2023 International Conference on Information Technologies (InfoTech-2023), Proceedings of the IEEE Conference, Rec # 58664
20-21 September 2023, Bulgaria

Data Leakage Prevention in ISO 27001: Compliance and Implementation

Veselin Monev
Information security practitioner
Veselin.Monev@tutanota.com

2023 International Conference on Information Technologies (InfoTech) | 979-8-3503-3805-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/INFOTECH58664.2023.10266873

Abstract – ***Control 8.12, Data Leakage Prevention*, was introduced in the 2022 version of the ISO 27001 standard. Information security professionals responsible for ensuring compliance with the latest standard should have a thorough understanding of how to implement this control properly. The present paper presents an in-depth analysis of this requirement and proposes several practical approaches for compliance and successful implementation.**

Keywords – **data; leakage; prevention; ISO 27001; implementation.**

I. Introduction

The proliferation of data confidentiality loss in organisations worldwide has raised the necessity for effective data leakage prevention measures. This need has been acknowledged in the most recent version of the ISO 27001:2022 standard, which introduced a control for *data leakage prevention*. However, information security professionals may still face challenges in implementing data leakage prevention measures due to the lack of a universally accepted definition and the potential overlap with related terms such as *data loss, data breach*, and *data exfiltration prevention*.

This research presents a novel contribution by proposing

- A comprehensive definition of data leakage prevention by analysing relevant ISO 27002:2022 guidance through core aspects of information security theory.
- Four approaches to demonstrating compliance with the relevant control in ISO 27001:2022
- Three approaches for implementing data leakage prevention measures.

The presented insights provide valuable guidance to information security practitioners in achieving compliance with ISO 27001:2022 and ensuring the effective implementation of relevant security controls. Organisations can utilise these approaches by tailoring them to their unique needs, circumstances, and preferences. Ultimately, this can enhance security assurance, procedural maturity, or control effectiveness, leading to a more secure organisation.

II. Defining Data Leakage Prevention

This section defines the term *data leakage prevention* and examines several essential aspects of it.

A. *Definition of Data Leakage Prevention*

The terms *Data Leakage Prevention* and *Data Loss Prevention* are frequently used interchangeably and have a close association. Despite being referenced in several security guidelines, publications, and standards [1] [2], their definitions lack consensus. To establish a clear understanding in this study, the author has derived a working definition from the ISO 27002:2022 standard [3], which provides guidance on the implementation of ISO 27001:2022 [4]:

Data leakage prevention is a set of organisational, technical, people and physical controls for detecting and preventing unauthorised disclosure and extraction of sensitive information from systems, networks and other devices by individuals or systems.

Based on the above definition, the author made the following deductions:

- Data leakage prevention primarily concentrates on protecting the *confidentiality* of sensitive electronic data, although it might also extend to verbal or paper-based information. In contrast, other security goals include the protection of the availability and integrity of information;
- The types of *controls* include policies, procedures, instructions, training, awareness and other *organisational* safeguards; They can also include *technical* measures, such as security tools for endpoint protection, web protection, and a dedicated Data Loss Prevention (DLP) solution; *people* measures, such as contract provisions and security incident reporting; and *physical* measures, such as media destruction devices and mantraps;
- The selected controls should serve the security functions *prevent* and *detect*, even though some might also qualify as *protect* or *identify*; The functions *response* and *recover* would be not applicable or at least not the main focus;
- The assets in the scope of the control are *networks*, *devices* and *systems*, such as servers, endpoints, networking and storage equipment, applications, portable media, printers, and others;
- The data can be both – *data* and *information* deemed sensitive, e.g. non-public, as per an established information classification scheme or in the absence of such (when an organisation does not fully comply with ISO 27001) – according to the organisation's perception of sensitivity;
- The related risk is *the unauthorised disclosure and extraction* of sensitive information from the assets in terms of established formal or informal organisational regulations for information security, such as a security incident management policy, rules for access control, information transfer, information handling, and cryptographic policy.

979-8-3503-3805-8/23/$31.00 ©2023 IEEE

- The threats are *internal* and *external* for an organisation's personnel and systems and can involve sources such as employees, contractors, partners, suppliers, consultants, guests, IT applications, APIs, cloud platforms, and others. These threat types are typically specified as social engineering, human errors, insider threats, malicious hackers, and malware.
  It is worth noting that the definition of data leakage in this paper diverges from the definition put forth in NIST SP 800-137 [5], which characterises it as the unintentional exposure of data, such as through the loss of a laptop or USB drive, while intentional data theft is instead referred to as "data loss". However, this definition from 2011 is overly restrictive and not keeping with the guidance provided in ISO 27002.
- The *8.12 Data leakage prevention* control is a high-level abstract of a set of controls (measures) with a more specific purpose.

