaluating the likelihood and impact of the risk, as well as the effectiveness of existing controls. This assessment is crucial for calculating the overall risk exposure, thereby determining the risk's criticality. In the provided example, the risk is assessed as critical, indicating the necessity for implementing a comprehensive risk mitigation plan.

Table 7. Extract from Fly Africa's risk mapping - part 4

Potential Risk Response Options	Cost of Potential Risk Response Option	Benefit of Potential Risk Response Option (Efficiency, Effectiveness, Exposure and Capacity)
Accept (3)	Low (3)	Low (1)
Avoid (NA)	NA	NA
Reduce (6)	Medium (2)	High (3)
Transfer (3)	High (1)	High (3)

Part 4 of the risk mapping extract is dedicated to evaluating potential risk response options. This evaluation includes scoring various response strategies, taking into account factors such as cost and benefit. In the example given, the favored risk response is one that represents a balance of medium cost and high benefit in its implementation.

3.3.2 Complete the risk profile

Mapping of Applications, Processes and It Infrastructures Related to Critical Sub-Processes: This section involves mapping applications, processes, and IT infrastructures that are related to critical sub-processes. It is essential to identify business processes, assess their criticality, and understand their interrelations with IT applications, processes, and infrastructures. In the case of Fly Africa, an existing business process mapping serves as a foundation. For each identified process, corresponding IT applications, processes, and infrastructures were defined. Critical processes were then pinpointed to facilitate the implementation of necessary action plans (as detailed in Table 8).

An illustrative case is the identification of the "Personnel Payroll Management" process within the "HR Operations" macro-process as critical. This necessitates the formulation of an action plan to ensure continuous availability and functionality of the system. Potential measures might include installing a backup server, implementing multi-level validation for the authorizations matrix, and appointing dedicated personnel for the functional and technical administration of the system.

Table 8. Extract from the mapping of applications, processes and IT infrastructures required for the operation of business processes, particularly critical ones (Fly Africa)

Macro Process	Process	App. IT	Process IT	Infra. IT	Process Critical?
HR Operations	Payroll management	HR Access	Functional and technical administration Authorization management Database management Maintenance management	Local server	Yes
HR Operations	Training management	HR Access	Functional and technical administration Authorization management Database management Maintenance management	Local server	No
HR Operations	Internal communication	Outlook & SharePoint	Functional and technical administration Authorization management Database management Maintenance management	Cloud	No

IT Incident Database: The IT incident database is a key tool in this process. It chronicles various IT incidents that have occurred, accompanied by detailed descriptions of each incident's characteristics. While Fly Africa already maintains such a database, it requires further enrichment with additional attributes like corresponding risks, both qualitative and quantitative estimated impacts, detailed action plans, and the progress of these plans.

Subsequently, an extract from the IT incident database is provided, showcasing these incidents along with their attributes (Tables 9 and 10).

Table 9. Extract from the IT incident database (Fly Africa) – part 1

Description of the Incident	Corresponding Risk	Date of the Incident	Root Causes
IT budget overrun for SAP FICO module implementation project	IT project budget overrun	05/20/2021	Unclear expression of needs Lack of technical expertise in ERP deployment
Following a system upgrade, interfacing problem between Fly Africa's sales system and the one of airlines in codeshare	Incorrect programs are selected for implementation and misaligned with corporate strategy and priorities	07/15/2020	Go-live before completion of functional and technical acceptance of evolution

Table 10. Extract from the IT incident database (Fly Africa) – part 2

Estimated Impact	Estimated Impact in Numbers (MAD)	Action Plan Implemented in Response to the Incident	Action Plan Progress
High / Significant	9 million MAD	Identification of a task force made up of business and IT experts	100%
		Include the project in a PMO approach for better follow-up	100%
High / Significant	5 million MAD	Redeployment of the previous saved version of the sales system	100%
		Relaunch of functional and technical acceptance tests for the new solution	10%

The essential attributes to be defined for each incident in the IT incident database are as follows:

- Linking to Risk: This attribute establishes a connection between the incident and its associated risk. This linkage is vital for updating the probability of the risk, its impact, and the effectiveness of existing controls as the situation surrounding the incident evolves.
- Incident Causes: Identifying the root causes of the incident is crucial for developing an effective action plan. This involves understanding the underlying factors that led to the incident, thereby enabling targeted response strategies.
- Incident Impact: Assessing the impact of the incident is key to determining its criticality and overall significance. This evaluation helps in gauging the extent of the incident's effect on the organization's operations and objectives.
- Action Plan: Formulating an action plan is necessary not only to mitigate the impact of the current incident but also to reduce the likelihood of similar incidents occurring in the future. This plan should include specific steps and measures tailored to address the identified causes and impacts of the incident.

