OPERATIONAL RISK MANAGEMENT IN THE POSTAL SECTOR: A CASE STUDY OF A DEVELOPING COUNTRY

Ramzi Trabelsi *

* Committee of State Controllers, Government Presidency, Tunisia
Contact details: Committee of State Controllers, Government Presidency, Menzel Bouzelfa Nabeul 8010, Tunisia

How to cite this paper: Trabelsi, R. (2021). Operational risk management in the postal sector: A case study of a developing country. *Corporate Governance and Organizational Behavior Review, 5*(1), 37-45. https://doi.org/10.22495/cgobrv5i1p4

ISSN Online: 2521-1889
ISSN Print: 2521-1870

Received: 17.10.2020
Accepted: 15.03.2021

JEL Classification: G3, L10, L87, C83
DOI: 10.22495/cgobrv5i1p4

Abstract

The Tunisian Post is a multi-business organization and operates in a changing environment; it faces risks, internal or external. The Tunisian Post has taken a step in this new area of expertise, which is reflected in the establishment of an Operational Risk Management Unit. The main purpose of this article is to present the first experience of the Tunisian Post in this area of expertise. A survey was conducted by the risk management unit (RMU) on a sample of 65 postal offices in the period between 2015 and 2017. The survey covers almost all of the Tunisian territory. A database containing all the probable risks was sent to the post managers at the regional level to give their assessment in terms of frequency and impact of each type of risk on their structures. More than 40 executives and employees at the regional and central levels participated in the brainstorming for the development of recommendations and the establishment of a road map. The results showed that the risks related to IT risks are more frequent and critical, which can deter the quality of the services at the regional level. Despite the increasing attention to risk management in the public sector, more research is required, especially in the postal sector. Operational risk management is the unrevealed black box (Bracci, Tallaki, Gobbo, & Papi, 2021). So, this paper presents a practical and professional manner to analyze better the entities' function at the regional level.

Keywords: Postal Sector, Risk Management, Risk Map, Survey, Road Map

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

Acknowledgements: The paper has also greatly benefited from the great support of the operational risk unit chief and all the staff of different postal departments. We are solely responsible for all remaining errors and omissions.

1. INTRODUCTION

The Tunisian Post intends to continue and modernize its public service missions, improving performance and competitiveness to find a new sustainable economic equilibrium. With the digitalization of the national economy, the post is facing tough challenges, such as the opening of the postal market to competition, which requires the post office to innovate a new range of financial products. Consequently, we find the emergence and diffusion of postal services based on digital technology emerging and spreading, while other conventional services, such as mail deliveries, are gradually losing their weight in the turnover rate.

The digitization of the national economy goes through a rather advanced stage that is characterized by the emergence of a cluster of new disruptive technology, such as cloud computing, big data, digital printing, artificial intelligence, and the Internet of things. These challenges would force public decision-makers to reconsider how Tunisian Post operates as a company that seeks profitability and sustainability. Given the inevitable opening of the service sector to free competition, then the only choice will be centered on quality, competitiveness, and good governance. The post is considered to be a public institution that is subject to good governance considerations (OCDE, 2016), which is reflected in the creation of the Operational Risk Management Unit in 2013.

Indeed, it should be noted that risk management is a new concept in the public sphere (Renard, 2006), knowing that this unit has only three years since its start working in the post. The Tunisian Post is a multi-business organization and operates in a changing environment; it faces risks, whether internal or external. Operational risk management is considered among the areas of development in the postal organization. In this respect, the post is developing expertise in this area.

The purpose of this work is to highlight the challenges of the postal activity. In this context, we analyzed more specifically the challenge of risk management, which represents a new concept in the Tunisian Post.

The Tunisian Post is required to modernize its network of points of contact which are located near the citizens. Indeed, the improvement of the relationship with service users must be realized through post offices at the regional level. Risk analysis at post offices will help to improve postal service quality.

In this context, there are a few questions that arise and we are interested in providing some answers:

RQ1: What are the risks related to the postal activity and which influence the quality of the services provided by the post offices?

RQ2: What are the actions needed to limit or eliminate these risks?

