SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M1.1 - Basic Concepts

Contents

1. **Cybersecurity fundamentals**
   - Definitions and basics concepts
   - Knowledge areas
   - Why are risk assessment and management important?

2. **Standards overview**
   - Standard of Good Practice
   - ISO/IEC 27000 Suite
   - ISA/IEC 62443

3. **Frameworks overview**
   - NIST Cybersecurity Framework
   - MITRE Att&ck
   - National Framework for Cybersecurity
   - OWASP

4. **Effective Cybersecurity**
   - Management process
   - Cybersecurity information and decision flow

Contents

1. **Cybersecurity fundamentals**
   - Definitions and basics concepts
   - Knowledge areas
   - Why are risk assessment and management important?

CyberSpace

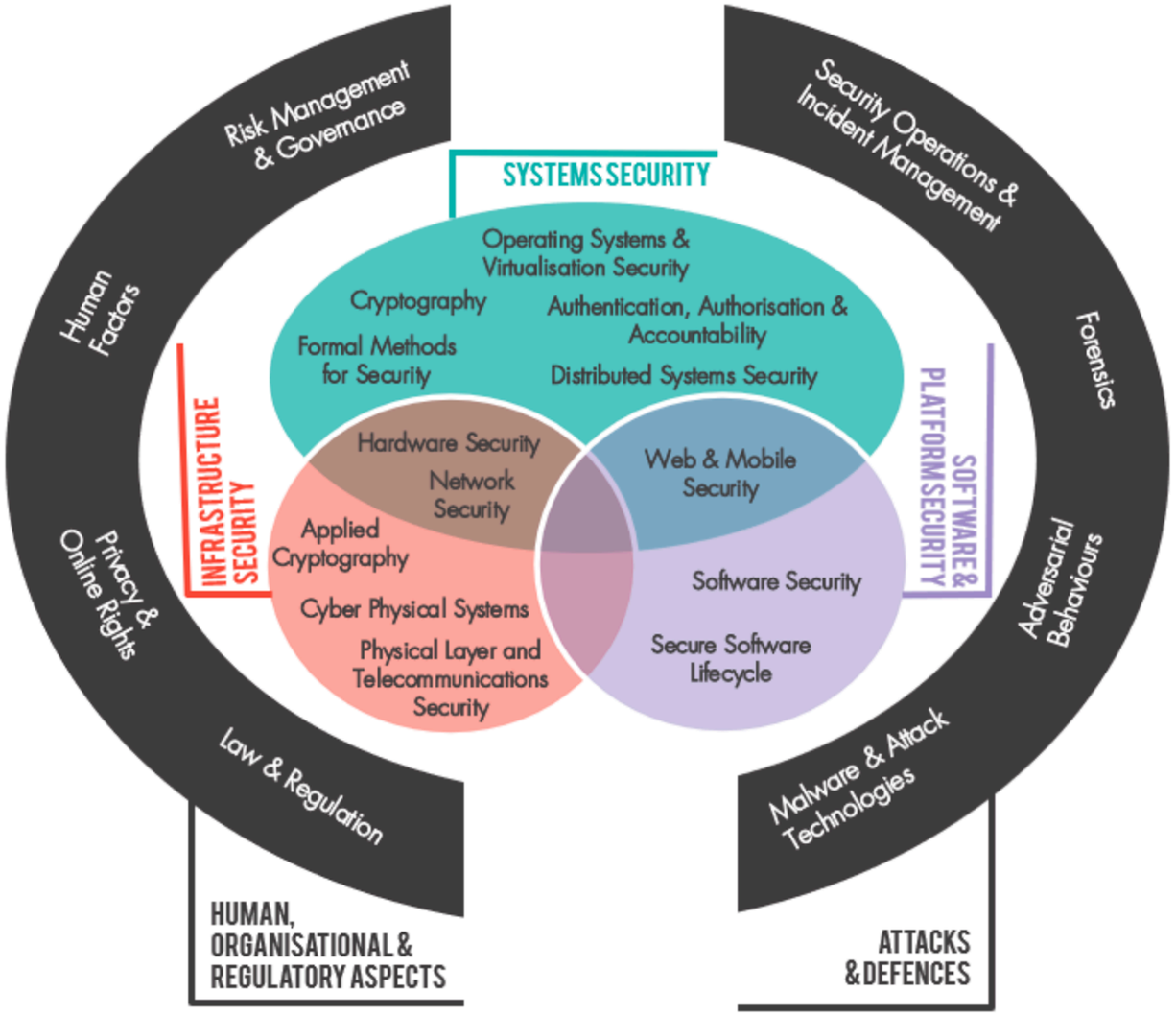
DEFINED BY NATION RESEARCH COUNCIL IN USA

Cyberspace consists of

- **artifacts** based on or dependent on computer and communications technology;
- the **information** that these artefacts use, store, handle, or process;
- the **interconnections** among these various elements.

Cybersecurity Knowledge Areas

KEY TOPIC AREAS



CyBOK

Cyber Security Body of Knowledge

It aims to **codify** the foundational and generally recognised knowledge on cyber security.

CyBOK grouped into **five (not orthogonal) broad categories**. Clearly, other possible categorisations of these Knowledge Areas (KAs) may be equally valid, and ultimately some of the structure is relatively arbitrary.

https://www.cybok.org

CyberSecurity

DEFINED BY ITU-T

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices and technologies that are used to protect the cyberspace environment and organizations and user's assets.

ORGANIZATION AND USER'S ASSETS INCLUDE

connected computing devices, infrastructure, applications, services, telecommunications systems, and the totality of **transmitted** and/or **stored** information in the cyberspace .

CYBERSECURITY IS COMMITTED TO ENSURE

the **achievement** and **maintenance** of the security properties of the organization and user's assets against relevant **security risks in the cyberspace** environment.

Useful Definitions

IMPORTANT TO ALL SPEAK THE SAME LANGUAGE

Asset

Software - Hardware

Data contained in an information system; or a service provided by a system; or a **system capability**, such as **processing power** or communication bandwidth; or an item of system equipment (such as **hardware**, firmware, **software**, or documentation).

Risk

Measure - Impact

The risk is the **possibility that human actions or events lead to consequences** that have an **impact** on what humans value. It is important to estimate the **likelihood** of events that may lead to an impact.

Threat

Capability - Danger

A **potential for violation of security** that exists when there is a circumstance, a capability, an action, or an event that could breach security and cause harm. Basically, a threat is a possible danger that might **exploit a vulnerability**.

Vulnerability

Flaw - Design

A **flaw or weakness in a system's design**, implementation, or operation and management that could be exploited to violate the system's security policy.

Information Security

DEFINED ISO 27000

Information security:
Preservation of **confidentiality**, **integrity** and **availability** of information

In addition, other properties, such as **authenticity**, **accountability**, **non-repudiation**, and **reliability** can also be involved.

