Learning from information security incidents

ISO 27002 Control 5.27

Control

Knowledge gained from information security incidents should be used to strengthen and improve the information security controls

Purpose

To reduce the likelihood or consequences of future incidents

Why is it important?

- To reduce the likelihood or the impact
- To identify recurring incidents
- To raising awareness

How ?

- Quantifying and monitoring the types, volumes, and costs of information security incidents
- Identifying recurring or serious incidents and their root causes
- Updating the organization’s information security risk assessment based on lessons learned
- Determining and implementing necessary additional controls to mitigate future incident

What is the added value ?

- Knowledge gained (from incidents)
- Likelihood or consequences (aimed for reduction)
- Information security risk assessment (must be updated)
- Incident types, volumes, and costs (metrics)

Link with other frameworks

- NIST 800-53 rev5 : IR-4
- NIST CSF 2.0 : ID.IM-03, ID.IM-04, RS.MA-02, RS.MA-03

Renaud Dardenne
Asphalia Consulting