International Journal of Engineering Insights: (2025) Vol. 3, Nro.1, Regular Paper
https://doi.org/10.61961/injei.v3i1.23

IT Security Balanced Scorecard based on ISO 27001:2022

Jorge Luis Velasco Téran · Renato M. Toasa

Received: 10 May 2025 / Accepted: 25 Sep 2025 / Published: 15 Nov 2025

Abstract: The growing need to protect the IT systems of telecommunications companies drives the development of monitoring tools based on international standards. This paper presents the development of an endpoint-oriented IT security Balanced Scorecard (BSC) based on the ISO 27001:2022 standard, in order to implement and monitor security controls in a telecommunications company. The main objective is to design a KPI visualisation system using Power BI that allows real-time evaluation of the specific security requirements of the standard. This work analyses the requirements of ISO 27001:2022 relevant to endpoints, selects key indicators based on the controls of the standard, also develops the BSC with tools that ensure the availability and usability of the data, and finally validates the effectiveness of the BSC against the stipulated security standards. It is concluded that the adoption of a Balanced Scorecard based on ISO 27001:2022 not only facilitates real-time decision making, but also reinforces the organisational culture oriented towards information protection, promoting business continuity and user and customer confidence.

Keywords Monitoring · Dashboard · Computer security · ISO · 27001:2022

1 Introduction

The growing threat to information security in the digital realm has created an urgent need for robust regulatory frameworks to protect the assets and privacy of organisations. Internationally, ISO 27001:2022 has established itself as the reference standard for the implementation of an Information Security Management System (ISMS), providing a structured approach to mitigate cyber risks. This standard has been adopted by several global organisations, especially in sensitive sectors such as telecommunications, where the protection of data and critical infrastructure is crucial. Telecommunications companies, being a key communication and data bridge, are a frequent target of cyber-attacks, underlining the importance of having effective IT security mechanisms in place [1]. In Ecuador, the adoption of international cyber security standards is progressing, although there are still significant challenges for companies, especially in the telecommunications sector, to implement solid cyber protection frameworks. The Ley Orgánica de Protección de Datos Personales and the Reglamento a la Ley de Telecomunicaciones are examples of national efforts to ensure information security and privacy. However, many Ecuadorian companies still face challenges in integrating these regulations with their internal security management systems[2] . This article proposes the implementation of a Balanced Scorecard (BSC) for IT security, based on ISO 27001:2022, as an effective solution to address these challenges. By integrating key performance indicators (KPIs) tailored to the needs of the telecommunications sector, the BSC can provide a comprehensive tool for risk monitoring, policy compliance assessment and strategic decision making. This approach not only responds to global security needs, but also to the particularities of the Ecuadorian environment, enabling telecommunications companies to improve their ability to respond to security incidents and strengthen the confidence of their users.

1.1 Related Works

A review of the literature in scientific databases found the following related studies.
ISO 27001 is a globally recognised standard for information security management. Its adoption enables organisations to effectively manage the risks associated with cybersecurity and protect critical information assets. The latest version, ISO 27001:2022, incorporates

Jorge Luis Velasco Téran
Universidad Tecnológica Israel
Quito, Ecuador
E-mail: e1719068098@uisrael.edu.ec

Renato M. Toasa
Universidad Tecnológica Israel
Quito, Ecuador
E-mail: rtoasa@uisrael.edu.ec

improvements in risk management and provides a more flexible framework to adapt to emerging cyber threats. Several studies highlight the benefits of implementing this standard, especially in increasing resilience to cyber-attacks and improving data privacy management. According to one study [3], Organisations that adopt ISO 27001 experience greater effectiveness in protecting their digital infrastructure and strengthening their compliance processes.

The telecommunications sector, due to its essential role in the transmission of data and services, is particularly exposed to cyber risks, such as attacks on its critical infrastructure and data theft. The implementation of international standards such as ISO 27001 in this sector has been shown to improve IT security management. Telecommunications companies that adopt these standards are said to significantly improve operational efficiency and the protection of their networks [4]. In [5] conclude that the adoption of security frameworks also facilitates compliance with international regulations, which increases the competitiveness of companies in the global marketplace.