Cybersecurity Objectives

THE MOST FAMOUS THREE

CONFIDENTIALITY

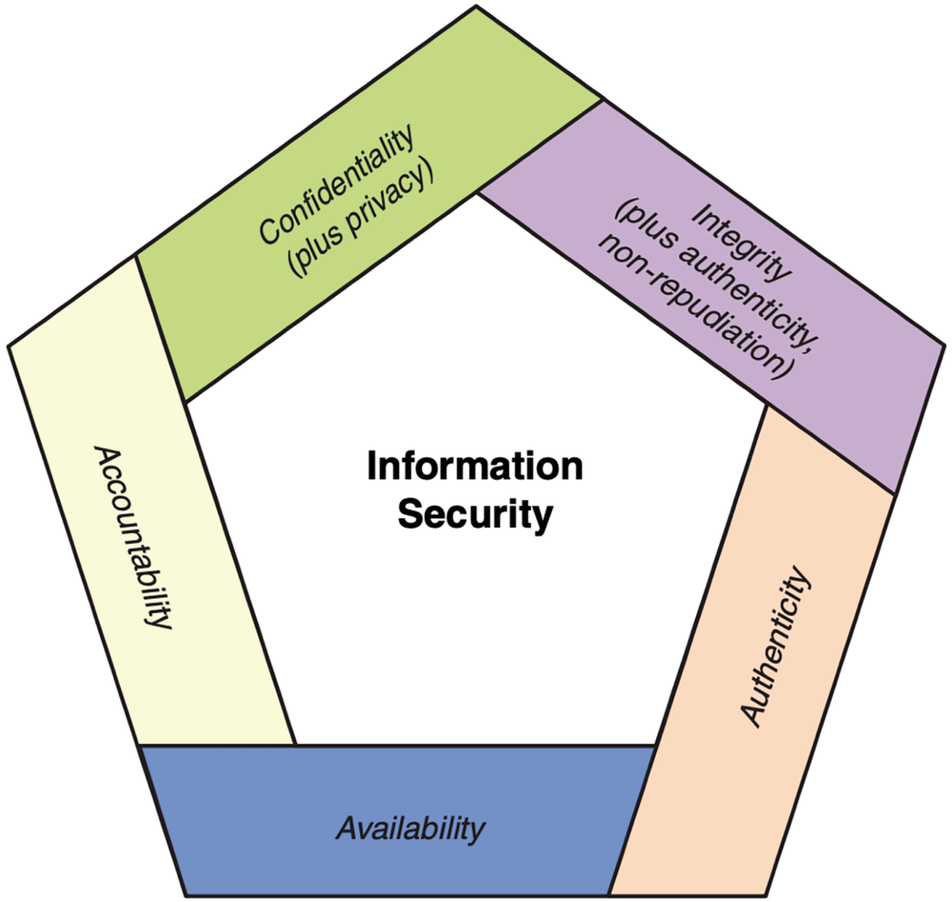
The property that data is not **disclosed** to system entities unless they have been authorized to know the data

INTEGRITY

The property that data has **not been changed**, destroyed, or lost in an unauthorized or accidental manner

AVAILABILITY

The property of a system or a system **resource being accessible or usable or operational upon demand**, by an authorized system entity, according to performance specifications for the system



Cybersecurity Objectives

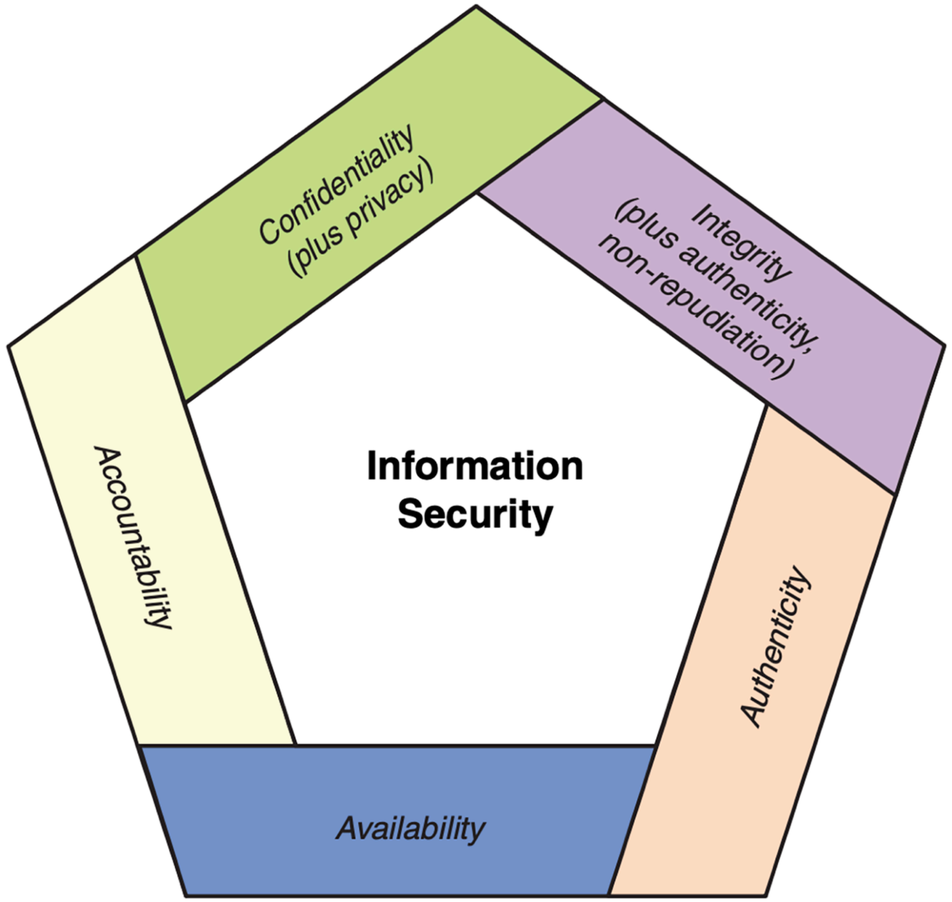
TWO MORE IN ADDITION

AUTHENTICITY

The property of being genuine and **being able to verify that users are who they say they are** and that each input arriving at the system came from a trusted source

ACCOUNTABILITY

The property of a system or system resource **ensuring that the actions of a system entity may be traced uniquely to that entity**, which can then be held **responsible** for its actions



Cybersecurity Dilemmas

IMPORTANT TO ALL SPEAK THE SAME LANGUAGE

Scale and Complexity of Cyberspace

Massive - Constantly changes

The scale and complexity of cyberspace are massive. Cyberspace involves **many devices and individuals** that require some level of access to resources. In addition cybersecurity constantly change as **technologies advance**.

Nature of Threat

Assets evolve - Legitimate actors

Organizational assets in cyberspace are under constant and **evolving threat** from criminals to hostile states. In addition legitimate actors (businesses and governments) collect, store and, analyze information from and about individuals for **evaluating** security risks.

User needs vs Security implementation

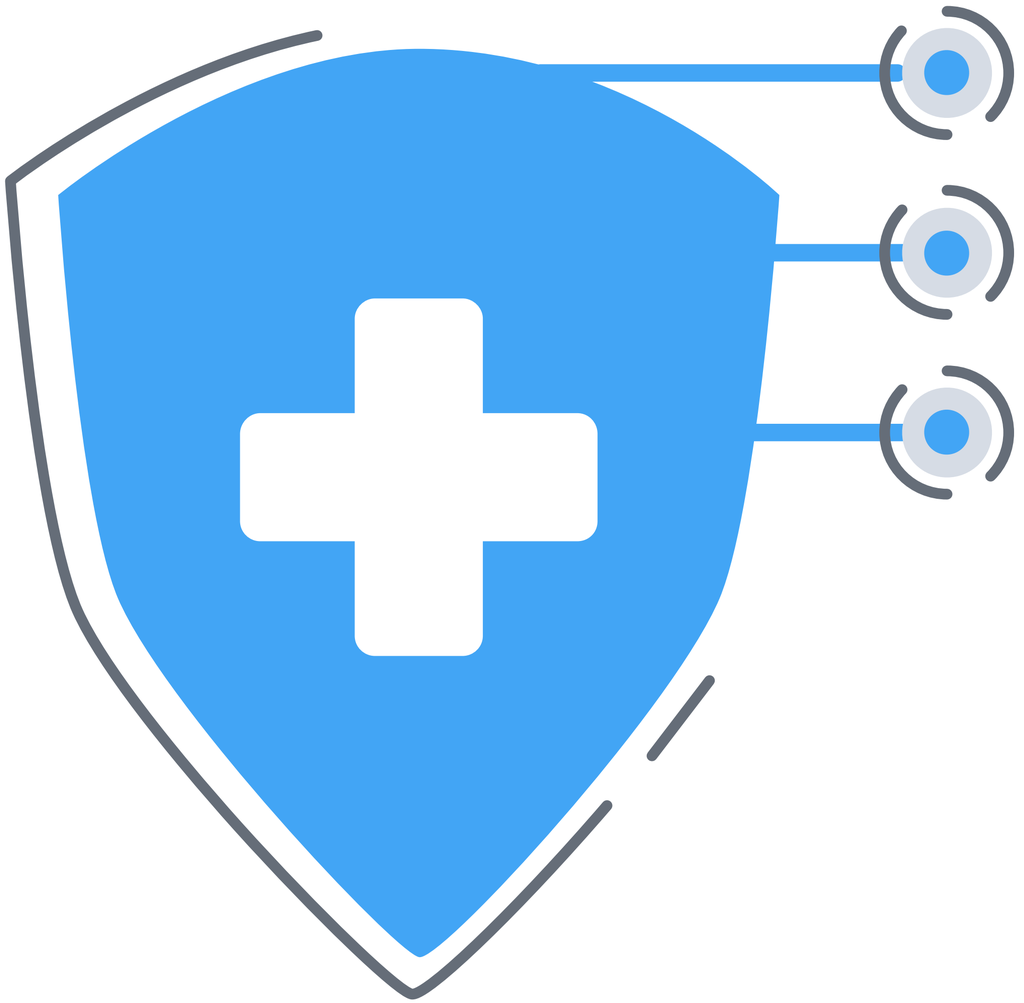
More features - Manage security

Users want technology with the most modern and **powerful features**. But there is an inherent conflict between greater ease of use and greater range of options. The simpler the system, and the more its individual elements are isolated from one another, the easier it is to implement **effective security**.

