Collection of evidence

ISO 27002 Control 5.28

Control

The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events

Purpose

To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions

Who should be involved ?

- Personnel who establish and implement internal procedures
- Legal advice
- Personnel with certification or other relevant means of qualification

What are the main steps ?

- Identification
- Collection
- Acquisition
- Retention
- Protection
- Notification to the authorities

What are the risks if badly implemented ?

- Necessary evidence might be destroyed intentionally or accidentally
- Evidence collected might be inadmissible in national courts of law or disciplinary forums

Link with other frameworks

- NIST 800-53 rev5 : AU-3, AU-4, AU-9, AU-10(3), AU-11*
- NIST CSF 2.0 : RS.AN-03, RS.AN-06

Renaud Dardenne
Asphalia Consulting