In Ecuador, although there are legislative advances, such as the Organic Law on Personal Data Protection and the Regulation to the Telecommunications Law, there are still challenges in the effective implementation of security frameworks in companies in the telecommunications sector. According to the Ministry of Telecommunications of Ecuador[2], Ecuadorian companies face obstacles such as lack of technical training and integration of security policies with national regulatory frameworks. In the academy, research has also been carried out on the proposed topic. For example, a degree project of an Ecuadorian University proposes an Information Security Management System based on the ISO 27000: 2013 standard, which will protect the integrity, availability and confidentiality of information [6], On the other hand, state institutions also address an Integral Command Control (CMI) Policy of Use, carried out by the Ministry of Government, Police and Worship, in coordination with the National Police, as a fundamental actor of the Citizen Security Policy, have assumed the commitment to self-evaluate the operational management of the police institution to examine strategies associated with result goals with respect to crime behaviour and the application of efficient and timely actions for the prevention and control of crime, as well as to evaluate their effectiveness on an ongoing basis, taking the necessary corrective measures to achieve the strengthening of Citizen Security[7]. In this context, a Balanced Scorecard (BSC) based on ISO 27001 offers an effective solution for monitoring security risks and aligning these indicators with strategic objectives. It should be noted that BSCs allow for a comprehensive measurement of organisational performance, facilitating decision making and the implementation of security policies. In the field of IT security, a BSC adapted to ISO 27001 helps to manage technological risks and improves organisational transparency[8].

Studies as in [9] The results show that the integration of ISO 27001 with a BSC in the telecommunications sector improves the effectiveness of decision-making and facilitates the alignment of security efforts with business objectives, which contributes to better protection of information assets.

The document is organized as follows: Section 1 includes the Introduction, Section 2 the Methodology, Section 3 the Proposal, and Section 4 the Conclusions.

2 Methodology

2.1 Research methodology

For the development of an ISO 27001:2022-based 'Balanced Scorecard for Endpoint Security (BSCSS) for a telecommunications company', the following research process will be used:

Qualitative research approach The choice of a qualitative research approach is justified by the complex nature of the topic and the need to gain a comprehensive and general understanding, allowing both the individual experiences and perceptions of participants to be explored, thus providing valuable insights and in-depth understanding. By integrating these perspectives into the Information Security Balanced Scorecard, a more complete and contextualised view of the challenges, practices and opportunities related to information security will be obtained, identifying areas for improvement, adapting strategies and making decisions to strengthen information security in the enterprise [9].
Convenience sampling Convenience sampling is justified by the difficulty of accessing a specific population, such as computer security experts and professionals in the telecommunications sector. Since these individuals are limited in number and not always readily available, convenience sampling allows for flexible selection of participants, taking advantage of available connections and contacts.

This facilitates sample formation without requiring a specific population frame and allows for a variety of perspectives relevant to the study.

Interview-based research technique Semi- structured interviews with information security experts and telecommunications professionals will provide detailed insights into the specific challenges and implementation requirements of the Balanced Scorecard. These in-

terviews will enable an in-depth exploration of participants' experiences and perspectives.

2.2 CRISP-DM Methodology

The cross-industry standard process for data mining (CRISPDM) is a framework for translating business problems into data mining tasks and carrying out data mining projects independent of both the application area and the used technology [3]. It is a widely adopted industry-oriented implementation of the generic Knowledge Discovery (KD) process, as described in [10].

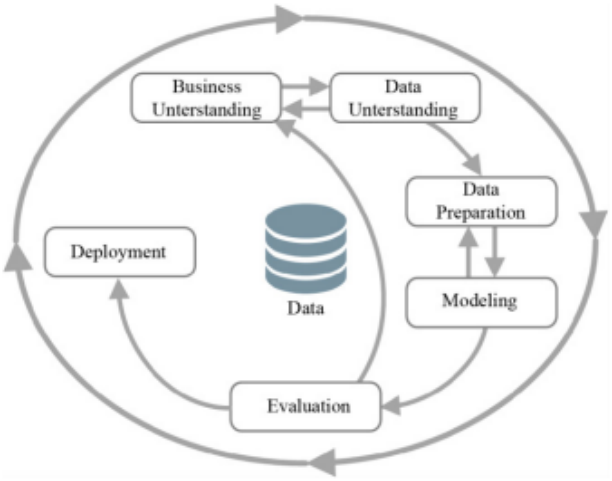

Fig. 1 CRISP-DM Phases.

