Use of cryptography

ISO 27002 Control 8.24

Control

Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography

Why is it important?

- Cryptography is essential for achieving confidentiality (encryption) and integrity/authenticity (digital signatures) of sensitive data
- Key management is critical because weak key handling compromises cryptographic effectiveness
- Ensures compliance with specific legal requirements related to cryptography

What is it about ?

- Data @ rest
- Data in transit
- Data in process
- Symmetric encryption
- Asymmetric/public key cryptography
- Hash functions
- Digital signatures and certificates
- End-to-end encryption
- Key management and HSMs

What process to put in place ?

- Cryptographic keys are generated, stored, and protected via secure processes
- Keys are retired and destroyed securely when no longer needed
- Information transfer and storage utilize approved cryptographic techniques

Link with other frameworks

- NIST 800-53 rev5 : SC-12, SC-13, SC-17
- NIST CSF 2.0 : NA

Renaud Dardenne
Asphalia Consulting