Difficulty estimating costs and benefits

Cost - Difficult getting consensus

It is difficult to estimate the **total cost of cybersecurity** breaches and, therefore, the benefits of security policies and mechanisms. This complicates the need to achieve **consensus** on the allocation of resources to security.



Which process for the Risk?

RISK IS AT THE HEART OF EVERYDAY LIFE

Risk

is the possibility that human **actions** or events **lead to consequences that have an impact** on what humans value

- **Risk Assessment** is a process of **collating observations and perceptions** of the world that can be **justified by logical reasoning** or comparisons with actual outcomes .
- **Risk Management** is the process of **developing and evaluating options** to **address the risks** in a manner that is agreeable to people whose values may be impacted.
- **Risk Governance** set of ongoing processes and principles that aims to **ensure an awareness and education of the risks** faced when certain actions occur, and to **inspire a sense of responsibility** and accountability to all involved in managing it.

Why Risk Assessment is important?

Identification and, if possible, estimation of hazard

Identification of events and estimation of the strength of the outcome

Assessment of exposure and/or vulnerability

Exposure aspects of a system or Vulnerability to attributes such as hardware, software, etc.

Estimation of risk combining the likelihood and severity (impact)

Quantitative or Qualitative and captures the expected impact.

Risk Assessment

Key point

The fundamental concept of risk assessment is **to use analytic and structured processes to capture** information, perceptions and evidence relating what is at stake, **the potential for desirable and undesirable events**, and a measure of the **likely outcomes** and **impact**.

Why Risk Management is important?

Intolerable

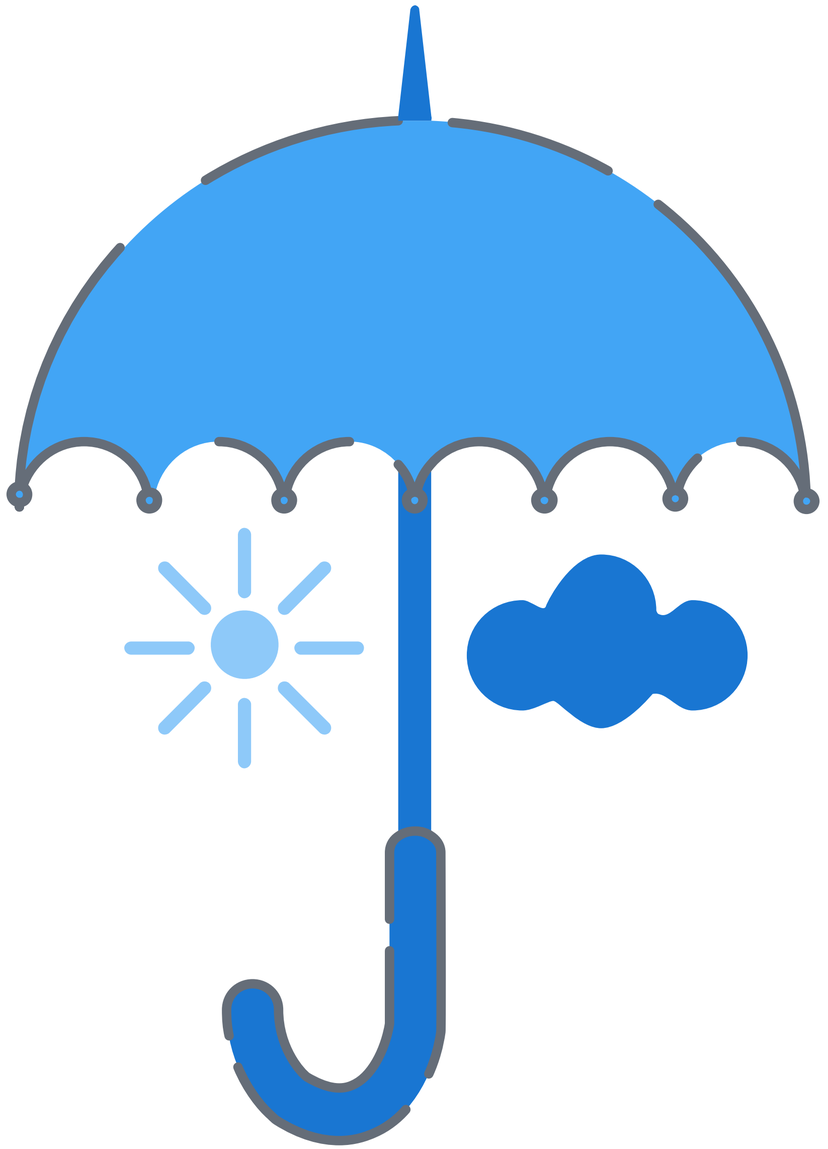
the aspect of the system at **risk needs to be abandoned or replaced**, or if not possible, vulnerabilities need to be reduced and exposure limited.

Tolerable

risks have been reduced with reasonable and appropriate methods to a level as low as reasonably possible (ALARP) or as low as reasonably allowable (ALARA)

Acceptable

risk reduction is not necessary and can proceed without intervention.



Risk Management Process

The risk management process involves **reviewing the information collected** as part of the **risk (and concern) assessments.** This information forms **the basis of decisions leading** to three outcomes for each perceived risk .

Cyber Risk

"CYBER" AS A SPECIAL CASE

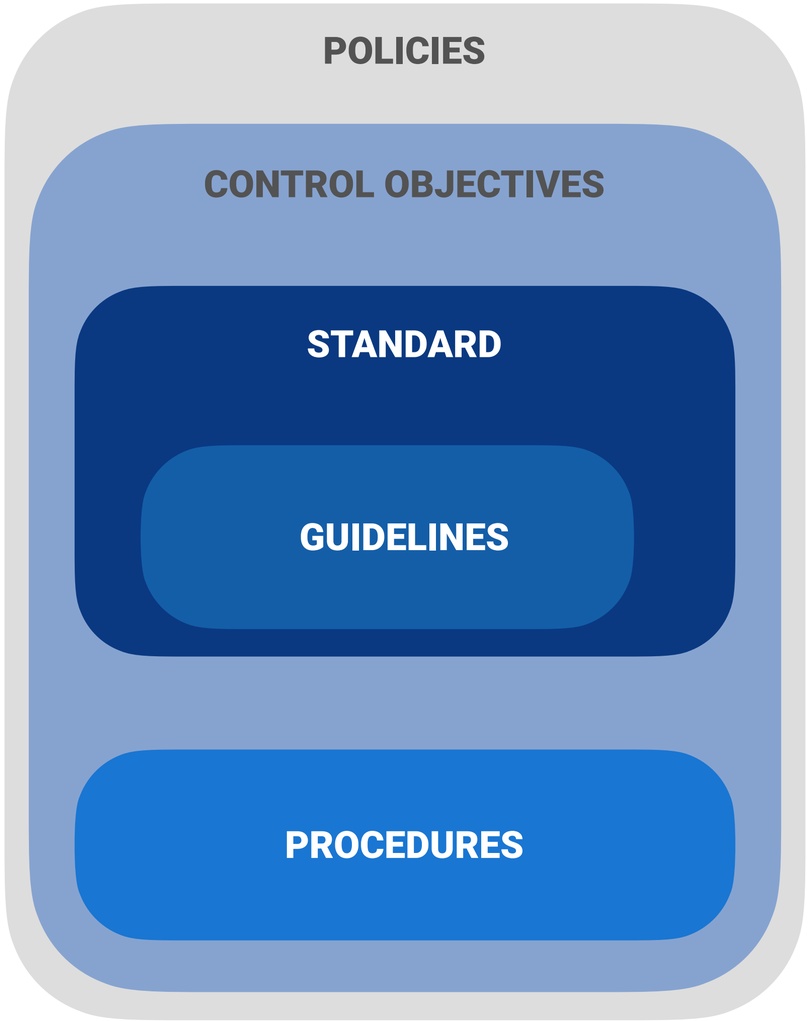
Cyber security risk assessment and **management** are a fundamental special cases that everyone living and working within the digital domain or **cyberspace** should understand and be a participant in it.