The phases of the CRISP-DM methodology are:

1. Phase 1: Understanding the Business
2. Phase 2: Understanding the data
3. Phase 3: Data Preparation
4. Phase 4: Modelling
5. Phase 5: Evaluation
6. Phase 6. Deployment

3 Proposal

3.1 Development of CRISP DM phases

Phase 1: Understanding the Business In order to better understand the requirements that are required by the company's staff in terms of IT security and compliance with ISO 27001:2022, the following activities are necessary:

- Meetings with IT security experts and company professionals, in order to conduct interviews to obtain an overview of the problems that exist and to better understand the requirements of the PC Infrastructure staff, in order to provide solutions to the current problems in this area.
- Review and analysis of the ISO 27001:2022 standard in line with the company's requirements.

Phase 2: Understanding the data In order to understand all the information involved in the development of the CMISPF, it is necessary to identify the data that will be used and the source of the data, the files that will be used are detailed below:

- Security Console: Microsoft Intune, Microsoft Defender, Active Directory
- PC formatting file
- Service desk formatting ticket information
- Application tickets USB whitelist
- Application Tickets for Local Administrator Users

Phase 3: Data Preparations Once the sources of information have been identified, it is necessary to prepare the data from these sources in order to make them part of the CMISPF, by doing the following:

- Select data that is related to compliance with ISO 27001:2022.
- Perform data cleansing, i.e. rectify or remove inconsistent, duplicate or erroneous information.
- Establish security policies and key performance indicators (KPIs), which will be measured in CMISPF.
- Create a centralised database, which will be fed by the different sources of information, as detailed in point 2 Phase 2: Understanding the data.
- Verify that the data that will be part of the database is in an appropriate format, e.g. date format, text format, etc.

Phase 4: Modelling In order to build models for data analysis based on the ISO 27001:2022 Standard and to be part of the CMISPF, which will help the monitoring and management of the IT security of a telecommunications company, the following will be carried out:

- Determine the security policies and KPIs that comply with ISO 27001:2022 to be monitored through the CMISPF, which will be developed through the Power BI tool.
- Define the method of evaluation of the model, for the development of the CMISPF the method to be used will be through user testing with the company's IT security experts.
- Establish the test data to be used in the development of the CMISPF.

Phase 5: Evaluation

The evaluation of results will assess the effectiveness of the models designed and the accuracy of the security policies and performance indicators according to ISO 27001:2022, including:

- Compare the CMISPF against the business requirements that were established in phase 1.
- Verify that the CMISPF complies with the company's requirements.

Phase 6. Deployment Develop the CMISPF prototype, for which the following should be done:

- Perform an initial design of the Balanced Scorecard, which should include the architecture and design of the database, dashboard structure and user interfaces.
- Development of the main dashboards, which should be clear, user-friendly and present information that is relevant to the user.
- Establish and configure the automatic processes that will continue to feed the database.
- Execute unit tests of the CMISPF, in order to assess whether the functionality of the CMISPF corresponds to what is expected according to the company's requirements.
- User testing, i.e. running functional tests with the end user, in order to make adjustments if necessary.
- Implement the developed CMISPF prototype, in a pilot environment, so that it can be used by the PC Infrastructure area.

3.2 Proposal Architecture

The CMISPF through an automatic process will take the information from Microsoft Intune, Microsoft Defender, Active Directory from cloud-type repository, PC formatting, USB white list and local administrator users, with which it will feed the Power BI database, with this information the PC Infrastructure staff, through a control panel, will verify compliance with the indicators based on the ISO 27001:2022 Standard.

In Figure 2 it can be seen that the architecture and the main components are related so that the developer is always in contact with the information sources (Power BI can read a large amount of data types) that can come from different sources, it has several extra applications that can be easily incorporated into the system, there is also an online connection for other users who wish to access the information or its results by means of queries.