B. Data Leakage Prevention in the Context of Information Security

Information security is the preservation of the confidentiality, integrity, and availability of information and systems. When applicable, other security goals should be added to this definition, such as authenticity, auditability, accountability and privacy [6]. Based on this definition, the data leakage prevention control aims to preserve the confidentiality and privacy of information. It is important to acknowledge that pertinent controls can facilitate the attainment of other goals, such as the integrity and availability of data. It is worth noting that organisations have already implemented such controls, which may be identified by distinct nomenclature, including "cryptographic controls," "encryption controls," "access management," “information classification”, or "malware defence."

In summary, the essential aspects of *data leakage prevention,* as defined in this paper, are shown in Table 1.

TABLE 1. ESSENTIAL ASPECTS OF DATA LEAKAGE PREVENTION

Data Leakage Prevention	
Security goals	Confidentiality and privacy
Security functions	Primary: detect and prevent Secondary: protect
Applicable control types	Primary: technical, organisational, people Secondary: physical
Scope of assets for protection	Networks, devices and systems
Scope of information types for protection	Primary: digital data Secondary: paper, verbal information
Scope of classified information	All sensitive types within the information classification scheme
Risks	• Unauthorised disclosure • Unauthorised extraction
Threat origin	• Internal and external • Humans and systems
Threat types	• Insider threat (unintentional or intentional misconduct) • Social engineering • Malicious hackers • Malware
Applicable documentation, including policies and procedures (non-exhaustive examples)	• Information Classification • Information Handling and Transfer • Acceptable Use • Access Control • Security Incident Management • Cryptography • Operational procedures

III. COMPLIANCE WITH ISO 27001

A. Basic Compliance Requirements

ISO 27001 explicitly requires implementing a set of measures for data leakage prevention. Although supporting documentation is not required, organisations can consider integrating data leakage prevention-related provisions into existing documents to increase procedural control maturity or prepare for an audit. These documents could include the Information Classification Policy, Acceptable Use Policy, or operating procedures. Also, defining a working definition for data leakage prevention may be beneficial. Additionally, D. Kosutic [7] suggested categorising the adopted measures into three groups: technology, organisation/processes, and people, which align with three of the four groups of controls within the Annex A of ISO 27001, except for *Physical controls*.

Another consideration is updating the risk catalogue and performing a risk assessment for this control. The Statement of Applicability must also be updated.

The overarching objective should be achieving compliance through a reasonable set of measures (controls) to detect and prevent unauthorised disclosure or extraction of sensitive data.

B. Approaches for Compliance with ISO 27001

In order to meet the fundamental requirements of ISO 27001, it is essential to consider several approaches depending on the extent of data leakage prevention measures already implemented in an organisation. Irrespective of the chosen approach, adding the data leakage risk to the risk catalogue, conducting a risk assessment, and updating the Statement of Applicability are indispensable steps that must be taken.

Scenario 1: Reasonable controls are implemented

In this scenario, the risk assessment and possibly other types of reviews, such as a gap assessment and maturity assessment, have determined that the organisation in scope has implemented a compliant/adequate set of controls for data leakage prevention. There is no need to modify existing controls or introduce additional ones. Hence, at least three approaches to demonstrating compliance should be considered. They are presented in the following paragraphs.

Approach 1: Preparing argumentation and evidence

Intentions

Demonstrate compliance with minimal preparation and effort.

Recommended actions

- Discuss the current controls with the responsible staff to have a better understanding of the current state;
- Review the existing documentation relevant to data leakage prevention – policies, procedures, templates, reports, and others;
- Take notes in preparation for the next audit;
- Prepare potential supporting evidence for the next audit.

Approach 2: Creating and updating documentation

Intentions

Improve the procedural maturity of the security controls and increase the security assurance level.

Recommended actions

- Discuss the current controls with the responsible staff and note suggestions for improvement;
- Review and update the existing documentation relevant to data leakage prevention;
- Take notes in preparation for the next audit;
- Prepare potential supporting evidence for the next audit.

Approach 3: Improving and expanding existing controls

Intentions

Improve the current level of data leakage prevention in terms of efficiency, effectiveness or maturity of the security controls. Also, increase the level of security assurance.

