

# Policies for Information Security

ISO 27002 Control 5.1

## Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur

## Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements

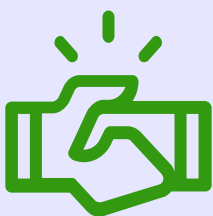
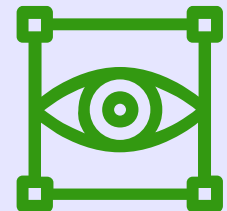


## Who should be involved ?

- Management : They are responsible for defining and approving the policies
- Relevant Personnel : These are the individuals who will be directly affected by the policies and need to acknowledge them
- Interested Parties : These could include external stakeholders who have an interest in the organization's information security

## Which topics should be addressed ?

One word : modularization : start with an overarching Information Security Policy containing general objectives and strategies related to information security and add topic-specific ones related to : Access Management, Suppliers Management, Cloud Services, Compliance Management and Operations Management,...



## What are the good properties of Policies ?

- Existence
- Approval
- Availability
- Communication
- Review Frequency

## Link with other frameworks

- NIST 800-53 rev5 : PM-1
- NIST CSF 2.0 : GV.RM-01, GV.RM-03, GV.RR-01, GV.SC-01, GV.SC-03, GV.SC-09



Renaud Dardenne  
Asphalia Consulting