Legal, statutory, regulatory and contractual requirements

ISO 27002 Control 5.31

Control

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security

What could happen if badly implemented ?

- Non-compliance resulting in legal action, fines, or contractual disputes
- Unlawful transfer of information across jurisdictional borders
- Failure to anticipate mandatory access methods by authorities to encrypted information

Which topics should be addressed ?

- List of legal requirements
- Classification of information
- Role and responsibilities
- Supplier Contractual Requirements
- Restriction on the use of cryptography
- Contractual requirement in contracts with suppliers

Examples of applicable legislation

- General Data Protection Regulation (GDPR)
- NIS2 Directive
- Electronic Identification, Authentication and Trust Services (eIDAS) Regulation
- Payment Services Directive 2 (PSD2)
- E-commerce Directive
- Data Governance Act

Link with other frameworks

- NIST 800-53 rev5 : All XX-1 controls, SC-12, SC-13, SC-17
- NIST CSF 2.0 : GV.OC-03

Renaud Dardenne
Asphalia Consulting