Recommended actions

- Engage in discussions with the responsible staff and, if applicable, an external consultancy to assess the current state of controls in place. Take notes on suggestions for improvement;
- Prepare a plan for modifying existing controls or implementing new ones for data leakage prevention; Consider the established organisational practices for planning, operations, and compliance;
- Implement the planned measures by modifying existing security controls and introducing new ones. Utilise additional guidance available in ISO 27002, Secure Controls Framework [8], as well as vendor-specific guidance [9] to make changes;
- Introduce new relevant security controls as part of an IT change or a project;
- Review and update the existing documentation relevant to data leakage prevention.

Scenario 2: Controls are partially implemented or not implemented

In this scenario, the risk assessment and possibly other types of reviews, such as a gap assessment and maturity assessment, have determined that non-compliant/ inadequate (e.g. ineffective) controls have been implemented for data leakage prevention within the organisation in scope. In order to demonstrate compliance, additional actions are required, as explained in the fourth compliance approach presented next.

Approach 4: Implementing new controls

Intentions

Modify existing controls and introduce additional ones to comply with the data leakage prevention requirement.

Recommended actions

- Engage in discussions with relevant staff and an external consultancy, if necessary, to review the results of the risk assessment. Identify deficiencies or gaps, and evaluate available resources for effective data leakage prevention;
- Prepare a plan for implementing data leakage prevention based on the established organisational practices for planning, operations, and compliance;
- Implement the planned measures by modifying existing security controls and introducing new ones. Utilise additional guidance available in ISO 27002, Secure Controls Framework, as well as vendor-specific guidance to make changes;
- Review and update the existing documentation relevant to data leakage prevention;
- Prepare potential supporting evidence for the next audit.

The suggested compliance approaches are a practical starting point for consideration before modifying security controls or implementing new ones. The actual security controls should be organisational-specific and are discussed in the next part.

IV. Implementation Approaches

In this part, three implementation approaches for data leakage prevention are proposed. Based on them, specific security controls can be defined. They should be tailored to the specifics and requirements of the organisation in scope.

A. Utilising ISO 27002:2022

One of the primary sources of information for data leakage prevention is the ISO 27002 standard. It provides guidance on implementing all of the Annex A-controls within ISO 27001. This norm explicitly mentions the following measures:

- Information classification to allow for identifying and protecting sensitive information;
- Technical security monitoring to identify data leakage via email, file transfers, mobile devices, and portable storage devices;
- Taking specific actions to prevent data leakage via these channels, e.g. quarantining emails containing sensitive information;
- Organisational controls such as policies for access control and secure document management.

Guidelines from solution vendors or organisations such as the National Institute of Standards and Technology (NIST) or Secure Controls Framework Council, LLC (SCF Council) can also be used to define and establish appropriate controls.

B. Utilising a Data Loss Prevention Solution

A dedicated *Data Loss Prevention (DLP)* solution for endpoints, networks, storage, and cloud systems could serve as direct evidence for compliance. Such a solution can supplement other controls by allowing more effective data leakage detection and prevention. Relevant configurations need to have an adequate scope and DLP policies (configurations) tailored to the sensitive data types of the organisation. Key capabilities of such solutions include [10]:

- Extensive visibility of data in use, data at rest, and data in motion;
- Context information for quick response to data leakage incidents;
- Automated and manual actions directly through the solution interface to respond, escalate, quarantine, restore, and block events of potential data leakage;
- Awareness and coaching capabilities to modify user behaviour;
- Centralised management of DLP policies;
- Behaviour analytics to identify anomalies.

C. Mapping and Aggregating Security Framework Controls

Another valuable approach is mapping and aggregating relevant ISO 27001 controls to data leakage prevention measures. The same can also be done with other security frameworks. The results can be useful for developing a security policy or strategy dedicated to data leakage prevention. Table 2 presents a high-level overview of the author's approach.