There are a number of **global standards** that aim to formalise and provide a common framework for cyber risk assessment and management.

Contents

What is the difference between…

FUNDAMENTAL TO BUILDING A SOLID GOVERNANCE STRUCTURE



POLICIES

Policies are **high-level statements of management** intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes. Policies are **enforced by standards** and **further implemented by procedures** to establish actionable and accountable requirements.

CONTROL OBJECTIVES

Control Objectives are targets or **desired conditions to be met.**

STANDARDS

Standards are **mandatory requirements** regarding processes, actions and configurations that are designed to satisfy Control Objectives.

PROCEDURES

Procedures are a **documented set of steps necessary to perform a specific task** or process in conformance with an applicable standard. Procedures help address the question of how the organization actually operationalizes a policy, standard or control.

GUIDELINES

Guidelines are **recommended practices that are based on industry-recognized** secure practices. We apply the guidelines **where we cannot apply the standard** or where we want to improve it according to our needs.

https://www.complianceforge.com/faq/word-crimes/policy-vs-standard-vs-control-vs-procedure

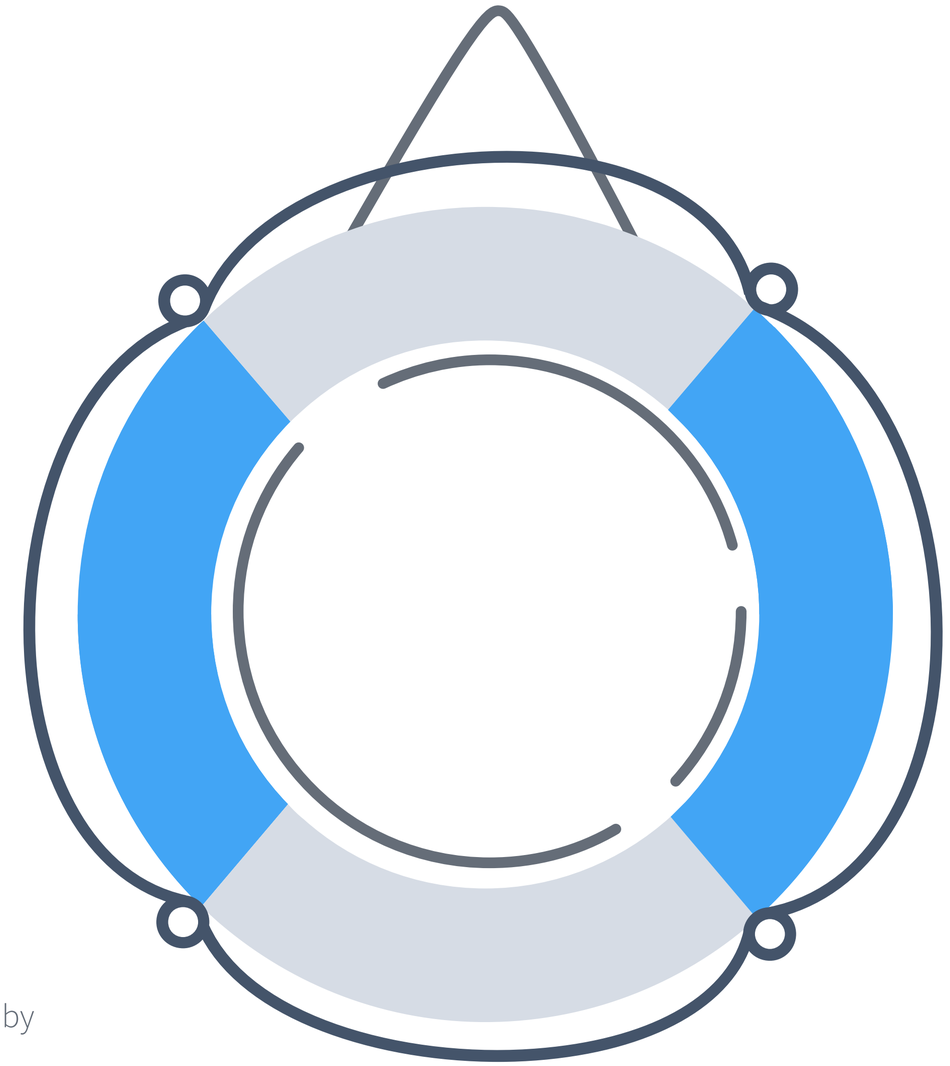
The value of Standards and Best Practices documents

A number of organizations, based on wide professional input, have developed best practices types of documents as well as standards for implementing and evaluating cybersecurity

- National Institute of Standards and Technology **(NIST)**
- International Organization for Standardization **(ISO)**
- International Electrotechnical Commission **(IEC)**
- International Telecommunication Union Telecommunication Standardization Sector **(ITU-T)**
- Internet Society **(ISOC)**
- Internet Engineering Task Force **(IETF)**

A number of professional and industry groups have produced best practices documents and guidelines

- International Society of Automation **(ISA)**
- Information Security Forum **(ISF)**
- Control Objectives for Information and Related Technology **(COBIT)** for information security issued by Information Systems Audit and Control Association **(ISACA)**
- Center for Internet Security **(CIS)**



Important Standards and Best Practices documents

A NON-EXHAUSTIVE LIST

Source	Title
NIST	Cybersecurity Framework **(CSF)**
ISO/IEC	**ISO/IEC 27001** - Information security management
ISA/IEC	**ISA/IEC 62443** international standard for the security of industrial automation control systems
ISF	Standard of Good Practice for Information Security **(SOGP)**
NIST	NIST Special Publication **(SP)** 800 seires
ISACA	Control Objectives for Information and Related Technology **(COBIT)**

Security Policy (1/2)

EFFECTIVE CYBERSECURITY GOVERNANCE

Security Policy

CISO and Security Manager

A **set of rules and practices** that specify or regulate h**ow a system or organization provides security services to protect sensitive and critical system resources.** It includes associated responsibilities and the information security principles to be followed by all relevant individuals. It applies to **all employees**, especially those with some responsibility for an asset or assets.

Security Policy (2/2)

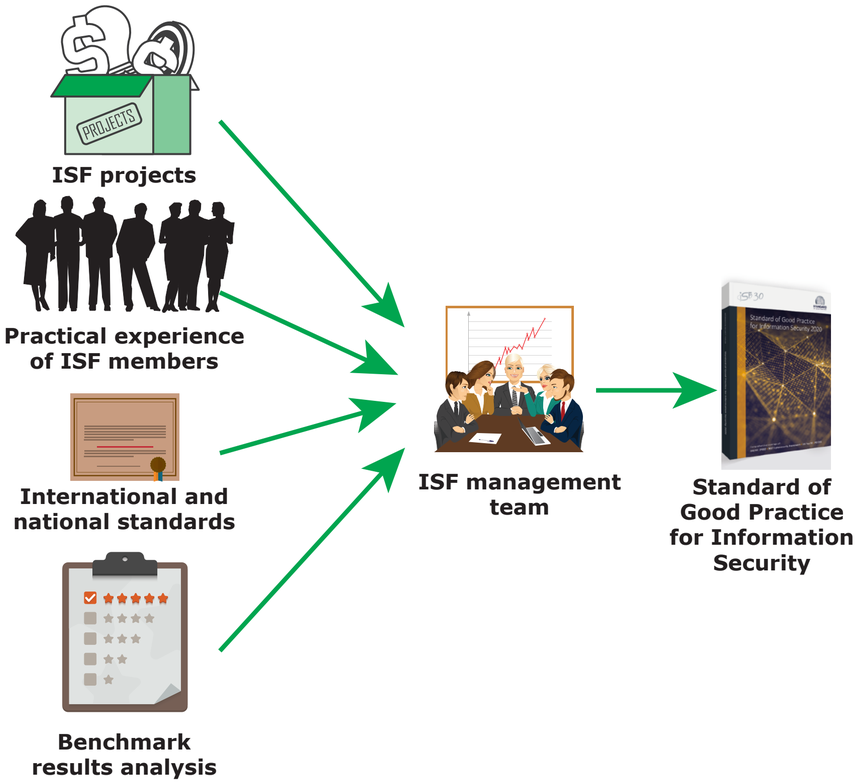
EFFECTIVE CYBERSECURITY GOVERNANCE

Security Policy Types

CISO and Security Manager

- **Access control policy:** How information is accessed
- **Contingency planning policy:** How availability of data is provided 24/7
- **Data classification policy:** How data are classified
- **Network security policy:** How network systems are secured
- **Incident response policy:** How incidents are reported and investigated
- **Encryption policy:** How data are encrypted, the encryption method used
- **Physical access policy:** How access to the physical area is obtained
- **Cloud computing policy:** Security aspects of using cloud computing resources
- **Security awareness policy:** How security awareness is carried out