So, the remainder of the paper is organised as follows. Section 2 presents a theoretical concept study of risk management. Section 3 outlines the sample and methodology used for the study; it is dedicated to a practical case study on risk assessment at the regional level, and more specifically, at the post office level. Section 4 presents the results and Section 5 concludes the paper.

2. THEORETICAL CONCEPT OF ENTERPRISE RISK MANAGEMENT (ERM)

International level

A risk is the danger of an activity, a structure, or context. It is a fact, an action, or an event that is able to create damage to the company. According to Zekos (2021), the risk is a tool that makes it possible for the decision-maker to get knowledge about the event with destructive effects and so, the decision-maker via the analysis of risk makes the event more certain and obtaining control on it. Therefore, the main issue of risk management is to avoid such potential damage by putting in place a whole battery of preventive actions to counter this type of harmful element. Companies face a number of risks, which is why risk management should be a central part of the strategic management of any company (Eleftheriadis & Vyttas, 2018; Calza, Profumo, & Tutore, 2017). Risk management helps you identify and address the risks facing your business and in doing so, increases the likelihood of successfully achieving your business goals. Companies in any sector are exposed to all types and sizes of internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. This uncertainty has an impact on an organization's objectives. It is the risk (Bracci, Tallaki, Gobbo, & Papi, 2021).

Risk management was defined clearly in the standard guidelines of the risk management ISO 31000 developed by the ISO (International Organization for Standardization). This international standard provides principles and generic guidelines on risk management. The first ERM framework was published in 2004. This document has subsequently become a standard reference in discussions on ERM implementation alongside ISO 31000 (2009)[1], which is an internationally agreed standard for the implementation of risk management principles. The purpose of frameworks such as ISO 31000 is to ensure compliance, assurance and to improve decision-making.

The COSO (2004) provides clear direction and guidance for ERM. It is dedicated to helping different entities to design and implement effective enterprise-wide approaches to risk management. This framework will bring together all the thoughts around the concept of risk management and its related components and principles. The guidance introduces an enterprise-wide approach to risk management as well as concepts, such as risk appetite, risk tolerance, portfolio view. This framework is now being used by organizations around the world to design and implement effective ERM processes. According to COSO (2004), good risk management and internal control are necessary for the long-term success of all organizations.

From a theoretical point of view, the main conventional trend in risk assessment is centralized around two main theoretical axes. The theory of expected utility starts from two primary motivations: the aversion to risk, which means the willingness to avoid dangerous situations, and the search for realizations, accept the risk and seek the remedy. These two motivations interfere with decision-making processes making preference not a constant, but a construction. The decision-maker, considered rational and conscious, maximizes a utility function under conventional time constraints and budget based on information. Confronted with different situations, he seeks the maximization of the expected utility given a probability associated with the risk in a hazardous way. ERM consists of risk governance and risk aggregation. The board of directors, on behalf of shareholders, adopts risk governance to deal with the agency problem of risk management. Managers tried to undermanage the risks characterized by a low probability and a high impact. In fact, external

[1] ISO Guide 73:2009, Risk management – Vocabulary (https://www.iso.org/standard/44651.html).

risks can be well managed if the enterprise knows well its environment. So, the board structure and composition matter in firms' environmental proactivity (Calza et al., 2017). It may present a high probability and can cause big damage and reduce the expected mean of future cash flows.

On another side, the theory of perspectives was founded by Kahneman and Tversky (1979), starting from the observation of non-linearity of the probabilities associated with the events with which individuals are confronted. Unlike the previous theory, two phases build the choice: the structuring phase of information, which is a preparatory phase of "reformulation-simplification", and an evaluation phase, which leads to evaluating the options and choosing the one that has the most value. In other words, subjective probabilities replace probabilities objectives of the previous theory. According to Gates (2006), the demand for ERM and improved governance of firms' risks became very important in the last two decades. Pressure from outside stakeholders has been an important influence on this development reflecting corporate scandals involving excessive risk-taking. Fraser, Simkins, and Narvaez (2015) argued that ERM is described as an evolving process that becomes codified and practiced in a consistent way. COSO (2016) has given another vision for this concept by giving ERM a strategic role as soon as it has to be integrated into the strategic decision-making process of the company. Alviniussen and Jankensgard (2009), opt for a more quantitative approach, framing ERM in terms of statistical summary measures of risk concerning financial axes. Many researchers, such as Power (2009), remain within the basic framework of ERM as a tool for risk control, driven by an accounting and auditing logic. Bogodistov and Wohlgemuth (2017) seek to integrate ERM under management focused on available resources in parallel with the dynamic capability framework in which a company uses its risk management tools to the protection and improvement of skills, productivity, and business performance. Nocco and Stulz (2006) tried to recognize the full extent to which risk management takes place within the context of an agency relationship and information asymmetries internal to the firm. Mikes and Kaplan (2015) argued in favor of a contingency theory that seeks to identify various design parameters that can explain the large observed variation in how ERM is implemented. They admitted that there is no one universal form of ERM that will maximize firm profit.

