When security meets privacy we enhance quality

Jose Jabier Zurikarai Marcilla

Deputy director. Technical Coordination and Dissemination. Eustat. Basque Statistical Institute. Spain

Jesus Nieto Gonzalez

Head of IT Department. Technical Coordination and Dissemination. Eustat. Basque Statistical Institute. Spain

Abstract

Statistical confidentiality has always been a core value of official statistics. However, the big increase of data handling from both public and private sector has raised the awareness of potential data misuse; both belonging to individuals, companies or institutions.

Besides, connections between different data storage systems have made interconnectivity possible at the expense of a higher cost of risk. All the statistical process is carried out with interconnected systems, opening the door to unwanted access and intrusion. Any public institution is nowadays under the menace of cyber-attack. We must be able to ensure that the potential risk is under control, as we already do with the previous risks, and as it should be in any other public agency.

In statistics, we have a very high responsibility with our data and our systems. In fact, our data doesn't really belong to us, but to the respondents and that's why we must keep them completely safe. And our data collecting systems must be available 24/7.

In order to ensure this, it is not enough any formal statement telling confidentiality is our core value. We must keep the confidentiality of the data and the proper functioning of our data collection systems, and we also must be able to prove that we are doing that properly.

In Spain, the Public Electronic Services law sets the requirements for the Security Management of public institutions and as a result there is the "National Security Scheme" ruled by a Royal Decree. It contains, among others, the Security Policy and Minimum Requirements, Systems auditing processes and the Categorization of the Public Administration systems. Implementing the National Security Scheme means that a public organization must audit their Systems and check the level of compliance with the policies and requirements as well as the definition of its criticality level. After finishing all the process, an external authorized auditor will certify the level of compliance.

There are different methodologies to implement the National Security Scheme. Some of them are derived from international standards. For instance, the ISO/IEC 27000 family provides a set of standards for the Information Security Management (maybe it is the world best known).

The aim of this presentation will be how to apply Security Management to the Statistical Process, regardless of the methodology or the standards followed and focusing on which are the real issues to certify a statistical system as we have already done in EUSTAT.

Keywords: ENS, ISO/IEC 27000, Security Management, Statistical system, EUSTAT

1. Introduction

In official statistics we are very focused on confidentiality and privacy of data. Most of statistical laws set the obligations and compliances for statistical officers regarding privacy. We know what we can do and what we do not have to do under any circumstances. In the code of practice of Eurostat, the principle number 5 is “Statistical Confidentiality and Data Protection” and it says that “The privacy of data providers, the confidentiality of the information they provide, its use only for statistical purposes and the security of the data are absolutely guaranteed” and there are several indicators, with 5.5 which clearly states that “The necessary regulatory, administrative, technical and organisational measures are in place to protect the security and integrity of statistical data and their transmission, in accordance with best practices, international standards, as well as European and national legislation.”

Currently we ensure our data providers that their safety and privacy of their information is guaranteed, but is there any proof of that?

On the other hand we have seen the huge increase of electronic services, both public and private electronic services. Financial sector has evolved to on-line services, many of public services; tax-payment, students enrollment, medical-prescription and more are on-line services. In the end, there is a constant transaction of confidential information and there are services that must be available 24/7. Due to the raise in the number of transactions and services, risk and uncertainty have also increased accordingly. There are many different sources of risk, some of them are more traditional, like natural disaster, fire, floods and others are very closely related to the digitalization like cyber-attacks. But all of them can be harmful and in the case of an event, consequences and effects are real.

In official statistics we have data to protect and services to be guaranteed, mainly data collection services and dissemination services. And the real question is if we are protecting our business with proper policies and techniques.

2. Our choice

If we want to ensure that we are meeting the requirements stated by principle number five, we have to work on security: how can this be done?

The first answer would be ISO 27000. This standard for International Standards for Management Systems is aimed for “Information security, cybersecurity and privacy protection”, thus ISO 27000 is an Information Security Management System.

The document for ISO 27000 describes the general situation whit proper words:

4.1 General

Organizations of all types and sizes:

a) collect, process, store, and transmit information;

b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;

c) face a range of risks that can affect the functioning of assets; and

d) address their perceived risk exposure by implementing information security controls.

All information held and processed by an organization is subject to threats of attack, error, nature (for example, flood or fire), etc., and is subject to vulnerabilities inherent in its use. The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity. Enabling accurate and complete information to be available in a timely manner to those with an authorized need is a catalyst for business efficiency.

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management.