The Standard Of Good Practice (SOGP) for Information Security



SOGP

is issued by the Information Security Forum (ISF). The **goal of the ISF** is the development of **best practice methodologies, processes, and solutions** that meet the needs of its members, including large and small business organizations, government agencies, and nonprofit organizations.

- This document is a business-focused **comprehensive guide to identifying and managing information security risks** in organizations and their supply chains
- The SOGP is **based on** research **projects** and input from ISF members as well as analysis of the leading **standards** on cybersecurity, information security, and risk management

Who needs the security policy?

SOGP EXAMPLE

The SOGP is of particular **interest** to the following **individuals**:

Who	Role
Chief information security officers (or equivalent)	Responsible for **developing** policy and implementing sound information security governance and information security assurance.
Information security managers (as well as security architects, local security coordinators, and information protection champions)	Responsible for **promoting** or **implementing** an information security assurance program
Business managers	Responsible for **ensuring** that critical business applications, processes, and local environments on which an organization's success depends are effectively managed and controlled
IT managers and technical staff	Responsible for **designing**, **planning**, developing, deploying, and maintaining key business applications, information systems, or facilities
Internal and external auditors	Responsible for **conducting** security audits
Procurement and vendor management teams	Responsible for defining appropriate information security **requirements in contract**

SOGP organization

GOOD PRACTICE CONTROLS FOR 132 SECURITY TOPICS

17 categories each of which is broken down into **2 areas**. Each area is further broken down into a number of topics, or business activities, for a total of **132 topics**.

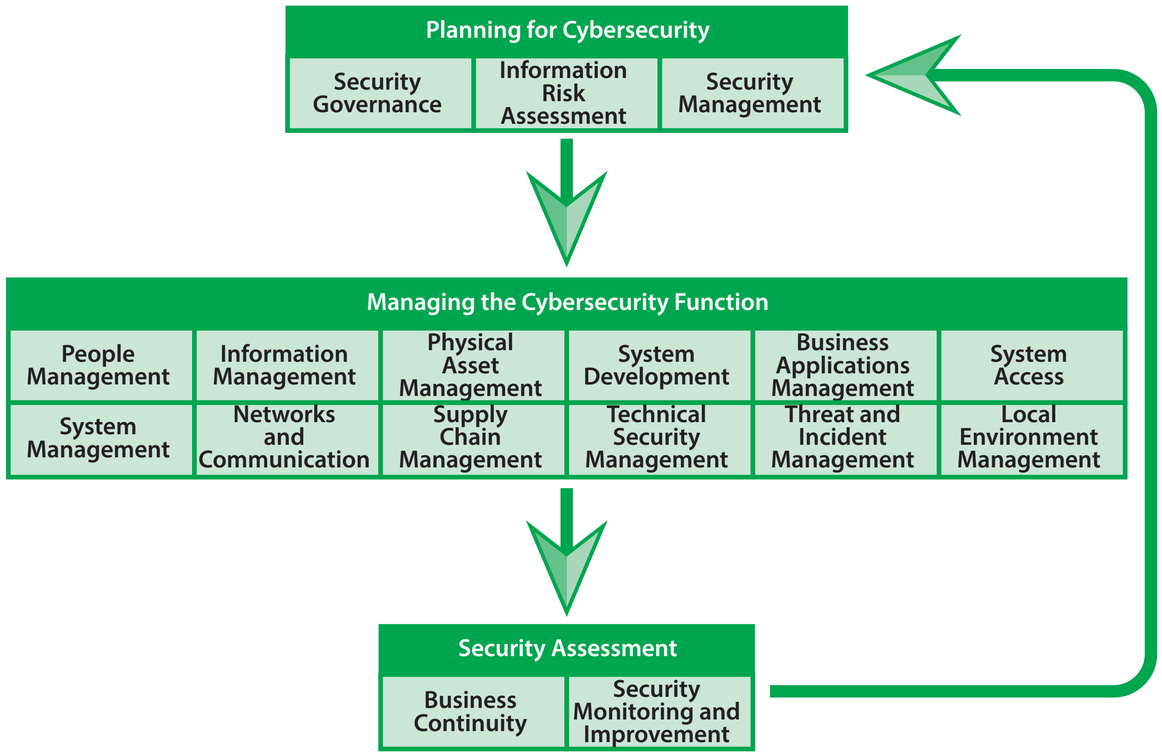
Each of the 132 topics **addresses good practice controls** relevant to a particular activity from an information security perspective.

The SOGP is **consistent** with the structure and flow of the **ISO/IEC 27000** suite of standards

SECURITY GOVERNANCE (SG) Security Governance Approach Security Governance Components INFORMATION RISK ASSESSMENT (IR) Information Risk Assessment Framework Information Risk Assessment Process SECURITY MANAGEMENT (SM) Security Policy Management Information Security Management PEOPLE MANAGEMENT (PM) Human Resource Security Security Awareness/Education INFORMATION MANAGEMENT (IM) Information Classification and Privacy Information Protection PHYSICAL ASSET MANAGEMENT (PA) Equipment Management Mobile Computing SYSTEM DEVELOPMENT (SD) System Development Management System Development Life Cycle BUSINESS APPLICATION MANAGEMENT (BA) Corporate Business Applications End User Developed Applications	SYSTEM ACCESS (SA) Access Management Customer Access SYSTEM MANAGEMENT (SY) System Configuration System Maintenance NETWORKS AND COMMUNICATIONS (NC) Network Management Electronic Communication SUPPLY CHAIN MANAGEMENT (SC) External Supplier Management Cloud Computing TECHNICAL SECURITY MANAGEMENT (TS) Security Solutions Cryptography THREAT AND INCIDENT MANAGEMENT (TM) Cybersecurity Resilience Security Incident Management LOCAL ENVIRONMENT MANAGEMENT (LE) Local Environments Physical and Environmental Security BUSINESS CONTINUITY (BC) Business Continuity Framework Business Continuity Process SECURITY MONITORING AND IMPROVEMENT (SI) Security Audit Security Performance

SOGP Activities

PROCESS



3 principal activities

The arrows suggest the process flow for the 17 SOGP categories

Planning for cybersecurity:

- developing **approaches** for managing and controlling the cybersecurity function(s);
- defining the **requirements** specific to a given IT environment;
- developing **policies** and procedures for managing the security function

Managing the cybersecurity function:

- managing the security controls to satisfy the defined security requirements.