National level

The mission of the RMU is to identify failures in production systems in the Tunisian Post. To fulfill this mission, the managers of this unit maintain a horizontal relationship with the production units. They are familiar with all the specific aspects of production. This advantage makes it easier for them to identify the different types of risks that can reduce the company's performance or profitability. The knowledge of the various operational risks is the result of the concerted efforts of all the structures and their contribution to the creation of a database that includes all types of risks. The unit collects risks through a network of contacts in each production site or central and regional departments.

The term "risk management" is widely circulated and known in the public sphere, its understanding and even more, its implementation, is still recent in the process of stabilization in public administrations. In Tunisia in particular, the "risk management" is in a phase of initialization. Today, public enterprises are exposed to probable risks in their fields of activity. Nowadays, the environment is characterized by gradual and rapid liberalization of the service sector, especially in postal services. The state is no longer the monopoly in this sector since it has abandoned its role of protection. These reasons pushed the Tunisian Post to develop a new culture to adapt easily to the new market rules. The Tunisian Post was a precursor in this field as soon as its administration wanted to move from the classic concept of public service to more competitive services. This ambitious initiative was reinforced by the creation and implementation of the Operational Risk Management Unit in September 2013. The implementation of risk management within the Tunisian Post is conducted according to a standard process. It consists of several steps: the managers must start with the risk identification phase. The risks are then evaluated according to their financial consequences and the likelihood of their occurrence and then ranked in order of priority. The third step of the risk management process is risk management, based on the evaluation of risk. Action plans are the main elements of risk management. This step includes an estimation of the impact on the business in terms of turnover rate. The process ends with risk management control. It encompasses the monitoring and management of risk management. As the process is continuous, risk management control is followed by the identification of new risks. Finally, centralized IT solutions will be used by the administration to implement the risk management process and support the production units.

Given the complexity of the postal business, multiple threats, incidents, and operational risks related to production, management, and the commercial network can hinder the achievement of objectives and negatively impact the profitability and performance of the enterprise. Thus, one of the principles of good governance within the company would be the identification of inherent risks in order to control them or to minimize them by implementing various mechanisms of coordination, evaluation, and follow-up.

The steps followed to perform the risk-mapping are as follows: first, the managers must locate the entities that own the operational risks. Then, they establish different approaches, contacts, and audits. They draw up the risk inventory by structures. Finally, they evaluate the impact of risks and draw the final map highlighting the severity of each threat. The assessment of severity will be based on financial impact, frequency, probability of occurrence, and negative effects on quality.

To do this, the GRO unit advocates the deployment of a networked computer application that will automatically link the risk owners to the various structures concerned by allowing them to report incidents immediately. It should be noted that the application is currently in the testing phase at the computer center for the features it offers and that it can be completed by the incident database by structure.

The Tunisian Post is required to modernize the network of contact points located near Tunisian citizens. The extensive commercial network in the area is a strong point for the Tunisian Post, especially in rural areas. Improving the relationship between the citizen and the post office must be done from the post offices or the front office. There is a need to optimize the office network according to the needs of the neighborhoods in which they are located. Thus, to maintain the trust of citizens, all efforts must be combined to provide quality customer-oriented services in all post offices. So, to improve the quality of postal services, we must act quickly against intolerable risks.