As information security risks and the effectiveness of controls change depending on shifting circumstances, organizations need to:

a) monitor and evaluate the effectiveness of implemented controls and procedures;

b) identify emerging risks to be treated; and

c) select, implement and improve appropriate controls as needed.

To interrelate and coordinate such information security activities, each organization needs to establish its policy and objectives for information security and achieve those objectives effectively by using a management system.

And it gives an overview of the ISMS

4.2.1 Overview and principles

An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS.

ISO 27.000 will always be a good starting point for Official Statistics. But we didn't go for it. The reason why is that we are under the requirements of spanish law and there are some differences that made us take another approach.

Spanish Certification Authority has its own methodology, named ENS which stands for "National Security Framework" (acronym for "Esquema Nacional de Seguridad"), based on open methodologies, like MAGERIT (acronym for "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información") which is a methodology for information systems risk analysis and management, accompanied by open standards, instructions, guides and recommendations, with the aim of improving the degree of cybersecurity of organisations (CCN-STIC Series).

Briefly explained, the ENS is a legal framework, which has considered the key points of security, and which allows it to be aligned with other security frameworks. Whereas ISO 27000 is more oriented to technical aspects, ENS is more focused in organizational aspects as it is aimed for public administration bodies.

Basically, all the Information Security Systems are just the same: a set of policies, procedures and guidelines established in an organisation, together with the resources and processes necessary to protect the information systems.

3. The security level and the certification

According to spanish law, there are certain requirements for any organization regarding the security management system. Depending on the security level for the assets, those requirements are more demanding. The levels stated are low, medium and high. These three levels are evaluated through the system, but in the end each level requires a different level of auditing:

1.- Low level system. Then self-evaluation is recognized and enough.

2.- Your system is medium level. It requires a extenal audition and evaluation of the audition by the central office for security which certifies the management system.

3.- Your system is high level. Is the same as the medium one regarding certification but the requirements and rules are more demanding.

4. Security Management System. Main elements adaptation

There are several elements part of a statistical security management system. All of them are essential to ensure that security is granted. The certification process adds the verification of the system, from the highest-level of security policies to the very precise issue like the inspection of fire extinguishers of the buildings.

On the other hand, and this can also be very important, we have “inserted” the Security Management System in our ISO 9000 set of procedures. This way we have a better integratation of the elements and ensure we manage the system without duplication and avoid unnecesary burden to the staff.

4.1 Security and Privacy Policy

This is the highest-level Policy, with the objectives or mission of the organization, the legal and regulatory frameworks, the security roles or functions, and the guidelines for structuring the system's security and privacy documentation.

Those are some extracts that help us with a better understanding of it:

- The main objective of the security and privacy policy of the information systems of Eustat is to guarantee the quality and protection of the information, ensuring compliance with the obligations derived from the duty of secrecy statistics, and the continued provision of services, acting preventively, supervising daily activity and reacting quickly to incidents.
- Other relevant objectives are compliance with security and privacy legislation and the achievement of full consciousness about security of the information among the staff.
- The policy is written in an extensive document. Its purpose is to establish the basis of the Information Security Management System. It must be able to set the appropriate arrangements to ensure security.

This policy applies to the whole set of Eustat ICT systems, which allow the institute to provide public service and all members of the organization, without exceptions, must know and comply with, regardless of the position and responsibility within it.

Eustat's ICT resources include all central systems, workstations, devices, storage systems, networks, applications (software) that are its property. Therefore, equipment not inventoried in the name of Eustat are out. However, if the corporate network is accessed through those equipments, they will be subject to the obligations established in this policy

Eustat staff are any person linked to the institute through an employment contract. Those collaborators who work with the institute and use its resources, they will be subject to the obligations established in this policy as well.

4.2 Privacy and security regulation: security document

It establishes technical and organizational measures necessary to guarantee the security of protected information (statistical information and personal data).

Its scope is the description of the main measures of security, derived from compliance with the European General Data Protection Regulation and the Organic Law on Data Protection; and the duty of statistical secrecy, as well as the EUSTAT Security Policy that is framed in the Basque Government Security Policy.

