

Information security incident management planning and preparation

ISO 27002 Control 5.24

Control

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities

Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events



Why is it important?

- To provide the organization with the capability for managing information security incidents effectively
- To ensure compliance with external requirements for timely reporting of incidents to relevant interested parties, such as regulator

Which topics should be addressed ?

- Defining roles and responsibilities to carry out incident management procedures
- Establishing a common method and point of contact for reporting information security events
- Evaluation criteria for determining what constitutes an information security incident
- Procedures for detection, triage, prioritization, analysis, communication, and coordinating interested parties



Small details are important

- The plan should consider different scenarios
- The need to coordinate with internal and external interested parties such as authorities, suppliers, and clients
- Ensuring reporting procedures include immediate actions to be taken, such as noting all pertinent detail

Link with other frameworks

- NIST 800-53 rev5 : IR-8
- NIST CSF 2.0 : ID.IM-04, PR.AT-01, DE.AE-02



Renaud Dardenne
Asphalia Consulting