3. SAMPLE AND METHODOLOGY

This survey was conducted by the GRO on a sample of 65 postal offices in the period between 2015 and 2017. The survey covers almost all of the Tunisian territory. A database containing all the probable risks was sent to the post managers at the regional level to give their assessment in terms of frequency and impact of each type of risk on their structures. More than 40 executives and employees at the regional and central levels participated in the brainstorming for the development of recommendations and the establishment of a road map. The methodology of this study is based on the following steps: we list all the types of risks likely to be encountered in the organization. The second step is the identification of each process/function/activity to be estimated. Then, we estimate each risk for each function or activity. This estimate, presented in the form of a double-entry table, will focus on two points: the assessment of the impact of the risk (severity); and the assessment of the estimated vulnerability (frequency).

This assessment is made by considering the maximum possible risk, also called intrinsic risk or specific risk, or inherent risk (during the maximum possible loss of insurers). Internal auditors are attentive to this constant adaptation when they track down the shortcomings resulting from the obsolescence of the systems in place. They will be even more, so if there is no risk manager in their organization.

In this case, in fact, it is the internal audit that will have to map the risks of the company, the starting point for any subsequent analysis, but it cannot own the risk management. This area then comes under general management.

Whatever the method used for risk assessment, the logical approach involves an additional step before the definition of the means to implement: the risk response.

Among the two components of risk – impact and probability – a strategy must be chosen for each risk identified: minimize the impact by developing a protection policy; or minimize the frequency by developing a prevention policy.

3.1. Identification of operational risks

This stage of the identification of operational risks related to the activity of the post offices is the most important because it makes it possible to list exhaustively all the risk of loss that can be attached to its management. To perform this task, we will collect the risks (see Table A.1 in Appendix).

Following the identification of the operational risks related to the operation of the post offices, we will proceed with their evaluation knowing that our work is done after the elaboration of a survey.

3.2. Operational risk assessment

In a Farmer's diagram, we can distinguish one that represents the border between acceptable risks and unacceptable risks, therefore to be reduced. Measures that reduce the frequency of risk are part of prevention; measures that reduce the severity of risk are part of protection (Mortureux, 2016).

We used a qualitative or quantitative analysis at the risk assessment stage. The goal is to better understand the risks and estimate their probabilities of occurrence or the severity of their consequences. Knowing that operational risks can arise from internal or external factors, we will proceed at stages of evaluation.

3.3. Assessment of the probability of operational risks' occurrence

The probability of occurrence of operational risks is a step that allowed us, during our interview with the operational staff, to get an idea of the quality of the system put in place at the post offices. The higher the quality, the lower are the risks. The frequency of occurrence of risk is attached to how often a failure can occur within a space of time. This evaluation is based on a scale of 1 to 5 according to the following table.

Table 1. The rating scale of the probability of occurrence of risk

Frequency	*Criterion*	*Level*
Non-existent	Less than one failure per year	1
Possible	One to seven failures per year	2
Certain	One to three failures per month	3
Frequent	One to five failures per week	4
Very frequent	At least one failure per day	5

Source: The elaboration of the Author and GRO unit.

Next, we are going to assess the different risks identified. In the next step, we will measure the impact of each risk.

3.4. Evaluation of the impact of operational risks

This step allows us to know the potential consequences caused by these risks. We will use the qualitative method to assess the impact of risks as we did with the frequency of risk occurrence. For the realization of this operation, we will be based on a rating scale of the impact of the risks indicated hereafter.

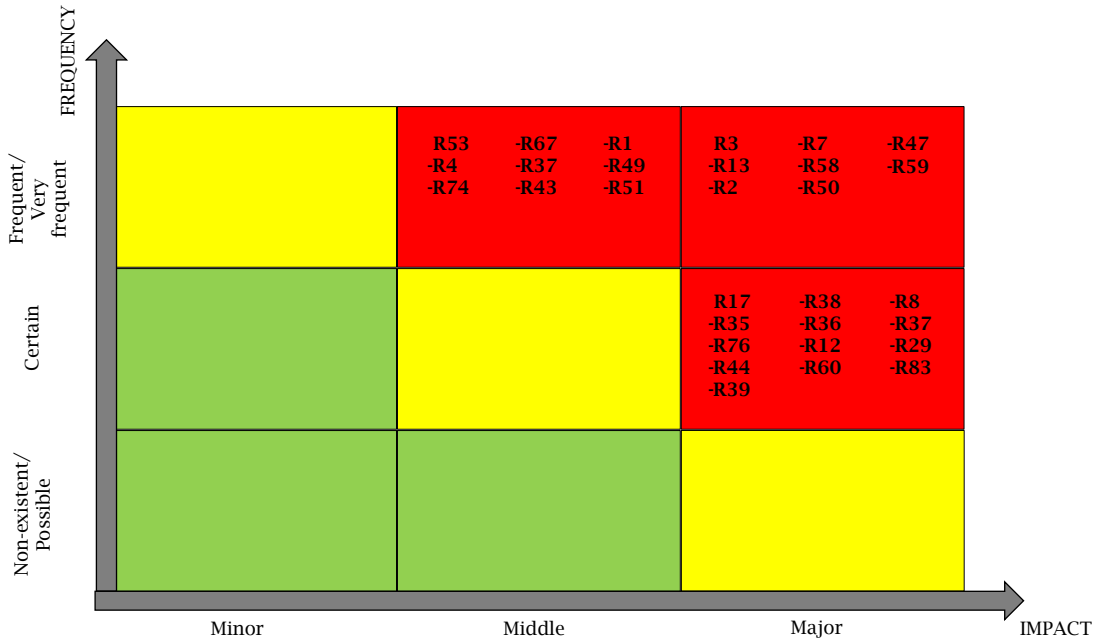
At the end of the operational risk assessment, according to the probability of occurrence and the risk impact, we will prioritize these risks, and then we will try to design a matrix that will allow us to schematically have an idea about the highest risks. This matrix consists of representing the probabilities on the ordinate and the impact on the abscissa. The principle of our work is unique because we will choose to produce a single risk matrix for all the regions of our sample.

Table 2. Evaluation of the impact of operational risks

Gravity	*Level*
Minor	1
Middle	2
Major	3

Source: The elaboration of the Author and GRO unit.

Figure 1. Operational risk mapping



Source: Author's elaboration.

3.5. Risk treatment

In this step, the manager must address the risks that represent an alert for the company. According to the risk map, the red zone corresponds to unacceptable risks. They are the most frequent and whose impact is the most severe, those are the dangers that must be removed quickly. To remedy these problems, it is better to put in place preventive measures to reduce the risk assessment to an acceptable level. For each identified risk, a "risk owner", a person responsible for developing a proposal for an action plan or a proposal for a specific risk monitoring should be designated.

The determination of the means of control of the risks is the main task of working group of the unit of GRO and the managers for each failure in the post offices. Brainstorming is a creative technique for solving these problems, it is used at this stage of our work to properly choose or propose actions to control risks. These actions must be realistic and applicable in the field. They can integrate technical, organizational, human, and environmental measures. The proposed actions must respect some principles.

The manager or the risk owners must avoid risks; evaluate risks that cannot be avoided; fight risks at the source; adapt the work to the workers (ergonomics) by acting on the conception, the organization, and the methods of work and production (e.g., to take into account the physical and mental aptitudes of the individual during the conception of a post working); take into account the state of evolution of the technical aspects; replace what is dangerous with what is not dangerous or what is less dangerous; take collective protective measures giving them priority over individual protection measures, and they must give appropriate instructions to workers.

After validation of the selected actions, they are implemented by the manager, under the control of the risk owner. The action plan may result in a decrease in risk, a transfer to insurance or avoidance by abandonment of an activity or project.

4. RESULTS

4.1. The road map

To value the results, we used the brainstorming tool with managers and staff in the Tunisian Post. The action plans are the actions to be taken to reduce the inherent risks to residual risks. Therefore, we must react against risks that pose a threat to the performance and profitability of post offices in all regions (the action plans are presented in Table A.2 in Appendix). The results show that the most inherent operational risks are related to the area of IT security. Managers must prioritize the implementation of solutions to ensure the availability, security, and integrity of information system and data. It is important to carry out audits of the security system, most often with the help of service providers and analyze the risks and malfunctions. The objective is to define or change security measures and standards (charter), in line with the nature of the activity of the business and its exposure to IT risks. Risk owners must monitor technology, so as to guarantee the logical and physical security of the information system.

5. CONCLUSION

The purpose of this work is to present the concept and practice of risk management with a concern to attract the attention of the reader, more specifically, to the leader. In fact, the environment in which the Tunisian Post is operating carries risks. Therefore, strengthening the unity of operational risk management through technical and human means is necessary. A decision-maker who places greater emphasis on the technical and financial aspects should appreciate the aspect of risk management which is a key strategic function. The lack of commitment and understanding of the board of directors can simply make the GRO unit obsolete.

To successfully implement this type of program, the person in charge of the GRO unit will have to be at the same level as the other directors, so as to be able to influence them and to retrieve the information necessary for the risk assessment in each of them. Once risk levels are identified, senior management will still need to ensure that the elements of this culture are passed on to their employees. Managers will need to provide employees with risk management objectives in order to share responsibility with them. In addition, the GRO unit must have a section in the future post-annual reports.

Good governance in the Tunisian Post requires the development of information and the creation of a database of all postal risks. As a result, the postal establishment will be reactive against new risks. On the one hand, it helps to limit losses and ensure that goals are achieved. On the other hand, risks will be properly managed and resources will be used responsibly. So, good risk management often comes down to adopting good management practices, with a good balance between the expected benefit and the risk when making the decision.

It is necessary to develop a tradition within the Post Office regarding the perception, evaluation, and control of operational risks. This can be initiated at the decentralized level. In fact, officers in the regional directorates and post offices must be well trained to correctly assimilate the concept of risk management, in order to react in an effective and autonomous way without going through the central management office. With the support of the GRO unit, post office managers can easily identify risks and make decisions by suggesting action plans to address them. In addition, the work of the GRO unit must be carried out by moving directly to the organism that will undergo a control, and the risk analysis must be generalized on all the post activities, such as logistics and financial investments. Finally, this work did not take into account most categories of risks such as financial and technological risks, especially with the tendency to liberalize this market in the future and the establishment of a postal bank, this debate can be a very interesting research axis in the future.

REFERENCES

1. Alviniussen, A., & Jankensgard, H. (2009). Enterprise risk budgeting: Bringing risk management into the financial planning process. *Journal of Applied Finance, 19*(1-2), 178-192. Retrieved from https://ssrn.com/abstract=1426023
2. Bogodistov, Y., & Wohlgemuth, V. (2017). Enterprise risk management: A capability-based perspective. *The Journal of Risk Finance, 18*(3), 234-251. https://doi.org/10.1108/JRF-10-2016-0131
3. Bracci, E., Tallaki, M., Gobbo, G., & Papi, L. (2021). Risk management in the public sector: A structured literature review. *International Journal of Public Sector Management, 34*(2), 205-223. https://doi.org/10.1108/IJPSM-02-2020-0049
4. Calza, F., Profumo, G., & Tutore, I. (2017). Boards of directors and firms' environmental proactivity. *Corporate Governance and Organizational Behavior Review, 1*(1), 52-64. http://doi.org/10.22495/cgobr_v1_i1_p6
5. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Enterprise risk management – Integrated framework: Executive summary.* Retrieved from https://www.academia.edu/13833787/Enterprise_Risk_Management_Integrated_Framework
6. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2016). *Enterprise risk management – Aligning risk with strategy and performance.* Retrieved from web-marketing.stern.nyu.edu
7. Coulmont, M., Berthelot, S., & Talbot, C. (2020). Risk disclosure and firm risk: Evidence from Canadian firms. *Risk Governance and Control: Financial Markets & Institutions, 10*(1), 52-60. https://doi.org/10.22495/rgcv10i1p4
8. Eleftheriadis, E., & Vyttas, V. (2018). The measurement of risk and performance in public organizations. *Risk Governance and Control: Financial Markets & Institutions, 8*(4), 7-15. https://doi.org/10.22495/rgcv8i4p1
9. Fraser, J. R. S., Simkins, B. J., & Narvaez, K. (2015). Enterprise risk management case studies: An introduction and overview. In J. R. S. Fraser, B. J. Simkins, & K. Narvaez (Eds.), *Implementing enterprise risk management: Case studies and best practices* (Chapter 1). Upper Saddle River, NJ: John Wiley & Sons.