Security assessment:

- **assuring** that the security management function enables business continuity;
- monitoring, **assessing, and improving the suite of cybersecurity controls**

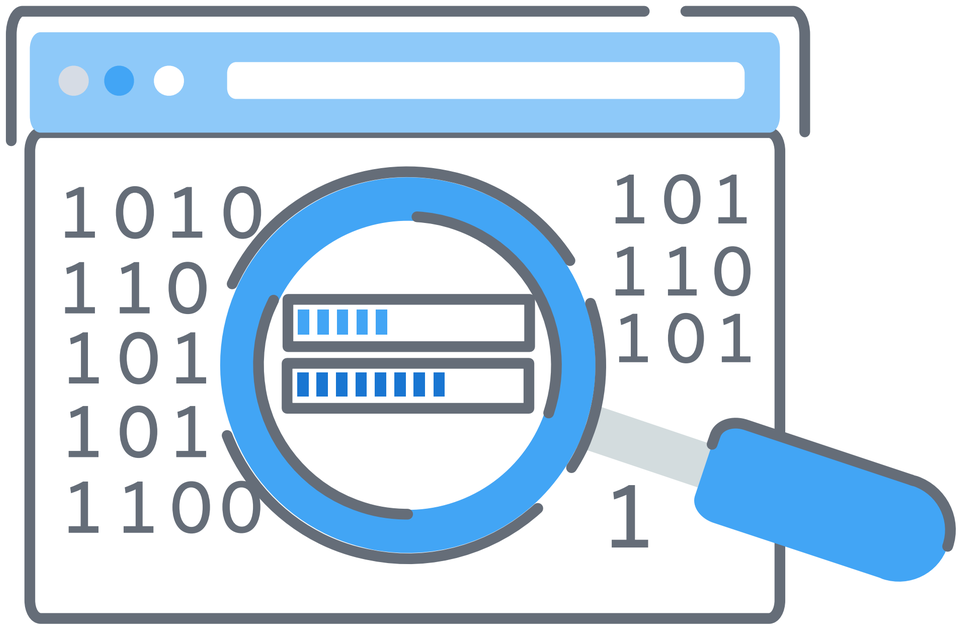
The ISO/IEC 27000 Suite of Information Security Standards

The ISO and IEC have developed a growing family of standards in the ISO/IEC 27000 series that deal with ISMSs

Information security management system (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, **with the scope** of protecting its information assets.

An ISMS is a **systematic approach** for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an **organization's information security to achieve business objectives.**

It is based upon a **risk assessment** and the organization's **risk acceptance levels** designed to effectively treat and manage risks. Analyzing requirements for the protection of assets, as required, contributes to the successful implementation of an ISMS



Standardization Bodies

- **ISO:** Founded in 1946, it is an **international agency for the development of standards** on a wide range of subjects to facilitate international exchange of goods and services and to develop cooperation
- **IEC:** Develops standards in a joint effort with ISO in the areas of data communications, networking, and security

ISO 27000 Principles

TO SUPPORT ISMS

Fundamental Principles

ISO 27000 suite

The following fundamental **principles also contribute to the successful implementation** of an **ISMS**:

- **awareness** of the need for information security
- **assignment** of responsibility for information security
- **incorporating** management commitment and the interests of stakeholders
- **enhancing** societal values
- **risk assessments** determining appropriate controls to reach acceptable levels of risk
- **security incorporated** as an essential element of information networks and systems
- **active prevention and detection** of information security incidents
- **ensuring a comprehensive approach** to information security management
- **continual reassessment of information security** and making of modifications as appropriate

ISO 27000 Family of Standards

ISMS overview and vocabulary	ISMS requirements		ISMS guidelines		ISMS sector-specific guidelines	
27000 ISMS overview	27001 ISMS requirements	27006 Audit and certification of ISMS	27002 Code of practice for IS controls	27003 ISMS implementation	27010 Intersector/ interorganizational comms	27011 Telecomms organizations
	27009 Sector-specific application		27004 ISM measurement	27005 IS risk management	27015 Financial services	27017 IS controls for cloud services
			27007 ISMS auditing	TR 27008 Auditors on IS control	27018 Protection of PII in public clouds	27019 Energy utility industry PCS
			27013 Integrated implementation of 27001/20000	27014 Governance of IS		
			TR 27016 Organizational economics	27036 IS for supplier relationships		

ISMS = Information Security Management System
PII = personally identifiable information
PCS = process control systems

4 categories

The ISO 27000 series deals with all aspects of an **ISMS**. It helps small, medium, and large businesses in any sector keep information assets secure.

This growing collection of standards falls into **four categories**

- **Overview and vocabulary:** Provide an overview and relevant vocabulary for **ISMS**
- **Requirements:** Discuss normative standards that define requirements for an **ISMS** and for those certifying such systems
- **Guidelines:** Provide direct support and detailed guidance and/or interpretation for the overall process of establishing, implementing, maintaining, and improving an **ISMS**
- **Sector-specific guidelines:** Address sector-specific guidelines for an **ISMS**

ISO 27001 ISMS Requirements

MAINLY FOR ISMS CERTIFICATION

ISO 27001 is a management standard initially designed for the certification of organizations.
The system works like this:

- **Certification Audit:** An organization develops an ISMS and then invites a certification body to determine that the ISMS is compliant with the standards.
- **Qualified individuals to develop and maintain the ISMS:** various certification programs have been developed for individuals (ISO 27001 Lead Implementer and ISO 27001 Lead Auditor programs).
- Obtaining such a certification **enhances the value** of an employee to an organization.

Certification: The provision by an **independent body** of written assurance (a certificate) that the product, service, or system in question meets specific requirements.
Also known as **third-party conformity assessment**.

4 Context of the organization 4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the information security management system 4.4 Information security management system **5 Leadership** 5.1 Leadership and commitment 5.2 Policy 5.3 Organizational roles, responsibilities and authorities **6 Planning** 6.1 Actions to address risks and opportunities 6.2 Information security objectives and planning to achieve them	**7 Support** 7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication 7.5 Documented information **8 Operation** 8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment **9 Perform ance evaluation** 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review **10 Im provem ent** 10.1 Nonconformity and corrective action 10.2 Continual improvement

ISO 27002 Code of Practice for Information Security Controls

DEFINE REQUIREMENTS

ISO 27002 provides the broadest treatment of ISMS topics in the ISO 27000 series.

- Controls in ISO 27002 and indicates that the organization can pick and **choose the controls that are needed to satisfy the ISMS requirements**.
- The **linkage** between the ISMS requirements defined in ISO 27001 and the information security controls defined in ISO 27002 is provided by Section 6.1.3 of ISO 27001.
- ISO 27001 also states that the organization **can select controls from any source**, not solely or necessarily ISO 27002

Security Controls: The management, operational, and technical controls (that is, countermeasures) prescribed for an information system **to protect the confidentiality, integrity, and availability of the system and its information.**

5 Information security policies 5.1 Management direction for information security **6 Organization of information security** 6.1 Internal organization 6.2 Mobile devices and teleworking **7 Human resource security** 7.1 Prior to employment 7.2 During employment 7.3 Termination and change of employment **8 Asset management** 8.1 Responsibility for assets 8.2 Information classification 8.3 Media handling **9 Access control** 9.1 Business requirements of access control 9.2 User access management 9.3 User responsibilities 9.4 System and application access control **10 Cryptography** 10.1 Cryptographic controls **11 Physical and environmental security** 11.1 Secure areas 11.2 Equipment **12 Operations security** 12.1 Operational procedures and responsibilities 12.2 Protection from malware 12.3 Backup 12.4 Logging and monitoring	**12 Operations security** 12.5 Control of operational software 12.6 Technical vulnerability management 12.7 Information systems audit considerations **13 Communications security** 13.1 Network security management 13.2 Information transfer **14 System acquisition, development and maintenance** 14.1 Security requirements of information systems 14.2 Security in development and support processes 14.3 Test data **15 Supplier relationships** 15.1 Information security in supplier relationships **16 Information security incident management** 16.1 Management of information security incidents and improvements **17 Information security aspects of business continuity management** 17.1 Information security continuity 17.2 Redundancies **18 Compliance** 18.1 Compliance with legal and contractual requirements 18.2 Information security reviews

Mapping ISO 27001 to ISF SOGP

USEFUL TOOL

For an organization that relies on ISO 27001 for certification and ISO 27002 for a selection of controls to meet ISO 27001 requirements, **the ISF SOGP is an invaluable and perhaps essential tool.**

It provides a far **more detailed description of the controls and represents the widest possible consensus among industry**, government, and academic security experts and practitioners.

The table **maps** the ISO 27001 requirements to the ISF SOGP security controls. For each of the detailed requirements, this table indicates the **controls that can be used to satisfy those requirements**, as documented in the ISF SOGP.

