Data Leakage Prevention in ISO 27001: Compliance and Implementation

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

20-21 September 2023, Bulgaria

Veselin Monev, PhD

Data Leakage Prevention in ISO 27001: Compliance and Implementation

Problem

- New requirement for Data leakage prevention within the latest version of ISO 27001:2022;
- No consensus on the definition of Data leakage prevention;
- Need to implement reasonable data leakage prevention measures within organisations.

Solution

- Working definition for Data leakage prevention, aligned with ISO 27002:2022;
- Proposal of approaches for compliance with ISO 27001:2022;
- Proposal of approaches for scoping Data leakage prevention measures.

Data Leakage Prevention in ISO 27001: Compliance and Implementation

DEFINING DATA LEAKAGE PREVENTION

- Definition derived from the guidance in ISO 27002:2022;
- Merging the NIST definitions for *Data leakage prevention* and *Data loss prevention.*

Security goals	Confidentiality and privacy
Security functions	Primary: detect and prevent Secondary: protect
Applicable control types	Primary: technical, organisational, people Secondary: physical
Assets for protection	Networks, devices and systems
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

Data Leakage Prevention in ISO 27001: Compliance and Implementation

APPROACHES FOR COMPLIANCE WITH ISO 27001:2022

Approach 1: Preparing argumentation and evidence
Intentions Demonstrate compliance with minimal preparation and effort.

Approach 2: Creating and updating documentation
Intentions Improve the procedural maturity of the security controls and increase the security assurance level.

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.

Approach 4: Implementing new controls
Intentions Modify existing controls and introduce additional ones to comply with the data leakage prevention requirement.

Data Leakage Prevention in ISO 27001: Compliance and Implementation

APPROACHES FOR IMPLEMENTATION OF DATA LEAKAGE PREVENTION MEASURES

A. Utilising ISO 27002:2022

B. Utilising a Data Loss Prevention Solution

C. Mapping and Aggregating Security Framework Controls

- **Control 1:** Management of weaknesses
- **Control 2:** Security in projects
- **Control 3:** Monitoring and event handling
- **Control 4:** Third-party risk management
- **Control 5:** Perimeter security
- **Control 6:** Data exchange/export channels control
- **Control 7:** Access control and authorization
- **Control 8:** Media disposal