10. Gates, S. (2006). Incorporating strategic risk into enterprise risk management: A survey of current corporate practice. *Journal of Applied Corporate Finance, 18*(4), 81-90. https://doi.org/10.1111/j.1745-6622.2006.00114.x
11. Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263-291. https://doi.org/10.2307/1914185
12. Mikes, A., & Kaplan, R. (2015). When one size doesn't fit all: Evolving directions in the research and practice of enterprise risk management. *Journal of Applied Corporate Finance, 27*(1), 37-40. https://doi.org/10.1111/jacf.12102
13. Mortureux, Y. (2016). *Fondamentaux de l'analyse de risque, regard fiabiliste sur la sécurité industrielle: Regard fiabiliste sur la sécurité industrielle* (Edition coordonnée par Clotilde Gagey et Caroline Kamaté, No. 2016-02). Retrieved from https://www.foncsi.org/fr/publications/regards/fondamentaux-analyse-risque-regard-fiabiliste/view
14. Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance, 18*(4), 8-20. https://doi.org/10.1111/j.1745-6622.2006.00106.x
15. OCDE. (2016). *Le contrôle interne et la gestion des risques pour renforcer la gouvernance en Tunisie*. Retrieved from https://www.oecd.org/mena/governance/le-controle-interne-et-la-gestion-des-risques-pour-renforcer-la-gouvernance-en-tunisie.pdf
16. Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6-7), 849-855. https://doi.org/10.1016/j.aos.2009.06.001
17. Renard, J. (2006). *Théorie de pratique et d'audit interne* (4iém éd.). Paris, France: Groupe Eyrolles.
18. Zekos, G. I. (Ed.). (2021). Risk management developments. In *Economics and law of artificial intelligence* (pp. 147-232). https://doi.org/10.1007/978-3-030-64254-9_5

APPENDIX

Table A.1. Risk identification phase (Part 1)

	Nature of risk (R1 until R78)
Post offices	1. Slow computer system 2. Computer system failure 3. System failure queue 4. Lack of computer consumables 5. Out of paper stock for the publication of accounting statements 6. Remote compensation scanner failure 7. Failure of computer equipment 8. Shutdown of the DAB system and failure 9. Acts of vandalism on DAB 10. External acts of vandalism 11. Decrepit and dangerous premises 12. Lack of liquidity at the opening of the office 13. Late arrival of funds 14. Lack of coins for wickets 15. Funds received with missing amounts 16. Surplus funds received 17. Deficits of cash agents of wickets 18. Deficits of cash at the level of the centralizer 19. Deficits in the office manager's fund 20. Deficits in the ATM fund 21. Embezzlement by a counter agent 22. Embezzlement by the head of office 23. Uncollected claims 24. Acceptance of counterfeit Tunisian banknotes 25. Delivery of fake Tunisian banknotes to customers 26. Delivery of foreign counterfeit notes to customers 27. Acts of fraud on the part of the customers 28. False or unintentional payments 29. Loss of documents and accounting documents 30. Loss of registered mail to the service 31. Wrong delivery of registered shipments 32. Disclosure of trade secrets 33. Impossibility of satisfying large withdrawal requests 34. Refusal of service 35. Late opening of the office 36. Advanced closure of the office 37. Out of stock of some printed matter 38. Loss on the exchange rate 39. Late payment of large clients 40. Hold up or attempt to hold up during the opening of the office 41. Hold up or attempt to hold up after closing the office 42. Hold up or attempt to hold up on the service home 43. Failure of the remote monitoring system 44. Anti-intrusion system failure 45. Unsecured counters 46. Locking the safe 47. Closed counter following an absence

Table A.1. Risk identification phase (Part 2)