3.4 Change Management, Communication, and Awareness-Raising

3.4.1 Ensure risk culture awareness

Communication Plan: The communication plan outlines a series of actions designed to highlight the significance of ITRM within the organization. It specifies the objectives of these actions, identifies the target audience, assigns responsibility for implementation to specific individuals, sets deadlines for completion, and tracks the rate of progress for each action.

The following is an example of a communication campaign (Table 11).

Table 11. Extract from the communication plan (Fly Africa)

Communication Action	Objective	Target	In Charge of Action	Deadline	% Action Progress
ITRM e-learning course	Understand the basic concepts of ITRM Get to know the RITM 23 methodological approach	All employees	Risk management function & training function	12/2022	10%
IT flash risk	Communicate periodically about critical and major IT risks and how to prevent them	All employees	Risk management function & training function	Monthly	50%

Risk Reporting Procedure: This procedure is a crucial component of ITRM, detailing the process and information to be reported and communicated regarding IT risks to relevant stakeholders. The risk reporting procedure developed for Fly Africa encompasses several key elements:

- Objective
- Scope
- Management rules
- Key stakeholders
- Flowchart
- Detailed process description

KRI Dashboard: An essential tool in ITRM, the KRI dashboard facilitates the monitoring of KRIss, enabling the ongoing updating of risk mapping to reflect changes in risk probability and impact. The dashboard, detailed in Table 12, includes:

- A listing of all KRIs defined in the IT risk mapping (output of phase 3).
- Specific calculation formulas for each KRI.
- Identification of the entity responsible for producing each KRI.
- A description of the process for obtaining, transmitting, and updating these indicators.
- The frequency with which these indicators are measured and reviewed.

Table 12. Extract from the KRI dashboard (Fly Africa)

KRI	Corresponding Risk	Calculation Formula	Producing Entity	Acquisition and Transmission Process	Measurement Frequency
No. of attacks	Company data stolen through unauthorized access obtained by phishing attack	Count all successful attempts to access the company's networks	Information security unit	Immediately after the attack, all successful attempts are recorded in a tracking table, and the consolidated tracking table is transmitted at the beginning of each month.	Monthly

3.4.2 Communicate and provide risk information

IT Risk Analysis Report: A key element in communicating and providing information on IT risks to stakeholders is the IT risk analysis report. This report is meticulously crafted and filled with accurate data to effectively convey the state of IT risks within the organization.

The report aggregates various IT risk analyses that have been conducted. It is generated based on the IT risk mapping, which is an output of phase 3 of the RITM 23 process. To ensure that stakeholders are kept informed and can make timely decisions, the report is disseminated quarterly, or more frequently if requested, to business line managers and IT process owners.

Examples of some graphics can be seen in Figures 10, 11, and 12, which present various aspects of the IT risk landscape in an accessible and informative manner.