ISO 27001 Topic	ISG SGP Category
4.1 Understanding the Organization and Its Context	Security Governance
4.2 Understanding the Needs and Expectations of Interested Parties	Security Governance
4.3 Determining the Scope of the Information Security Management System	Security Management
4.4 Information Security Management System	Security Management
5.1 Leadership and Commitment	Security Governance
5.2 Policy Security Management	Security Management
5.3 Organizational Roles, Responsibilities and Authorities	Security Governance
6.1 Actions to Address Risks and Opportunities	Information Risk Assessment
6.2 Information Security Objectives and Planning to Achieve Them	Security Management
7.1 Resources	Security Management
7.2 Competence	People Management
7.3 Awareness	People Management
7.4 Communication	People Management
7.5 Documented Information	Security Management
8.1 Operational Planning and Control	Security Management
8.2 Information Security Risk Assessment	Information Risk Assessment
8.3 Information Security Risk Treatment	Information Risk Assessment
9.1 Monitoring, Measurement, Analysis and Evaluation	Security Monitoring and Improvement
9.2 Internal Audit	Security Monitoring and Improvement
9.3 Management Review	Security Monitoring and Improvement
10.1 Non-conformity and Corrective Action	Security Monitoring and Improvement
10.2 Continual Improvement	Security Monitoring and Improvement

Mapping ISO 27002 to ISF SOGP

USEFUL TOOL

It should be mentioned that ISO 27001 and 27002 **do not cover a number of important topics discussed in the ISF SOGP**, including threat intelligence and system decommissioning, and the **ISF SOGP is far more detailed.**

Similarly, this table shows the mapping between the ISO 27002 security controls and the corresponding controls in ISF SOGP.

Even if an organization is using **ISO 27002 as a checklist** of controls to be chosen to meet security requirements, **these selections should be augmented by the more detailed information available in the ISF SOGP**.

ISO 27002 Topic	ISG SGP Category
5.1 Management Direction for Information Security	Security Monitoring and Improvement
6.1 Internal Organization	Security Governance
6.2 Mobile Devices and Teleworking	People Management
7.1 Prior to Employment	People Management
7.2 During Employment	People Management
7.3 Termination and Change of Employment	People Management
8.1 Responsibility for Assets	Physical Asset Management
8.2 Information Classification	Physical Asset Management
8.3 Media Handling	Physical Asset Management
9.1 Business Requirements of Access Control	System Access
9.2 User Access Management	System Access
9.3 User Responsibilities	System Access
9.4 System and Application Access Control	System Access
10.1 Cryptographic Controls	Technical Security Management
11.1 Secure Areas	Local Environment Management
11.2 Equipment	Local Environment Management
12.1 Operational Procedures and Responsibilities	System Development
12.2 Protection from Malware	Technical Security Management
12.3 Backup	System Management
12.4 Logging and Monitoring	Threat and Incident Management
12.5 Control of Operational Software	System Development
12.6 Technical Vulnerability Management	System Development
12.7 Information Systems Audit Considerations	Security Monitoring and Improvement
13.1 Network Security Management	Networks and Communications
13.2 Information Transfer	Networks and Communications
14.1 Security Requirements of Information Systems	Security Management
14.2 Security in Development and Support Processes	System Development
14.3 Test Data	System Development
15.1 Information Security in Supplier Relationships	Supply Chain Management
16.1 Management of Information Security Incidents and Improvements	Threat and Incident Management
17.1 Information Security Continuity	Business Continuity
17.2 Redundancies	Business Continuity
18.1 Compliance with Legal and Contractual Requirements	Security Management
18.2 Information Security Reviews	Security Monitoring and Improvement

IEC 62443 organization

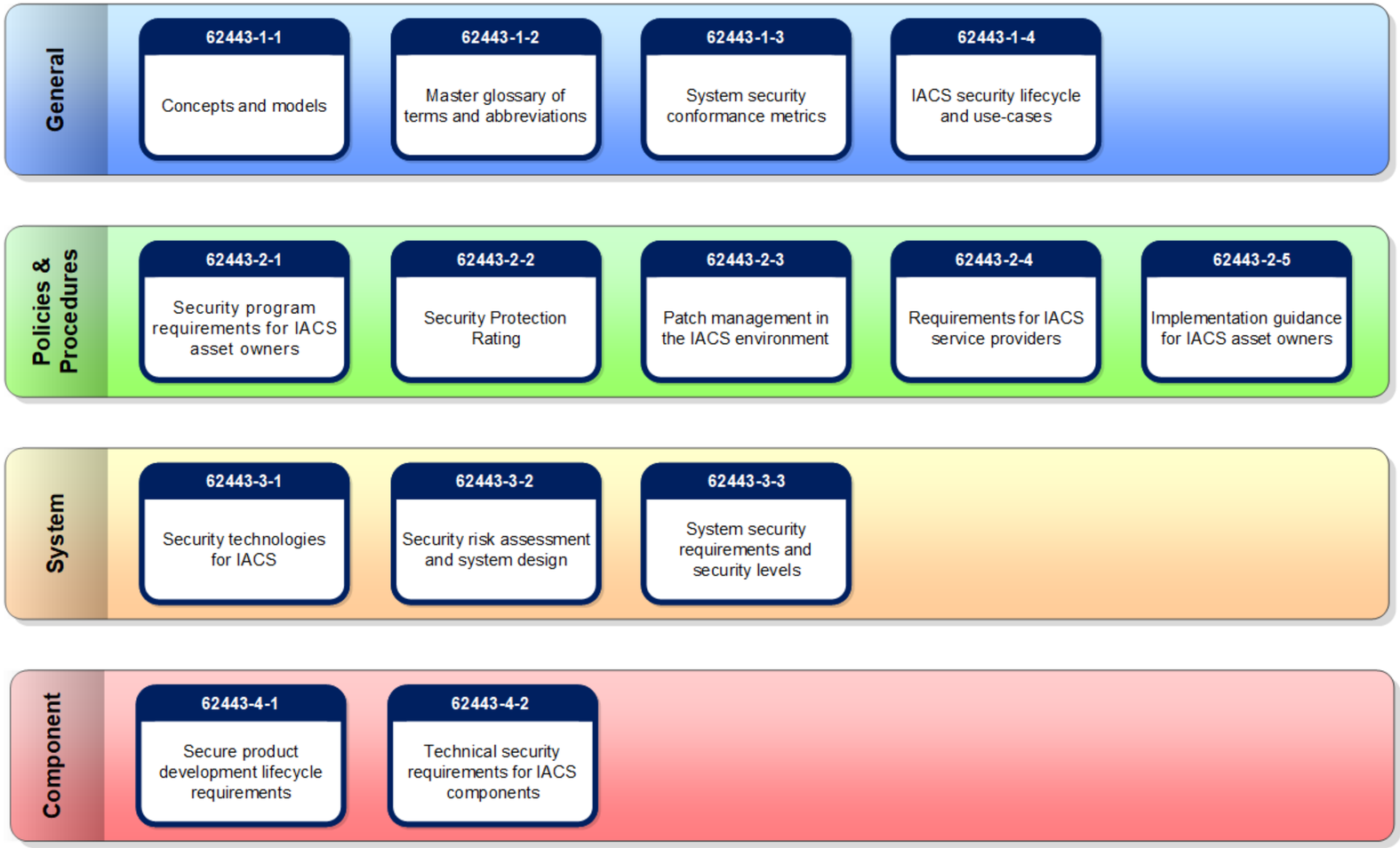
PROTECTION OF INDUSTRIAL AUTOMATION CONTROL SYSTEMS (IACS)

IEC 62443 deals with security of the industrial control system, popularly known as the Industrial Automation and Control System (IACS)

The aim of the standard is **to ensure that a product supplier, integrator or an asset owner follows an efficient method for secured process with a key aspect on safety of the personnel** and the production, availability, efficiency and quality of the production of the IACS as well as the safety of the environment.

IEC 62443 standard family is divided into **four parts** i.e.