	Nature of risk (R1 until R78)
Post offices	48. Work accidents 49. Unliquidated leave of absence 50. The imbalance between counters and internal services 51. The aggression of staff by clients 52. The aggression of customers by staff 53. Violence between customers at the counters 54. Violence between agents 55. Loss of office keys 56. Loss of keys from the safe 57. Vehicle breakdown of the mobile post office 58. Absence of specimen signatures for CCPs 59. Lack of proxies in the system for CCPs 60. Absence envelopes 61. Lack of accounting documents for related agencies 62. Lack of funds for payments from affiliated agencies 63. Lack of support and supervision visits 64. Declining general turnover 65. A decrease in sales for certain products 66. Workbooks not updated 67. Late arrival of circulars and working documents 68. Wrong interpretation of workbooks 69. Late receipt of the accounting of the attached offices 70. Difficulty replacing the heads of attached offices 71. Lack of control of attached offices 72. Send funds to rural offices unsecured 73. Infiltration of water and power failure 74. Absence of the security guard 75. Absence of the cleaning agent 76. Stopped service after social movements

Source: The elaboration of the Author and GRO unit.

Table A.2. Relevant actions to control operational risks (Part 1)

Nature of risks	*Possible risk management actions to put in place*
Slow computer system	• Filtering and limiting the size of data transmitted over a bandwidth • Improved internet connection speed (optical fibers) • Redesign of the computer system
Failure of the queuing system	• Implementation of an application related to the postal system • Recruitment of reception officers able to restore order • Periodic system maintenance
Computer hardware failure	• Fully depreciated hardware replacement • Preventive maintenance • Security stock in replacement equipment per office
Computer system failure	• Improvement of central servers and decentralization of data centers
Failure connection/communication network	• Cable review in all offices (network cabling + Telecom) • Emergency link prediction
Failure of the remote monitoring system	• Automatic signaling with the operating room • Contract with a security company to provide guards
Anti-intrusion system failure	• Signage and immediate intervention of service providers • Update of firewall certificates
DAB shutdown following system failure	• Automatic signage to suppliers • Create an Android application called SOS DAB • Periodic and preventive maintenance
Electrical failure	• Monitoring of regional maintenance services with the presence of qualified agent at the central level • Set up of generators and sophisticated inverters • Recruitment of senior electrical engineering technicians in each regional directorate to intervene quickly at the post office level
Sending funds to rural unsecured offices	• Agreement with private companies to transport funds • Creation of a CIT company • Limit the amount outstanding
The counter closed following an absence	• Establishment of regional reserve brigade of counter agents • Strengthening the reserve brigade in each region
Late opening of the office Advanced closure of the office	• Strengthen the monitoring role of the regional inspectorate • Head office accommodation nearby • Double post office key at the Regional Director • Unannounced check visits
Violence between customers at the counters	• Linking the alarm system with the police stations
Customer aggression by clients	• Qualified security officers in all offices • Workforce rotation to minimize load and manage stress
Lack of specimen signatures for CCP Lack of proxies in the system for CCP	• Integrate all printed in the system e-office (printed side) to print them directly and immediately in case of need

Table A.2. Relevant actions to control operational risks (Part 2)

Nature of risks	*Possible risk management actions to put in place*
Lack of computer consumables Out of the stock of certain printed Lack of postage products and envelopes	• Follow-up of consumables usage by office • revive the Central Cost Accounting unit to manage consumable needs • forecast inventory management at the material account center (central store and regional stores) • The regional office must synchronize between neighboring post offices to perform a two-way exchange of missed product
Lack of liquidity at the opening of the office	• Create urgent requests with fund carriers • Management planning in consultation with the Central Fund and the Regional Fund
Loss on the exchange rate	• Provide currency stock management and optimize the management of the operating room • Creation of an econometric study unit and use of sophisticated statistical forecasting software such as STATA, R, AMOS, and SPSS
Agent cash deficits in counter	• Creation of insurance for confirmed and unrecoverable deficits • Opening of the new counter • Reciprocal verification of transactions by a second agent in the back office during peak hours
An imbalance between external and internal services	• Optimize personnel management • The versatility of agents through intensive training (at least 4 times per year) to facilitate turnover in several tasks • Staff monitoring units at the personnel management level
Loss of documents and accounting documents	• Allow the heads of offices to constitute duplicates • Electronic archiving
Unliquidated leave and absence	• Recruitment of seasonal workers • Liquidation in off-peak periods • Install vacation management software at the office level • Creation of regional reserve brigade of the agents

Source: Author's elaboration.