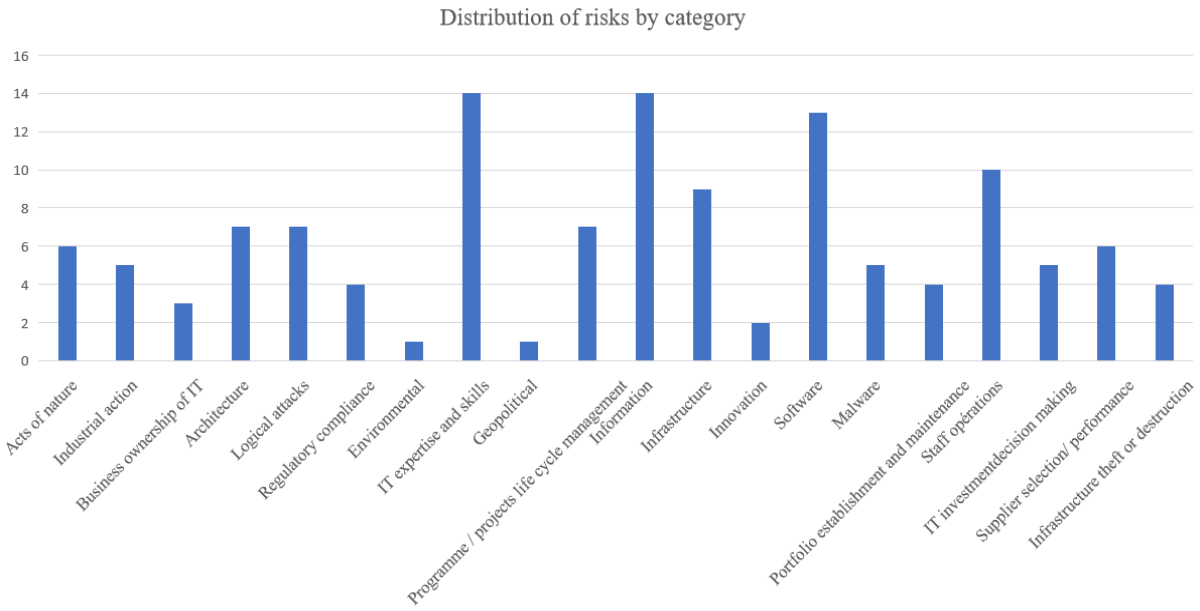

Figure 10. Distribution of IT risks by category (Fly Africa)

Figure 10 offers a detailed breakdown of risks by category, main categories containing a significant number of risks are: IT expertise and skills, information, software, personnel operations.

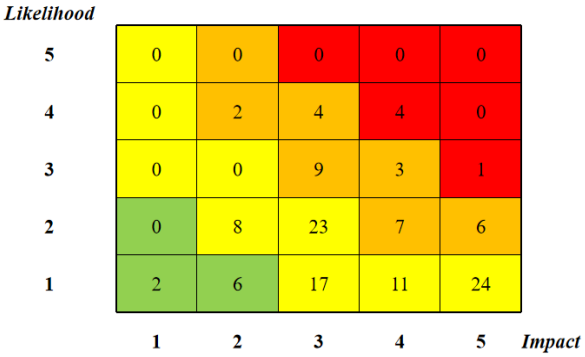

Figure 11. Net risk matrix (Fly Africa)

Figure 11 presents the risks categorized within the Farmer matrix. In this matrix, risks are divided into four distinct categories: 5 are identified as critical, 31 as major, 83 as moderate, and 8 as minor. The matrix provides a closer look at the critical and major risks, detailing the specific mitigation action plans that need to be implemented for these higher-priority risks.

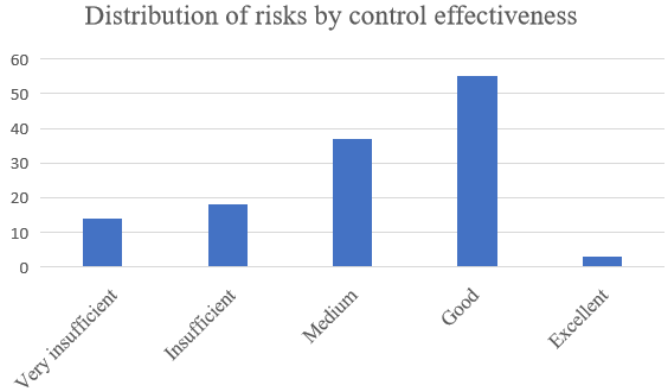

Figure 12. Breakdown of IT risks by effectiveness of existing controls (Fly Africa)

Figure 12 displays the distribution of risks based on the effectiveness of existing controls. It reveals that the majority of risks are managed with satisfactory controls. However, there are 32 risks identified with ineffective controls, highlighting the need for actions to enhance control effectiveness.

