Information security roles & responsibilities

ISO 27002 Control 5.2

Control

Information security roles and responsibilities should be defined and allocated according to the organization needs

Purpose

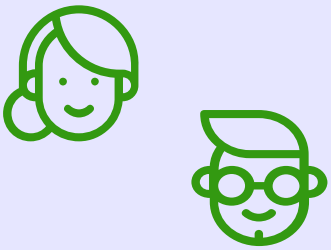
To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization

Why should it be defined ?

- To protect information and assets
- To carrying out information security processes
- To make sure that risk owners are defined
- To define the accountability and responsibility of the various roles

Which roles should be defined ?

- The responsible of the Information Security Management System
- The responsibilities of Top Management
- The CISO
- The Security Committee



Are there other people involved in the SMSI ?

- Legal
- DPO
- Facilities
- Procurement
- Risk Management
- Internal Audit

Link with other frameworks

- NIST 800-53 rev5 : PL-9, PM-2, PM-6, PM-29, PM-13, PS-9, PS-3, SA-9
- NIST CSF 2.0 : GV.OC-02, GV.RM-05, GV.RR-01, GV.RR-02, GV.SC-02, GV.SC-06, GV.SC-06

Renaud Dardenne
Asphalia Consulting