Protection of records

ISO 27002 Control 5.33

Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records

What are the steps ?

- Definition of which documents to protect
- Definition of a document protection procedure
- Set the conservation duration
- Identify applicable legislation

How to implement the control ?

- Issue guidelines on the storage, handling chain of custody, and disposal of records
- Draw up a retention schedule defining records and the period for which they should be retained
- Choose data storage systems that allow retrieval in an acceptable time frame and format
- Establish procedures to safeguard against loss due to future technological change (e.g., format readability)

Which details are important ?

- The system should permit appropriate destruction of records after the retention period
- Records should be categorized into record types with details of retention periods
- Cryptographic keys associated with encrypted archives must also be retained for the length of time the records are kept
- Storage and handling procedures should be implemented in accordance with manufacturer recommendations

Link with other frameworks

- NIST 800-53 rev5 : AC-3*, AC-23, AU-9, CP-9, SC-8, SC-8(1)*, SC-13, SC-28, SC-28(1)*
- NIST CSF 2.0 : GV.OC-03, PR.DS-11

Renaud Dardenne
Asphalia Consulting