Management System Standards in Support of Policy
19 September 2017

Ralph ECKMAIER

Information Security Advisor and Auditor
Member of the CEN-CENELEC Focus Group on Cybersecurity

Management Systems

- What is a Management System?
- How many Management Systems are there?
- What is the difference between a Management System (MS) and a Management System Standard (MSS)
- What does it take to have Management System?
- How can a Management System Standard help with the challenges in the Digital Age?

What is a Management System

- A management system is a "set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives".
- The system elements include the organization’s structure, roles and responsibilities, planning, operation, etc.
- A management system can address a single discipline or several disciplines.

ISO/IEC Directives, Part 1 Consolidated ISO Supplement -- Procedures specific to ISO

Surprise

- **You have ALREADY a Management System in place within your Organisation.**

- **There is only ONE Management System in an Organisation.**

- **Achieve conformance with one or several Management System Standards.**

Management System **Standards**

- A set of requirements against which conformance can be audited.
- ISO/IEC standards - Requirements
  - 9001 Quality management system
  - 14001 Environmental management systems
  - **27001 Information security management system**
  - 27552 Enhancement to ISO/IEC 27001 for privacy management
  - 45001 Occupational health and safety

High Level Structure – Identical Text

- Context of the organization
- Leadership
- Planning
- Support
- Operation
- Performance evaluation
- Improvement

Definitions

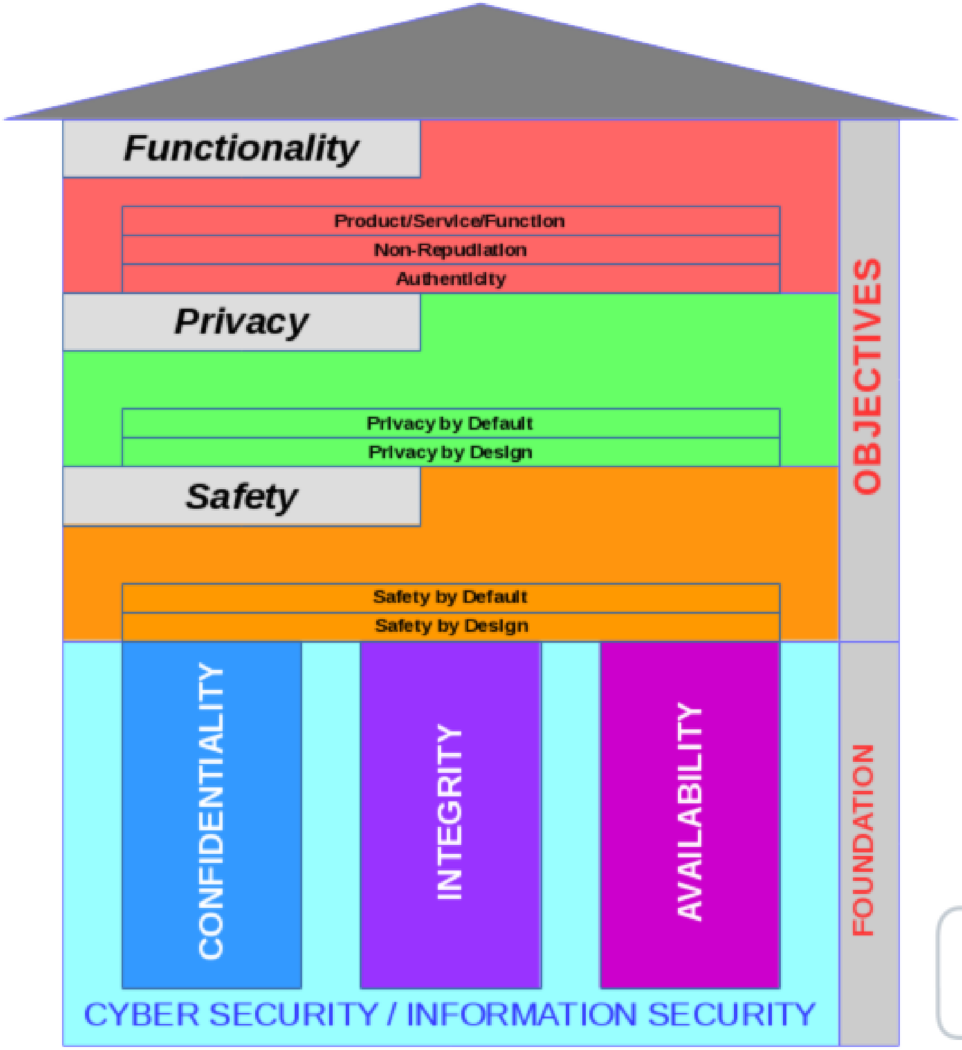
- One globally accepted definition for **Information Security** !
- No such definition for **Cyber Security** (yet) !
- Information Security equals Cyber Security?
- Information security is the preservation of confidentiality, integrity and availablity of information. (ISO/IEC 27000)

Detailed Definition

- Confidentiality
  - **property** that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity
  - **property** of accuracy and completeness
- Availability
  - **property** of being accessible and usable upon demand by an authorized entity

Property, not an objective !

Relationship



Support for Policy

- Seeking compliance with ISO/IEC 27001 provides an organisation with a structured approach
  - To determine external policies or requirements
  - To determine and communicate internal policies
  - To determine and communicate relevant objectives
  - To provide necessary resources
  - To address informations security risks
  - To implement a continous improvement cycle

Summary

- A management system is a "set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives"