Integrated Risk Management in Quality and Information Security Systems

Joaquim Machado[1], Magda Ribeiro[2]

[1] Head of Technological Infrastructure and Information Security Unit, Statistics Portugal, Portugal

[2] Head of Planning, Control and Quality Unit, Statistics Portugal, Portugal

Abstract

In today's complex and dynamic business environment, organizations face multifaceted challenges related to quality assurance, information security, and overall risk management. National Statistical Institutes are examples of organizations that are facing up to these challenges. Our study explores the interconnectedness of these critical domains and emphasizes the need for an integrated approach to address the evolving landscape of risks.

Quality systems play a pivotal role in ensuring that products and services meet or exceed customer expectations. However, the pursuit of quality must be accompanied by a comprehensive risk management strategy to identify, assess, and mitigate potential threats. Integration of risk management into quality systems not only ensures the integrity of products and processes but also improves the overall organizational resilience.

Simultaneously, information security has become paramount in the digital age, where organizations rely heavily on interconnected technologies and data-driven processes. The paper underscores the inseparable link between information security and risk management, emphasizing the importance of a proactive and adaptive security framework. Such a framework must address the evolving nature of cyber threats, privacy concerns, and regulatory requirements to protect sensitive information.

Furthermore, the paper delves into the synergies between quality systems and information security, highlighting how a harmonized approach can amplify the effectiveness of risk management efforts. The convergence of quality assurance and information security fosters a culture of continuous improvement and resilience. It enables organizations to identify vulnerabilities across processes and information systems, implement preventive measures, and respond promptly to emerging risks.

In this study, we will present the approach taken by Statistics Portugal to build an integrated information management, quality and security system, namely by adopting a common risk analysis and management methodology and tool.

The paper concludes by emphasizing the need for a holistic risk management strategy that integrates quality systems and information security. By doing so, organizations can create a robust framework that not only ensures the delivery of high-quality products and services but also strengthens the confidentiality, integrity, and availability of critical information assets. This integrated approach positions organizations to navigate uncertainties with agility, maintain stakeholder trust, and sustain long-term success in an ever-evolving business landscape including national statistical offices.

Keywords: Risk Management; Quality; Information Security Systems

1. Introduction

Statistics Portugal has a Quality Management System in place since 1996. The system is supported by the Principles of the National Statistical System (NSS), as inscribed in Law no. 22/2008, as well as the General Guidelines of Official Statistical Activity 2023-2027 (which constitute an important framework for the strategic objectives of the NSS and the relevant actions for the national statistical authorities for this period). The quality management system is aligned in commitment with European Statistics Code of Practice at national level. The ISO 9000 family of standards, as well as the ISO 10004, ISO 10002, ISO 19001 and more recently the ISO/IEC 27001, have always been a reference for Statistics Portugal Quality Management System. The four main objectives of Statistics Portugal Quality Management System are to continuously improve the quality of: i) systems and process; ii) the products; iii) the services rendered to respondents and users; iv) the work and inter-department relations at all levels of the organisation.

On the other hand, since 2018, Statistics Portugal has been dealing with ISO/IEC 27001 and the Statistics Portugal Information Security Management System (ISMS) has been certified in 2019 for 3 years according to the ISO/IEC 27001 standard, in the context of the Micro-Data Exchange Intra-EU process between Statistics Portugal and the ESS, by APCER (Portuguese Certification Association). Certification has been a means of transmitting to the public Statistics Portugal involvement with information security and privacy, as well as a valuable tool to improve this system. In 2022 the scope of this certification has been extended to include all international trade statistics processes - intra and extra EU.

Although the scope of certification is specific, this system applies to the entire organisation.

The existence of these two management systems, the development and use of two standards that share common requirements and the position that quality and information security occupy as strategic assets of the SP, particularly in view of the main activity involved, quickly made it clear that they needed to be aligned for integration.

Step by step, these two systems (quality management system and information security system) converged into an Integrated Management System.

This was fully understood when we began the ISO 9001 certification process for the Quality Management System within the scope of the statistical production process and the high level of maturity in the Information Security Management System. At this stage Statistics Portugal considered it strategic to converge on to an Integrated Management System. The Integrated Management System follows a process approach and is comprised by 9 processes divided as follow:

Figure 1: Integrated Management System

Macroprocess Strategy and improvement	System management	Planning	Information Security Management	External Relations Management
Core Business Macroprocess	Statistical production			
Support macroprocess	Financial Management	Purchasing Management	Human Resources Management	System management

The main activity macro-process, related to the entire statistical production process, is supported by the Generic Statistical Process Model (GSBPM) and covers all of Statistics Portugal's official statistics.

There are many advantages to an integrated management system. We believe that these advantages will be even greater in the medium term when the system reaches a more developed state. One of the biggest advantages of integrating the two systems is that it makes organisational processes more efficient. This reduces duplication of effort; minimises communication errors and simplifies coordination between units.

This article will look into this Integrated Risk Management Procedure and related software implementation tool.

2. General approach

The formalisation of a risk management procedure at Statistics Portugal first took place within the scope of the Information Security Management System in 2018, in the context of the requirements of ISO 27001, having been designed based on ISO 31000 - Risk management Guidelines.

From a general point of view, the risk management addressed in the context of information security is much more detailed and demanding than that addressed in the context of Quality Management. This is clear, for example, when we analyse the references to this subject in ISO 9001 and ISO 27001. While ISO 9001 refers to risk-based thinking, ISO 27001 refers to the application of a risk management process.

However, we believe that this situation is much more complex when the organisation's business is itself technologically data-driven, and more complex when the organisation's business is itself the production and dissemination of official statistics. We would be at

precisely this level when Both, QMS and ISMS, are implemented to suit the needs and requirements in the production and dissemination of official statistics such as a National Statistical Institute. And although in theory it is more complex, in practice it is simplified by aligning concepts with the most elementary methodology that has been defined for the context of information security.

3. What we have done

We started by examining the procedure employed in the Information Security Management System (ISMS), guided by the architecture and scope established for the Integrated Management System (IMS). Our goal was to assess its applicability within the framework of ISO 9001. We emphasised that we were in the context of an information management system whose purpose is to produce and disseminate official statistics.

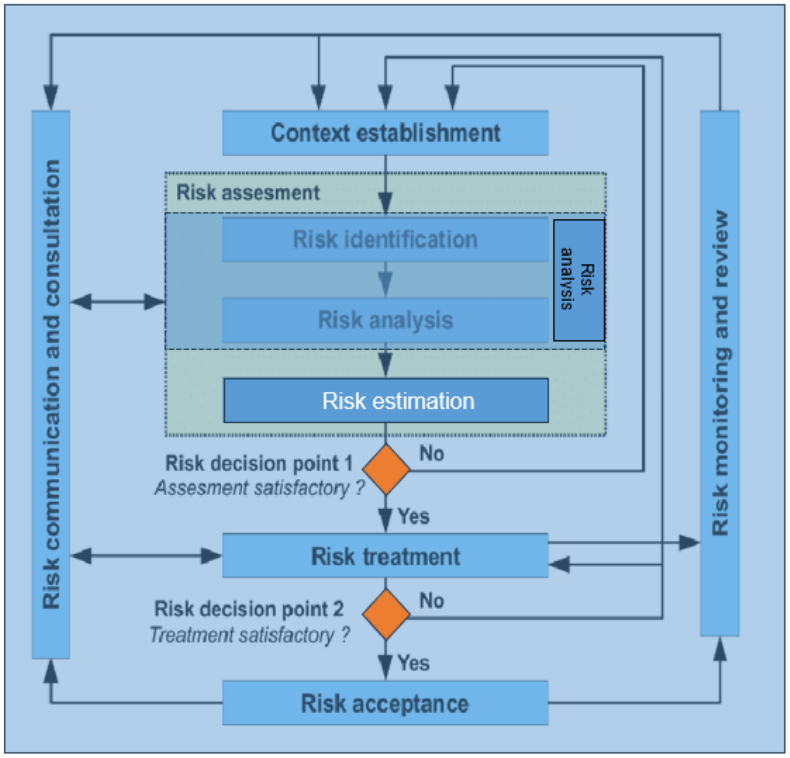
The Risk Management Procedure used in the ISMS involves the systematic application of policies, procedures and best practices across various activities. These activities include communication and consultation, establishing the context, as well as risk assessment, treatment, monitoring, review, recording and reporting, as shown in the image below (Figure 2).

This approach was also well-suited for the integrated management system, particularly when addressing risk management from a quality management perspective. This scheme is based on ISO 31000, which is applicable throughout the organization lifecycle and can be implemented in any activity, including decision-making at all levels.

The internal procedure includes the following steps:

- Inventory, identification and classification of assets.
- Impact assessment on assets.
- Identifying threats and vulnerabilities.
- Assessing the probability of threats to the assets.
- Compiling a risk assessment report.
- Defining the Treatment Plan.
- Implementation and Monitoring.
- Implementing the Risks and Opportunities Treatment Plan.
- Monitoring the implementation of the plan.

Figure 2: Workflow



Adapted from SP‘s internal Risk Management procedure and the ISO/IEC 27005:2022, ed.4.

From the analysis carried out, we realised that adjustments were necessary, particularly in aligning concepts in the following areas:

Table 1: The main points of changes

Alignment of concepts	Without adjustments
Inventory, identification and classification of assets	Impact assessment on assets
Assessing the probability of threats to the assets	Identifying threats and vulnerabilities
Definition of the Treatment Plan	Calculate the risks (=impact x probability)
Identifying the Controls - > Identifying Requirements	

3.1 Step-by-step alignment of the stages of the risk management procedure

Inventory, identification and classification of assets

We evaluated whether the assets listed in the ISMS could also be classified as assets within the Integrated Management System. The conclusion was affirmative, as the assets included in the ISMS comprehensively encompass all direct and adjacent aspects of INE's business operations. Indeed, these assets can be integrated into a quality management system, especially when the scope is the production of official statistics. The necessary adjustments were minimal, mainly involving the alignment of concepts and introduction of a few new assets. Some examples include:

- Retained Assets:
    - **Data and metadata**: The main assets of the core process.
    - **Human resources**: One of the main assets.
    - **Supporting information assets**: This category now explicitly includes policies and procedures.
- Newly added Assets:
    - **Reputation**: This encompasses the perception of providers, users and other stakeholders.
    - **Processes**: All processes are now considered primary assets in the Integrated Management System.

Analysing the impact of assets

We have assumed that the three vectors of the ISMS can be the same as those of the Quality Management System, when the core process is the Production and Dissemination of official statistics.

- **Confidentiality**: guaranteeing that information is accessible only to users and external entities duly authorised to do so.
- **Integrity**: safeguarding the accuracy of information and processing methods.
- **Availability**: guarantee that authorised users have access to the information whenever necessary.

From this alignment onwards, the methodology remains the same. After identifying and classifying the type of asset, the next step is to assess the assets impact using predefined vectors and scales.

Assessing the probability of threats to the assets

Each "Asset-Threat-Vulnerability" combination is assigned an estimated probability of occurrence based on an internally defined scale. By analysing each combination within information security and quality management, the overall probability level of that asset is obtained, calculated according to the levels identified in each strand.

Based on the calculated value, the asset's overall probability level is categorised.

Calculating the risks

The risk estimate is calculated by considering both the impact and probability of the threat occurring on the asset.

Minor syntax adjustments have been made in this section.

