Management responsibilities

ISO 27002 Control 5.4

Control

Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization

Purpose

To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities

Why is it important ?

- To communicate the information security roles and responsibilities to everyone involved
- To ensure that the mandate for information security is provided
- For compliance with various legislations
- To provide resources for the management system

How can it be achieved ?

- By providing budget
- By promoting the awareness sessions
- By actively participating to the security steerings
- By approving the Information Security Policies
- By allocating and re-allocating resources when needed

How can it be proved ?

- Minutes of steering committee
- Signature of policies
- Disciplinary actions taken for non-compliance
- Training attendance records
- Performance evaluation forms
- Project plans, resource allocation documents, and records of project completion

Link with other frameworks

- NIST 800-53 rev5 : PM-1, PS-1, PS-3, PL-4, PL-1, PM-3, AT-3
- NIST CSF 2.0 : GV.RM-01, GV.RM-03, GV.RR-01, GV.RR-04, GV.RR-03, GV.SC-01, GV.SC-03, GV.SC-09, PR.AT-01, PR.AT-02

Renaud Dardenne
Asphalia Consulting