The technical and organizational measures are defined under the following sections:

A. It defines roles and duties:
   Information Manager -> General Director

Responsible for privacy measures -> Deputy Director of Technical Coordination and Dissemination

Data protection representative -> Computer technician and Legal technician

Security Manager -> Data proccess center Manager

Responsible for Services -> Deputy Director of Technical Coordination and Dissemination

Responsible for the System -> Head of the Information Systems Area

B. Creates the High-Level Security Group and the Technical Security Group
C. The guidelines, rules and procedures are the main part of this document, and they are defined for several assets: People, Statistical Activities, Personal data protection and IT systems architecture
D. Penalties

4.3. Setting the Scope

What are we considering when we are talking about security? What must be secured? All our information systems? We define the scope with the following sentence:

The information systems that support business processes for the collection of information, data storage, statistical exploitation, statistical analysis and dissemination of the results of statistical operations established through the current law of the Basque statistics plan, as well as the auxiliary systems to support their management.

4.4. Statement of Applicability

The Statement of Applicability, in the scope of the ENS, is the document that formalizes the list of security measures that must be applied to an information system according to its category.

Indeed it is very similar to the SoA of the ISO 27.001. In the ISO 270001 template for SoA we can find 114 controls divided into 14 distinct categories, while in the ENS template for SoA we can find 73 measures divided into 3 chapters.

5 Security Policies	A. Organizational framework

6 Organisation of information security 7 Human resource security 8 Asset management 9 Access control 10 Cryptography 11 Physical and environmental security 12 Operations security 13 Communications security 14 System acquisition, development and maintenance 15 Supplier relationships 16 Information security incident management 17 Information security aspects of business continuity management 18 Compliance	B. Operational framework C. Protection measures

4.5.- Systems Categorization

It is necessary to identify the information and services that are going to be secured as a result of the scope. In our case the information is the data we have stored as a result of our statistical process. It is mainly the data we have collected which will be in our databases. The services are those which help us with the entire process: data collection services, statistical software, or even dissemination services as our web site.

What we have to do is assess the impact that an incident that affects the security of the information and systems. To determine this impact, we must consider the five dimensions of the security: Availability [D], Integrity [I], Confidentiality [C], Authenticity [A], Traceability [T], to put in a nutshell [DICAT]

SYSTEMS	Availability	Integrity	Confidentiality	Authenticity	Traceability

Information *Dissemination DB*	Low Medium High	Low Medium High	Low Medium High	Low Medium High	Low Medium High
Information *Landing FS*	Low Medium High	Low Medium High	Low Medium High	Low Medium High	Low Medium High
….					
Service *Survey Platform*	Low Medium High	Low Medium High	Low Medium High	Low Medium High	Low Medium High
Service *Argus*	Low Medium High	Low Medium High	Low Medium High	Low Medium High	Low Medium High

As a result of our assesmente, the Category for our system is determined. In our case, for EUSTAT is MEDIUM. The category will be the result of the highest level in the categorization.

In the case of LOW category there is no need to certify externally the management system and self-evaluation is enough. To clarify, low Category does not mean there's nothing to worry about. It is more likely that the risk of your system's being really down and its effects during certain time are something you can live with without major issues, or better said, you can solve the effects easily and fast.

In the case of MEDIUM or HIGH, the management system must be certified, and proof of security measures must be provided.

4.6.- Risk Analisys

Risk analysis is a process that includes the identification of computer assets, their vulnerabilities and threats to which they are exposed, as well as their probability of occurrence and their impact, in order to determine the appropriate controls to accept, reduce, transfer or avoid the occurrence of the risk.

Risk analysis allows to determine what the system is like, how much it is worth and how protected it is, and to implement its safeguards (or countermeasures).

It is somehow an addition to the SoA (Statement of Applicability) and must be carried out continuously, whenever a change happens in our system, to update the SoA. Risk analysis

must be done at least once a year, and the Certification rules defines the framework for this analysis, in our case, for MEDIUM category:

A semi-formal analysis must be carried out, using a specific language, with a basic catalog of threats and defined semantics. That is, a presentation with tables that describe the following aspects:

- *Identify and qualitatively value the system's most valuable assets.*
- *Identify and quantify the most likely threats.*
- *Identify and assess the safeguards that protect against these threats.*
- *Identify and assess residual risk*

5. Conclusion

Our Security Managements System is built on both organizational and operational procedures which are integrated in our quality system for the IT Department (ISO 9001). We can ensure to any individual or organization that provides us their information that we have the proper system for the maximun safety about privacy concerns and we can give proof of that.

An information security framework is a tool for risk management, cyber-resilience and operational improvement, but it is not a magic wand to fix all our problems. In our case, obtaining the ENS certification has not meant that we have a flawless information system, but that we are more aware of the failures we have, that every year we are going to evaluate the existing risks and that we have Action plans for the implementation of measures that mitigate risks or correct the problems detected. Nothing more, nothing less.