Definition of the Treatment Plan

In this section, adjustments were needed to interpret relevant concepts according to the scope of analysis.

- **Security framework** - Each risk identified in the "Identification of the Degree of Security - Risk Calculation" activity is analysed by the Information Security Manager, Asset Manager and Risk Manager to determine the actions to be taken to address it.
- **Quality framework** - Each risk identified in the "Identification of the Degree of Quality System- Risk Calculation" activity is analysed by the Information Security Manager, Quality Manager, Asset Manager and Risk Manager to determine the actions to be taken to address it.

The Risk and Opportunity Treatment Plan is therefore drawn up considering four types of action aimed at managing the risk.

- **Risk Acceptance**: Acknowledging that the risk may occur and planning to manage its impact when it does.
- **Risk Avoidance**: Implementing process changes to avoid the identified risk.
- **Risk Transfer**: Transfer the risk to an external organisation (e.g. insurance company).
- **Risk Mitigation**: Introducing new controls or modifying existing ones to reduce the current level of risk. The residual risk level should be considered when selecting appropriate controls.

Implementation of the Risks and Opportunities Treatment Plan and Monitoring the implementation of the Plan

Depending on the defined risk and opportunity treatment plan, controls are implemented based on a set of actions. Once the actions associated with the controls have been implemented,

the effectiveness must be assessed, the residual risks calculated, a decision made as to whether the residual risk is acceptable and, if not, further treatment. This is a cyclical process. Additionally, periodic reviews (at least once a year) of risk analysis and management are carried out in accordance with the activities defined above.
These two processes are universally applicable to risk analysis, and there is no need to adjust the process.

3.2 Risk Management software implementation tool

All these activities are recorded in the Risk Management application developed internally by Statistics Portugal. This application is prepared for risk management in the context of risk security, quality management and any other area that uses the procedure described above. All actions defined to deal with risks are potentially treated as objectives related to the context in which they are being analysed. Recognised as a valuable asset in risk management, this application significantly enhances the efficiency and effectiveness of the process. Its adaptable nature has facilitated the expansion of risk management approaches to other sectors within Statistics Portugal.

4. Main conclusions

To conclude, we would like to mention the main advantages and at the same time the main motivations for using a single approach to risk management.

- **Consistency and Efficiency**: By adopting the same methodology for both systems, organisations can promote consistency in their risk management approaches. This simplifies processes, saves time, and resources, and reduces the possibility of errors arising from different methods.
- **Enhanced Communication**: This can improve communication between teams, promote a broader understanding of organisational risks and facilitate collaboration on corrective and preventive actions.
- **Optimized Resource Utilization**: By using a unified methodology, organisations can maximise the use of human and financial resources. Staff can be trained in a single methodology that can be applied to both systems, eliminating the need for separate training for different approaches.
- **Strategic Alignment**: A common risk management methodology ensures that quality and information security objectives are aligned with the organisation's overall objectives. This allows for a more holistic approach to managing risks that impact the organisation as a whole.

- **Informed Decision Making**: A unified approach can provide a clearer and more comprehensive view of the risks faced by the organisation. This allows for better decision-making, as leaders have a more complete understanding of the risks and how they can impact organisational objectives.
- **Regulatory Compliance**: Regulatory requirements for information quality and security often overlap. Adopting a common methodology can facilitate compliance with these requirements, ensuring that all relevant aspects are effectively addressed and efficiently.

By embracing a single approach to risk management, organizations can reap these benefits, driving efficiency, effectiveness, and alignment across the organization's risk management practices.

References

ISO 27001:2013 – Information technlology, security techiques, Information security management systems – Requirements.

ISO 27005:2022 – Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

ISO 31000:2018 – Risk management Guideline.

ISO 9001:2015 – Quality management systems – Requirements.

European Statistics Code of Practice, 16th November 2017, Eurostat https://ec.europa.eu/eurostat/web/quality/european-quality-standards/european-statistics-code-of-practice