3.5 Monitoring and Surveillance

3.5.1 Respond to incidents

Business Continuity Plan (BCP): The BCP is a critical document devised by the organization to ensure the sustained operation of essential activities. Its primary function is to outline the strategy and necessary actions to be taken in the event of an IT incident that disrupts regular operations. The goal is to initiate a downgraded mode of operation, maintaining a minimum level of service, and to efficiently manage the recovery process and return to normal operations. For Fly Africa, the IT BCP was collaboratively developed by IT process owners, business process owners, and the risk management function. Following its development, the plan was subsequently validated by the business line managers. The IT BCP for Fly Africa includes several key sections:

- Define the organizational context
- Define the scope
- Management involvement and commitment
- BCP policy and objectives
- Provision of resources and skills
- Control and document management
- Organizational impact analysis
- Crisis and continuity management strategy
- Risk treatment strategies
- Exercises and tests

Incident Analysis Report: The report encompasses a range of analyses of IT incidents that have occurred within the organization. Compiled from the IT incident database, which is a deliverable of phase 3, this report is routinely communicated to business line managers and IT process owners on a quarterly basis or upon request. An extract from the incident analysis report is provided in Tables 13 and 14.

Notably, the initial analysis in this report classifies incidents based on the estimated impact of the damage, as detailed in Table 13.

Table 13. Fly Africa's IT incident ranking (top 3 extract)

Risk	Incident Description	Date of Incident	Estimated Impact
IT project budget overrun	IT budget overrun for SAP FICO module implementation project	05/20/2021	9 million MAD
Incorrect programs are selected for implementation and misaligned with corporate strategy and priorities.	Interfacing problem between Fly Africa's sales systems and codeshare airlines following a system upgrade	07/15/2020	5 million MAD
Company data is stolen by unauthorized access following a phishing attack.	Attempted intranet access via phishing email	05/20/2020	1 million MAD

Table 14. Extract from the analysis of IT incident causes and related action plan - Fly Africa

Incident Description	Root Causes	Action Plan Implemented in Response to the Incident	Action Plan Progress
IT budget overrun for SAP FICO module implementation project	Unclear expression of needs	Identification of a task force made up of business and IT experts	100%
	Lack of technical expertise in ERP deployment	Include the project in a PMO approach for better follow-up	100%
Interfacing problem between Fly Africa's sales systems and codeshare airlines following a system upgrade	Go-live before completion of functional and technical acceptance of evolution	Redeployment of the previous saved version of the sales system	100%
		Relaunch of functional and technical acceptance tests for the new solution	10%
Attempted intranet access via phishing email	Increase in cyber-attacks with the shift to remote working	VPN security for corporate network access	50%
		Awareness campaign against phishing e-mails	0%

The second analysis in the IT Incident Analysis Report delves into the causes that triggered each incident, as well as the action plans implemented to mitigate their impacts. This detailed analysis is presented in Table 14.

3.5.2 Monitor ITRM

This stage encompasses a series of actions undertaken for risk monitoring and surveillance. A risk monitoring report, compiled based on the outputs of the previous phases, is regularly communicated to business line managers and IT process owners, either quarterly or as requested. An extract from this report, including various graphs and tables, is represented in Tables 15, 16, 17, 18, and 19.

Table 15. Extract from the inventory of control activities and monitoring of risk mitigation plans - Fly Africa

Risk	Control Activities	Risk Mitigation Plan	Rate of Progress
Company data is stolen following unauthorized access gained through a phishing attack.	The IT infrastructure will be adequately protected by firewalls and continuous network monitoring to ensure day-to-day operations.	- Implement a data and cyber-risk governance structure to regularly review the data landscape and determine what actions need to be taken to effectively manage risks - Launch an employee awareness campaign and online training - Use intrusion detection tools to monitor infrastructure for unauthorized access, and ensure that any events are integrated into general event monitoring and incident management	20%

Table 15 in the risk monitoring report enumerates the control activities associated with each identified risk and tracks the progression of the corresponding mitigation plans. For critical and major risks, designated risk relays within the respective areas are tasked with initiating second-level controls to ascertain the effectiveness of the existing control activities.

Table 16. Extract from Fly Africa's KRI dashboard - part 1

KRI	Corresponding Risk	Measure 1	Target 1	Gap 1	Measure 2	Target 2	Gap 2
Number of cyber-attacks	Company data is stolen following unauthorized access gained through a phishing attack.	1	0	1	3	0	3

Table 17. Extract from Fly Africa's KRI dashboard - part 2

Measure 3	Target 3	Gap 3	Measure 4	Target 4	Gap 4	Explications of Gaps	Corrective Measures
0	0	0	3	0	3	Employee access to phishing emails	- Updating and strengthening detection and protection systems - Raising awareness of cyber-attacks and best practices for mitigating them

The KRI dashboard is designed to facilitate the monitoring of risk indicators in accordance with the specified frequency for each KRI. This tool enables the implementation of necessary corrective actions whenever deviations from the established targets are observed.

