Response to information security incidents

ISO 27002 Control 5.26

Control

Information security incidents should be responded to in accordance with the documented procedures

Purpose

To ensure efficient and effective response to information security incidents

Details are important

- Collecting evidence should occur as soon as possible after the incident
- Ensuring that all response activities are properly logged
- Communication must follow the need-to-know principle

Which topics should be addressed ?

- Procedures for containing systems affected by the incident if consequences could spread
- Collection of evidence as soon as possible after the incident occurrence
- Communication of the incident following the need-to-know principle
- Post-incident analysis to identify the root cause
- Identifying and managing vulnerabilities and weaknesses that contributed to the incident

How can it be evidenced ?

- Documented incident response procedures communicated to all relevant parties
- Logs documenting all involved response activities for analysis
- Records showing the formal closure of the incident
- Documentation of the post-incident analysis and identified root cause

Link with other frameworks

- NIST 800-53 rev5 : IR-4
- NIST CSF 2.0 : RS.MA-02

Renaud Dardenne
Asphalia Consulting