TABLE 2. SAMPLE OF SECURITY CONTROLS RELEVANT TO DATA LEAKAGE PREVENTION

Control 1: Management of weaknesses
Identifying and managing weaknesses that can be exploited and lead to data leakage. Weaknesses can be detected by vulnerability scans, penetration tests, audits, other security solutions, and incident reporting.
Control 2: Security in projects
Every project must include security requirements to comply with internal and external regulations. This control allows for early consideration of any data leakage-related measures and how they should be maintained during the entire lifecycle of a given (software) solution. If a dedicated DLP solution is in use, a project management team should account for the potential need to modify the DLP policies accordingly.
Control 3: Monitoring and event handling
Monitoring and event-handling capabilities should be implemented for data in motion, data in use and data at rest. They should provide sufficient information to their recipients to take action where necessary. These actions include acting upon a potential data leak or drafting recommendations to improve existing controls. Monitoring is available for networks, systems and devices and could be facilitated with solutions for Extended Detection and Response (XDR), Security Information and Event Management (SIEM), Network Detection and Response (NDR), Data Loss Prevention (DLP), and others.
Control 4: Third-party risk management
Measures should be in place for continuous risk management of third parties, such as IT suppliers. These measures should help detect and prevent data leakage caused by a third-party system or a person, part of the extended security exposure of an organisation. This control can be achieved with a process for "supplier risk assessment", data handling policy, and access control rules for third-party accounts.
Control 5: Perimeter security
Various technical tools can support data leakage prevention at the organisational borders, such as firewalls, intrusion prevention systems (IPSs), Web Filtering, Email Filtering, Acess Controls Lists, Virtual Private Network (VPN), and data encryption methods.
Control 6: Data exchange/export channels control
Several controls related to data leakage prevention can be utilised, such as email encryption; enforcing encrypted file transfer protocols (SFTP, HTTPS); electronic data classification based on sensitivity levels; configurations for restrictions of removable media devices; content filtering tools; access and authorisation management solutions.
Control 7: Access control and authorisation
Along with conventional controls for access control and authorisation, which aim to apply the principles of need-to-know and least privilege when access and permissions are granted, modified, and revoked, there are also technical solutions for privileged user monitoring, as well as access and usage monitoring. This type of monitoring is useful for detecting and preventing dangerous actions with sensitive data or assets.
Control 8: Media disposal
Media disposal is an essential measure for data loss prevention, which involves the secure and responsible management of electronic devices that have reached the end of their useful life. By properly disposing of electronic devices, organisations can prevent unauthorised access to sensitive data, thus minimising the risk of data leakage.

V. CONCLUSION

In conclusion, this paper explored the concept of *data leakage prevention* within ISO 27001:2022 and ISO 27002:2022. A definition for data leakage prevention was proposed and then analysed using core concepts of the information security theory, including security functions, risks, threats, controls, and scope. The study revealed that organisations typically already have relevant security controls in place that they name with a specific nomenclature.

Next, the control for data leakage prevention in ISO 27001 was analysed from a compliance perspective, followed by a proposal of four approaches for achieving and demonstrating compliance with the norm, depending on an organisation's current state of data leakage prevention. Organisations should also consider these approaches to improve procedural maturity and increase control effectiveness or security assurance.

Lastly, three implementation approaches for data leakage prevention were proposed, including:

➢ Utilising ISO 27002 as guidance;
➢ Utilising a dedicated DLP-branded solution;

- ➢ Mapping and aggregating relevant controls from a security framework to data leakage prevention measures.

Overall, the provided insights into data leakage prevention can be helpful to organisations to protect their sensitive data from unauthorised exfiltration or disclosure and simultaneously comply with the relevant control in ISO 27001.

References

[1] "data loss prevention," NIST, 2023. [Online]. Available: https://csrc.nist.gov/glossary/term/data_loss_prevention. [Accessed April 2023].

[2] "What is Data Loss Prevention (DLP)?," Fortinet, [Online]. Available: https://www.fortinet.com/resources/cyberglossary/dlp. [Accessed April 2023].

[3] ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls, Geneva: ISO copyright office, 2022.

[4] ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Geneva: ISO copyright office, 2022.

[5] K. Dempsey, N. S. Chawla, A. Johnson and e. al., "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," NIST, Gaithersburg, 2011.

[6] V. Monev, “Measuring the Optimal Information Security Complexity for Blockchain Operations,” IEEE, St. St. Constantine and Elena, Bulgaria, 2020.

[7] D. Kosutic, "Detailed explanation of 11 new security controls in ISO 27001:2022," Advisera, [Online]. Available: https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/. [Accessed April 2023].

[8] "SCF Resources," [Online]. Available: https://securecontrolsframework.com/scf-download/. [Accessed April 2023].

[9] "ISO 27002:2022, Control 8.12 – Data Leakage Prevention," ISMS.online, [Online]. Available: https://www.isms.online/iso-27002/control-8-12-data-leakage-prevention/. [Accessed April 2023].

[10] Symantec, "Symantec® Data Loss Prevention Core Solution," [Online]. Available: https://docs.broadcom.com/doc/data-loss-prevention-core-solution. [Accessed April 2023].