Suitability of Information Security Frameworks for an IT-Centric ISMS

2024 International Conference on Information Technologies (InfoTech-2024)

Proceedings, 11-12 September 2024, Bulgaria

Veselin Monev, PhD

Suitability of Information Security Frameworks for an IT-Centric ISMS

Problem

- Establishing a holistic Information Security Management System (ISMS) is complex;
- Non-IT units may be minimally involved in ISMS implementation;
- IT departments face challenges in applying multidisciplinary implementation approaches.

Solution

- Establish an IT-centric ISMS due to organisational constraints;
- Apply a method to evaluate and select the most suitable controls from security frameworks.

Limitation

- The approach may not suit externally mandated security controls.

Suitability of Information Security Frameworks for an IT-Centric ISMS

Information Technology

Perspectives Towards an IT Organisation	Components
Infrastructure	IT assets, IT software, IT hardware, IT networks.
Human factors	IT personnel, IT department, IT competencies, IT knowledge and skills, IT management, IT governance, IT culture.
Services	IT support, IT solutions, IT processes, information.

Security Frameworks

- Classification 1:
  - Law and regulations;
  - Standards and guidelines;
- Classification 2:
  - Program frameworks (e.g. NIST Cybersecurity Framework, ISO 27001);
  - Control frameworks (e.g. CIS Critical Security Controls and NIST SP 800-53);
  - Risk frameworks (e.g. NIST 800-30 and ISO 27005);
  - Hybrid frameworks (e.g. COBIT, GDPR, SABSA).

Suitability of Information Security Frameworks for an IT-Centric ISMS

Criteria for Suitability of Controls

- ***Criterion 1:*** The control pertains to assets managed by the IT unit;
- ***Criterion 2:*** The IT unit has the technical capabilities and skills to implement the control effectively;
- ***Criterion 3:*** The control aligns with the organisation's IT security strategy;
- ***Criterion 4:*** The control is useful and recognised by relevant third parties, such as partners and customers.

Suitability Levels for a Criterion

- ***Level 0:*** None or very low. Indicates a lack of suitability between a security control in the framework and the criterion;
- ***Level 1:*** Low degree of suitability;
- ***Level 2:*** Moderate or acceptable degree of suitability;
- ***Level 3:*** High or very high degree of suitability.

Suitability of Information Security Frameworks for an IT-Centric ISMS

Example of Control Evaluation: ISO 27001:2022 (hypothetical organisation)

Control ID	***5.18***
Control description	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.
Criterion 1	**(2) Moderate**
Justification for Criterion 1	Most assets are under IT control, but some SaaS and Operational Technology assets aren't.
Criterion 2	**(3) High**
Justification for Criterion 2	All necessary technical tools for implementing the control are within the capabilities of the IT unit. Other units do not have competencies and access to manage their assets.
Criterion 3	**(3) High**
Justification for Criterion 3	The IT Security Strategy establishes a baseline for information security, which explicitly prescribes an equivalent security control.
Criterion 4	**(3) High**
Justification for Criterion 4	Internal and external audits typically look for this type of control. This is a basic expectation from the organisation's customers in their due diligence process.
Control result	**(2) Moderate**