Information security in project management

ISO 27002 Control 5.8

Control

Information security should be integrated into project management

Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle

Why is it important ?

To ensure that :

- Information security risks and security requirements are assessed and treated at an early stage and periodically
- Progress on information security risk treatment is reviewed and effectiveness of the treatment is evaluated and tested

How can it be organized ?

- By using a standardized project management methodology
- By ensuring that the proper decision body or steering committee has the mandate to include the security aspects at the beginning, during and at the end of the project

What risks or security topics should be addressed ?

- Identity and Access Management
- Suppliers requirements
- Infrastructure aspects
- Secure development
- Business and Data requirements
- Continuity
- Monitoring

Link with other frameworks

- NIST 800-53 rev5 : PL-2, PL-7, PL-8, SA-3, SA-4, SA-9, SA-15
- NIST CSF 2.0 : ID.AM-08, PR.PS-06

Renaud Dardenne
Asphalia Consulting