Table 18. Extract from Fly Africa's IT incident tracking table

Incident Description	Date of Incident	Estimated Impact	Quantified Impact	Corresponding Risk	Action Plan Implemented in Response to the Incident	Rate of Progress
Attempted intranet access via phishing email	05/20/2020	Very low / not significant	0	Company data is stolen by unauthorized access following a phishing attack.	Awareness campaign against phishing emails	100%

Within the scope of tracking and monitoring activities, the ongoing monitoring of recorded incidents plays a crucial role. This process allows for the assessment of the progress of the incident response plan, ensuring that the incident is effectively managed and under control. Additionally, incident tracking includes the task of updating the quantified impact of each incident, maintaining an accurate and current understanding of its ramifications.

Table 19. Extract from Fly Africa's objectives monitoring table

Identified Objectives	Corresponding Risk	Target (%)	% of Objectives Achieved	Gap Analysis
Improving IS security	Company data is stolen by unauthorized access following a phishing attack.	90%	50%	System for improving IS security currently being deployed

Monitoring and controlling risk also involves tracking the progress of objectives that are linked to identified risks. This is a key aspect of our risk management activities.

4. Discussion

The implementation of the RITM 23 approach at Fly Africa has culminated in the establishment of a comprehensive system for ITRM. This system encompasses both the management and governance processes of IT risks, transcending the conventional phases of identification, assessment, and treatment typically observed in existing research. Notably, RITM 23, an amalgamation of COSO ERM, ISO 31000, and COBIT 5 standards, facilitated a streamlined deployment, dovetailing with Fly Africa's existing COSO ERM-based methodological approach. The alignment of RITM 23 with these three standards has been instrumental in creating an environment tailored for ITRM, yielding pertinent and direct analyses.

Advantages of utilizing RITM 23 in comparison to existing frameworks are observed in various phases:

Project Framing: The extant framework permits only a 5-level rating scale. In contrast, RITM 23 introduces a flexible approach with three types of scales (4-level, 5-level, or 6-level) within its methodological framework, adaptable to organizational needs.

Data Collection and Synthesis: Absent in the existing framework, this phase in RITM 23 involves a thorough analysis of the organization's internal and external environment, identifying potential IT risks.

Development of ITRM System: In the existing framework, IT risk identification primarily relies on brainstorming by IT process owners. However, RITM 23 adopts a more comprehensive and structured approach for this purpose. This approach leverages generic COBIT 5 scenarios and incorporates an in-depth analysis of organizational specifics, external and internal factors, IT incidents, and competitor IT risk assessments. Unlike the existing framework, which utilizes generic risk categories, RITM 23 employs categories more tailored to IT concerns, such as Infrastructure/Software, Information (encompassing data breach, data leakage, and access issues), and Malware. Furthermore, RITM 23 enhances the risk profile by identifying critical business processes and correlating them with relevant IT applications, processes, and infrastructures. This alignment facilitates the development of action plans aimed at ensuring the continuous availability of these critical processes.

Change Management, Communication, and Awareness Raising: While an enterprise communication plan already exists, RITM 23 introduces a risk culture awareness tool specifically tailored to IT risks. This tool complements the existing framework, offering more frequent and detailed insights. In contrast to the annual production of the existing risk analysis report, the IT risk analysis report under RITM 23 is communicated quarterly. It features comprehensive analyses, including the categorization of IT risks, an evaluation of their net criticality, a focus on the top 10 IT risks, and an assessment of the ITRM process's effectiveness. The report also highlights IT risks with inadequate control effectiveness, particularly those with major or critical net criticality, and summarizes the findings of objective assessments, internal audits, and quality assurance reports, with special attention to IT risks escalating to major or critical status. Furthermore, unlike the annual update of IT risk mapping in the existing framework, RITM 23 mandates updates to the IT risk mapping with every new report or incident, ensuring a more dynamic and responsive ITRM process.

