Assessment and decision on information security events

ISO 27002 Control 5.25

Control

The organization should assess information security events and decide if they are to be categorized as information security incidents.

Purpose

To ensure effective categorization and prioritization of information security events

Why is it important?

- To ensure effective categorization and prioritization of information security events
- To decide whether an event is severe enough to be categorized as a formal incident requiring defined response procedures

What needs to be defined ?

- Establishing criteria based on organizational impact for identifying an event as an incident.
- Defining escalation paths based on the categorization and prioritization scheme.
- Maintaining a record of the assessment and decision details.

What tasks should be carried out ?

Systematically :

- Evaluating if an event is an incident
- Categorize incidents
- Prioritize incidents

Link with other frameworks

- NIST 800-53 rev5 : AU-6, IR-4
- NIST CSF 2.0 : DE.AE-02, RS.MA-03

Renaud Dardenne
Asphalia Consulting