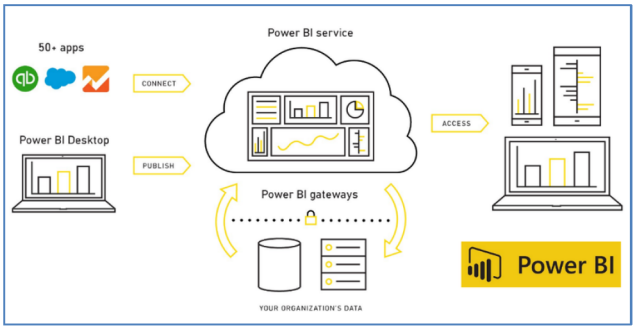

Fig. 2 Architecture with Power BI

3.3 Computer security policies

For the development of the CMISPF, the following IT security policies have been defined to be implemented:

Operation of anti-virus and anti-malware software

- Implementation of specialised anti-virus and anti-malware software on all endpoints (devices).
- Perform automatic software updates so that the company and its information is protected against new virus definitions and threats.
-

Patches and updates procedure

- Procedure for continuous application of security patches and updates to endpoints.
- Continuous monitoring of the availability of new patches to be applied immediately.

Acceptable use policies

- Definition of the use of endpoints in the company, i.e. permitted and prohibited devices.

Access and Authentication

- Only authorised personnel may be granted administrator permissions.

Test

In order to carry out a proper quality assurance and quality control (QA) in the development of the CMISPF, the following documents have been elaborated:

- Test plan: This describes the steps to be taken and the approach to testing, in order to ensure the quality and performance of the project.
- Functional tests report: In which the functional tests carried out by the PC Infrastructure area are evidenced and the use of the CMISPF is authorised.
- Non-functional test report: In which the technical tests carried out by the CMISPF are evidenced.

4 Conclusions

The Endpoint Security Balanced Scorecard project was developed based on the controls in ISO 27001:2022, thus aligning with international standards related to IT security, which allows for control and monitoring of the risks that may occur in the telecommunications company. The CMISPF has a centralised display of key performance indicators (KPIs), for which special rules have been established to enable operational decisions to be taken. Power BI is a powerful technological tool that has enabled the development of the CMISPF, which has facilitated the visualisation of information in real time through interactive panels and graphs in order to make it more comprehensible for the user to interpret it. Through the verification of the operation of the CMISPF, it has been possible to validate that it complies with the IT security controls established in the ISO 27001:2022 Standard and which have been requested by the PC Infrastructure area, thus providing a tool for the management and monitoring of IT security.

References

1. B. Krumay, E. W. Bernroider, and R. Walser, "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the nist cybersecurity framework," in *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23*. Springer, 2018, pp. 369–384.
2. A. Michelena, "Ministerio de telecomunicaciones y de la socidad de la información," *Quito, Pichincha, Ecuador. Obtenido de https://www. telecomunicaciones. gob. ec/wp-content/uploads/2020/06/ACUERDO-MINISTERIAL-12-signed-1.pdf*, 2020.
3. J. Brenner, "Iso 27001 risk management and compliance." *Risk management*, vol. 54, no. 1, pp. 24–29, 2007.
4. M. I. Ladino, P. A. Villa, and A. L. E. María, "Fundamentos de iso 27001 y su aplicación en las empresas," *Scientia et technica*, vol. 1, no. 47, pp. 334–339, 2011.
5. F. Morales, S. Toapanta, and R. M. Toasa, "Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información," *Revista Iberica de sistemas e tecnologías de informacao*, no. E27, pp. 553–565, 2020.
6. D. A. Hernández Mera, "Diseño de un esquema de seguridad informática para el área de sistematización de la universidad israel, aplicando iso 27002 y csf de nits." Master's thesis, Quito, Ecuador: Universidad Tecnológica Israel, 2023.
7. D. Pontón Cevallos, "Progresismo y tecnología policial: análisis del boom punitivo en ecuador," *Perfiles latinoamericanos*, vol. 31, no. 62, 2023.
8. E. R. Armenta and A. L. I. Carrillo, "Towards an implementation of information technologies governance," in *2022 IEEE Mexican International Conference on Computer Science (ENC)*. IEEE, 2022, pp. 1–6.
9. E. Falcón Huallpa and E. J. Martínez Zambrano, "Propuesta de mejora para la gestión de seguridad de la información sgsi bajo normas iso 27001, para el departamento de análisis de telecomunicaciones de la unidad nacional de telecomunicación móvil"(quito-ecuador)," 2023.
10. C. Schröer, F. Kruse, and J. M. Gómez, "A systematic literature review on applying crisp-dm process model," *Procedia Computer Science*, vol. 181, pp. 526–534, 2021.

License