Monitoring and Surveillance: RITM 23 introduces the development of a BCP based on IT incidents, a feature absent in the existing framework. Unlike the current approach, which primarily maintains an IT incident database, RITM 23 utilizes an IT incident analysis report. This report categorizes IT incidents, aiding in the prioritization of necessary action plans. Additionally, RITM 23 fosters a more integrated approach to ITRM. Each component is interconnected, meaning changes in one area automatically trigger updates in related components. For instance, recording a new IT incident in the database directly leads to modifications in the IT risk mapping, ensuring a cohesive and responsive risk management system.

5. Conclusions

This article has delineated the successful implementation of Information Technology Risk Management (ITRM) at Fly Africa, utilizing the RITM 23 approach. This approach, integrating standards such as COSO ERM, ISO 31000, and COBIT 5, provided a holistic and streamlined method tailored for ITRM. The deployment process encompassed not only the ITRM processes but also extended to IT risk governance procedures.

The initial phase involved the project's conceptual framing, followed by the meticulous collection and

structuring of internal and external IT risk-related data. Subsequently, the development of the ITRM framework was undertaken. Concurrently, from the data collection phase through to the project's conclusion, efforts were concentrated on communication and awareness-raising activities in relation to ITRM. Finally, tools were prepared and continually updated for the effective monitoring of IT risk evolution.

A significant outcome of this implementation was the creation of a comprehensive IT risk mapping. This mapping proved more advantageous than the previous version, which was primarily derived from IT process owners' brainstorming without reference to an established IT risk database. The new IT risk analysis report, offering detailed and pertinent analyses, surpasses the existing framework in terms of frequency and content, enabling better ITRM. This report is designed for dynamic updating in response to changes impacting IT risks, as opposed to the annual updates of the previous report. Another noteworthy advancement is the integration of all ITRM data within the RITM 23 system, ensuring that any modification in one component automatically updates corresponding elements, thus providing a constantly current view of IT risk trends.

RITM 23 demonstrates its potential as a standalone framework suitable not only for aviation but also for other industries. Looking ahead, this methodological approach could be applied across various sectors to validate its efficacy further. Additionally, the implementation at Fly Africa highlighted the necessity for business process owners' expertise in executing the stages of the RITM 23 approach. Future iterations could explore the integration of Artificial Intelligence to further automate the approach and reduce reliance on IT experts. This potential advancement could significantly enhance the efficiency and effectiveness of ITRM implementation in diverse organizational contexts.

Data Availability

The data supporting our research results are under privacy or ethical restrictions. The data are available from the team project for researchers, who meet the criteria for accessing confidential data.

Conflicts of Interest

The authors declare no conflict of interest.

References

Air France KLM Group. (2020). *Document d'enregistrement universel 2019*. Paris: Air France KLM Group. https://www.edf.fr/sites/default/files/contrib/groupe-edf/espaces-dedies/espace-finance-fr/informations-financieres/informations-reglementees/urd/edf-urd-rapport-financier-annuel-2019-fr.pdf

Air France KLM Group. (2021). *Document d'enregistrement universel 2020*. Paris: Air France KLM Group. https://www.edf.fr/sites/default/files/contrib/groupe-edf/espaces-dedies/espace-finance-fr/informations-financieres/informations-reglementees/urd/edf-urd-rapport-financier-annuel-2020-fr.pdf

Amansou, S. (2019). Risk management: Theoretical underpinnings and critical analysis. *Insur. Risk Manag.*, *86*(2-3), 265-287. https://doi.org/10.7202/1068509ar.

Berrada, H., Boutahar, J., & El Ghazi El Houssaïni, S. (2021). Simplified IT risk management maturity audit system based on "COBIT 5 for Risk." *Int. J. Adv. Comput. Sci. Appl.*, *12*(8), 1.

Berrada, H., Boutahar, J., & El Ghazi El Houssaini, S. (2023). RITM 23: A system to an IT risk management implementation. In *2023 3rd International Conference on Innovative Research in Applied Science, Engineering and Technology* (*IRASET*), Mohamedia, Morocco (pp. 1-6). https://doi.org/10.1109/IRASET57153.2023.10152978.

CBS News. (2016). *Delta struggles to recover from system-wide delays, cancellations*. https://www.cbsnews.com/news/outage-causes-massive-delays-cancellations-for-delta-flights/

COSO. (2013). *Internal control - Integrated framework*. COSO Publication. https://www.coso.org/guidance-on-ic

COSO. (2017). *Enterprise risk management - Integrating with strategy and performance*. COSO Publication. https://www.coso.org/enterprise-risk-management

Easyjet. (2021). *Annual report and accounts 2020*. London, UK: Easyjet.

Ernawati, T., Suhardi, & Nugroho, D. R. (2012). IT risk management framework based on ISO 31000:2009. In *2012 International Conference on System Engineering and Technology* (*ICSET*), Bandung, Indonesia (pp. 1-8). https://doi.org/10.1109/ICSEngT.2012.6339352.

Hern, A. (2017). *British Airways IT failure: Experts doubt* "*power surge*" *claim*. The Guardian. https://www.theguardian.com/business/2017/may/30/british-airways-it-failure-experts-doubt-power-surge-claim

IAG. (2021). *Annual report and accounts 2020*. IAG (International Airlines Group). https://www.iairgroup.com/investors-and-shareholders/financial-reporting/annual-reports/

IBM. (2008). *Méthodologie de gestion du risque informatique pour les Directeurs des Systèmes d'Information:*

Un levier exceptionnel de création de valeur et de croissance. https://dokumen.tips/documents/5716-gben-prf-ibmcom-du-fait-de-lomnipresence-de-linformatique-dans.html?page=2
ISACA. (2012a). *COBIT 5: A business framework for governance and management of enterprise IT*. USA: ISACA Publication. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0
ISACA. (2012b). *COBIT 5: Enabling processes. USA: ISACA Publication*. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCIEA0
ISACA. (2013). *COBIT 5 for risk. USA: ISACA Publication*. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoAmEAK
ISACA. (2014). *Relating the COSO internal control - Integrated framework and COBIT*. ISACA COBIT Series White Paper.
ISO. (2018). *ISO 31000 - Management du risque.* ISO Publication.
Kozina, M. (2021). IT risk management in the enterprise using CobiT 5. In *Proceedings of the Central European Conference on Information and Intelligent Systems*, Varaždin, Croatia (pp. 249-256).
Lufthansa Group. (2021). *Annual report 2020*. Frankfurt: Lufthansa Group.
Nugraha, U. & Istambul, R. (2019). Implementation of ISO 31000 for information technology risk management in the government environment. *Int. J. Adv. Sci. Technol.*, *28*(6), 140-145.
Putri, N. L. & Wijaya, A. F. (2023). Information technology risk management in educational institutions using ISO 31000 framework. *J. Inf. Syst. Informatics*, *5*(2), 630-649. https://doi.org/10.51519/journalisi.v5i2.468.
Renard, J. (2012). *Comprendre et mettre en oeuvre le contrôle interne*. Paris, France: Eyrolles.
Ryanair. (2020). *Annual report 2019*. Ireland: Ryanair.
Saeidi, P., Saeidi, S. P., Sofian, S., Saeidi, S. P., Nilashi, M., & Mardani, A. (2019). The impact of enterprise risk management on competitive advantage by moderating role of information technology. *Comput. Stand. Interfaces*, 63, 67-82. https://doi.org/10.1016/j.csi.2018.11.009.
Safran. (2021). *Document d'enregistrement universel 2020*. France: Safran.
Suroso, J. S. & Rahadi, B. (2017). Development of IT risk management framework using COBIT 4.1, implementation in IT governance for support business strategy. Singapore: ICEMT.
Sutra, G. (2018). *Management des risques: une approche stratégique*. Afnor Editions.
Tangprasert, S. (2020). A study of information technology risk management of government and business organizations in Thailand using COSO-ERM based on the COBIT 5 Framework. *J. Appl. Sci.*, *19*(1), 13-24. https://doi.org/10.14416/j.appsci.2020.01.002.
Walid, A. A. & Basil, M. (2015). A code of practice for effective information security risk management using COBIT 5. In *the 2nd International Conference Information Security Cyber Forensics*, Cape Town, South Africa (pp. 145-151).
Weise, E. (2017). *Massive Amazon cloud service outage disrupts sites*. USA TODAY. https://www.usatoday.com/story/tech/news/2017/02/28/amazons-cloud-service-goes-down-sites-scramble/98530914/
Wulandari, S. A., Dewi, A. P., Pohan, M. R., Sensuse, D. I., Mishbah, M., & Syamsudin. (2019). Risk assessment and recommendation strategy based on COBIT 5 for risk: Case study SIKN JIKN Helpdesk service. In *the Fifth Information Systems International Conference 2019*, Jakarta, Indonesia.

Appendix

Simplified Guide to Implement Information Technology Risk Management

Phase	Actions
Phase 1	**Framing the project**
Step 1.1	*General directions and shared expectations*
☐	Understand the strategic orientations and the level of maturity of IT risk management
☐	Conduct interviews with top management in order to: Clarify mutual objectives and expectations, Exchange on strategic orientations, Identify major risks
Step 1.2	*Project organization*
☐	Define and compose the project team
☐	Identify the key players and stakeholders
☐	Draw up the overall project schedule
Step 1.3	*Methodological framework for IT risk management*
☐	Definition of the rating scales for the likelihood, impact, control system and risks criticality

☐	Definition of the risk matrix and criticality levels
Phase 2	**Data collection and synthesis**
☐	Identify a method for collecting, classifying and analyzing IT risk data
☐	Analyze the internal and external environment of the company that may have impact on IT risk management
☐	Specify IT risks and their mitigation plans related to the industry peers
☐	Record data on IT incidents and their impact on the organization
☐	Summarize the data collected and highlight IT risk events
Phase 3	**Development of IT risk management framework**
Step 3.1	*Analyze and map IT risks*
☐	Identify potential IT risks (the generic scenarios defined by COBIT 5 for risk can be used)
☐	Identify for each risk the macro process, process and category
☐	Define risk indicators that allow the monitoring of risks
☐	Define specific control activities for each risk
☐	Estimate the likelihood and impact associated to each risk
☐	Assess existing controls, and estimate residual risk
☐	Compare residual risk to acceptable risk tolerance and define risks that may need a response
☐	Analyze costs and benefits of potential risk response options
☐	Propose the optimal risk response
☐	Identify requirements for the implementation of the risk mitigation response
☐	Consolidate all identified risks in an overall risk profile (risk mapping)
Step 3.2	*Complete the risk profile*
☐	Inventory business processes and identify dependency on IT applications, services and infrastructures
☐	Identify critical IT applications, services and infrastructures necessary to keep business processes running
☐	Document IT incidents that have occurred
Phase 4	**Change management / Communication and awareness-raising**
Step 4.1	*Ensure risk culture awareness*
☐	Promote a culture of IT risk awareness and empower the organization to proactively identify IT risks, opportunities and potential business impacts
☐	Provide and deploy a risk communication plan (covering all levels of the business) in order to romote a culture of IT risk awareness
☐	Ensure the integration of IT risk management strategy and operations with the global risk management system
☐	Implement an appropriate procedure that explains how to respond quickly to changing risks and report to appropriate levels of management
☐	According to the risk mapping, identify the risk indicators to be monitored and determine the procedures for obtaining and reporting measures
Step 4.2	*Communicate and provide risk information*
☐	Prepare and adapt supports to communicate the results of the risk analysis to corresponding stakeholders in order to support business decisions
☐	Communicate the current risk profile to corresponding stakeholders, including the effectiveness of incident management, corrective actions and their impact on the risk profile

☐	Analyze the results of objective third-party assessments, internal audits, and quality assurance controls and relate the impact on the risk profile

Phase 5	**Monitoring and surveillance**
Step 5.1	*Respond to incidents*
☐	Prepare, maintain and test Business Continuity Plans that specify the steps to be taken when a risk when occurring may cause an interruption of business
☐	Apply the appropriate response plan to minimize the impact when the risk occurs and update the action plan and its status in the IT incident database
☐	Rank incidents and compare current exposures with risk tolerance levels. Analyze incidents by specifying root causes, business impacts, additional risk mitigation plan, improvements to processes…
☐	Communicate the incident analysis to the appropriate stakeholders and update risk profile and IT incident database
Step 5.2	*Monitor IT risk management*
☐	Maintain an inventory of control activities in place to manage risk
☐	Monitor mitigation risk plans and their status and determine whether each organizational unit monitors risks within tolerance levels
☐	Monitor key risk indicators vs. targets, analyze the gaps and take corrective action to address the underlying causes
☐	Monitor the company's progress toward identified objectives
☐	Report about the monitoring activities and any risk management issues to the appropriate stakeholders