(1) General; (2) Policies & Procedures, (3) System and, (4) Component



IT system vs IACS

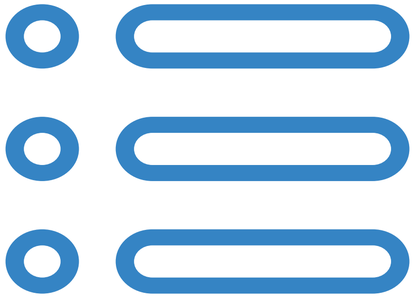
KEY DIFFERENCES

There are several **key differences** with respect to the security between the traditional **IT security environment** and **IACS security environment**

Security Topic	IT System	IACS
Antivirus	Widely used and updated	Not always and difficult to use
Life cycle	3-5 years	5-20 years
Patch management	Often	Rare, often approved by manufacturers
Change management	Regular and schedule	Rare
Time dependency	Delay accepted	Critical
Availability	Working hours, short failures accepted	24/7 base
IT Security Awarness	Good	Poor
Security Tests	Widespread	Rare and problematic
Test Environment	Available	Rarely available

IEC 62433 Structure

4 CATEGORIES



General: explains the basic terminologies, concepts, and abbreviations used in the series.

- **Standard 62443-1-1** presents the concepts and models of the series.
- The technical report **62443-1-2** contains a glossary of terms and abbreviations used throughout the series.
- The **standard 62443-1-3** describes a series of metrics derived from the basic requirements (FR) and system requirements (SR).

Policies and procedures: describes the policies and procedures that are required and used to implement a cyber-security management system.

- **Standard 62443-2-1** describes what is required to define and implement an effective IACS Cyber Security Management System. This standard is aligned with the ISO 27000 series.
- The **standard 62443-2-2** provides specific guidance on what is required to operate an effective IACS Cyber Security Management System.
- **Technical Report 62443-2-3** provides guidance on the specific topic of Patch Management for IACS.
- **Standard 62443-2-4** specifies requirements for suppliers of IACS.

System requirements: describes the security requirements for a system in an IACS environment.

- The technical report **62443-3-1** describes the application for different safety technologies to an IACS environment.
- The **standard 62443-3-2** addresses the risk assessment and the system design for IACS.
- **Standard 62443-3-3** describes the basics of the security requirements and the Security Assurance level (SL).

Component Requirements: describes the security requirement of a component in an IACS environment.

- **Standard 62443-4-1** describes requirements that apply to the development of products.
- The **standard 62443-4-2** contains requirements, which allow a detailed mapping of the system requirements (SR) to subsystems and components of the system under scope.

IEC62443 Roles (1/3)

IEC 62443 STANDARD DEFINES THREE DIFFERENT ROLES

PRODUCT SUPPLIER

The product supplier is **responsible** for the **development and testing of the control system** comprising of the application (antivirus, whitelisting etc.), **embedded device** (PLC, DCS etc.), network device (firewalls, routers, switches etc.), **host devices** (operator stations, engineering stations etc.) working together as system or a subsystem defined in IEC 62443 3-3, IEC 62443 4-1, IEC 62443 4-2.

RESPONSABILITIES

IEC62443 Roles (2/3)

IEC 62443 STANDARD DEFINES THREE DIFFERENT ROLES

SYSTEM INTEGRATOR

System integrators are responsible for the **integration** and **starting up** an IACS automation solution of the product in conformance with the **security levels (SL)** required by the customer using a process compliant with IEC 62443 2-4, IEC 62443 3-2, IEC 62443 3-3.

RESPONSABILITIES

IEC62443 Roles (3/3)

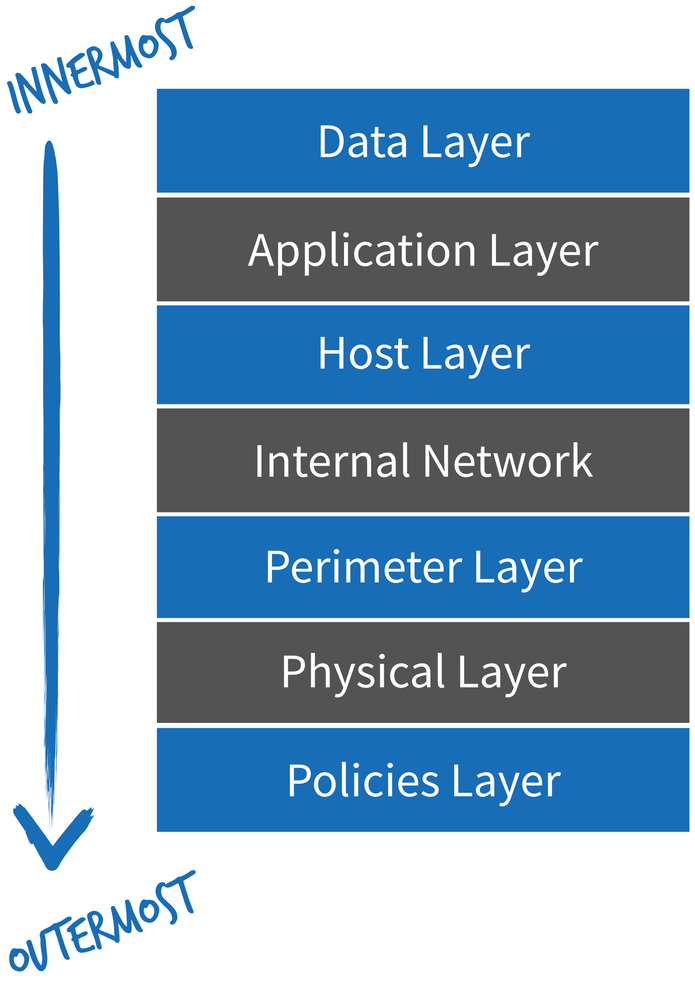
IEC 62443 STANDARD DEFINES THREE DIFFERENT ROLES

ASSET OWNER

The asset owner is **responsible** for the **operational and maintenance capabilities** with the help of the policies and procedures defined in IEC 62443 2-1, IEC 62443 2-3 and IEC 62443 2-4 of the automation system developed by installation of the automation solution at a particular site.

RESPONSABILITIES

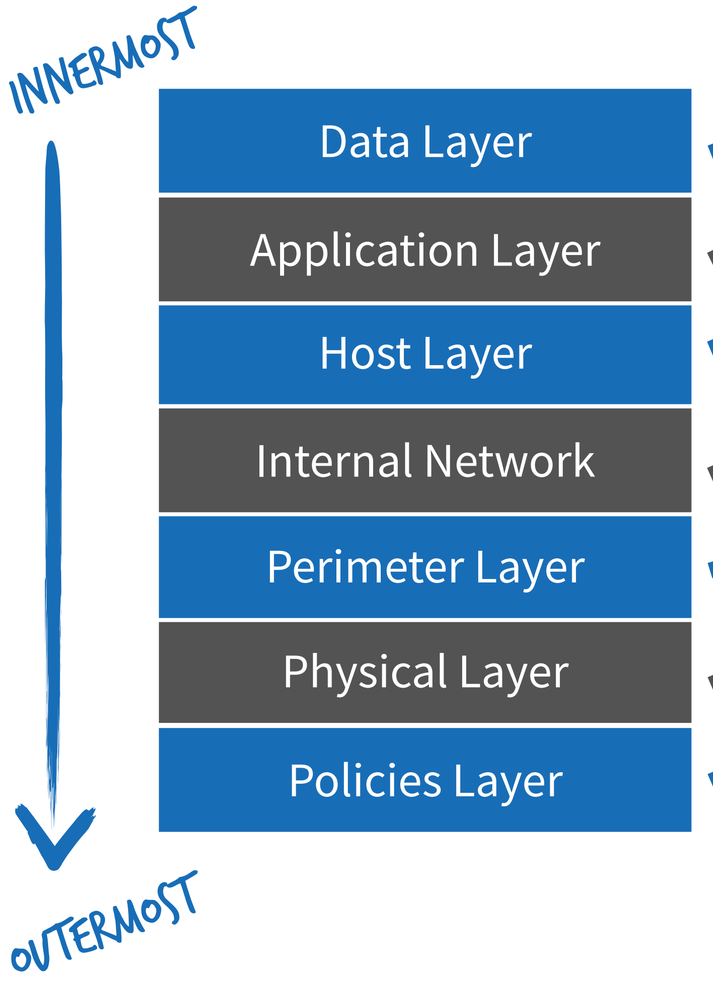
IEC 62443 Concepts: Defense in Depth (1/2)



Concept

Defense in depth is a **layered security mechanism that enhances security of the whole system.** The **benefit** of this mechanism is that during an attack, **if one layer gets affected, other layers can keep assisting** to protect against, detect and react to other attacks.

IEC 62443 Concepts: Defense in Depth (1/2)

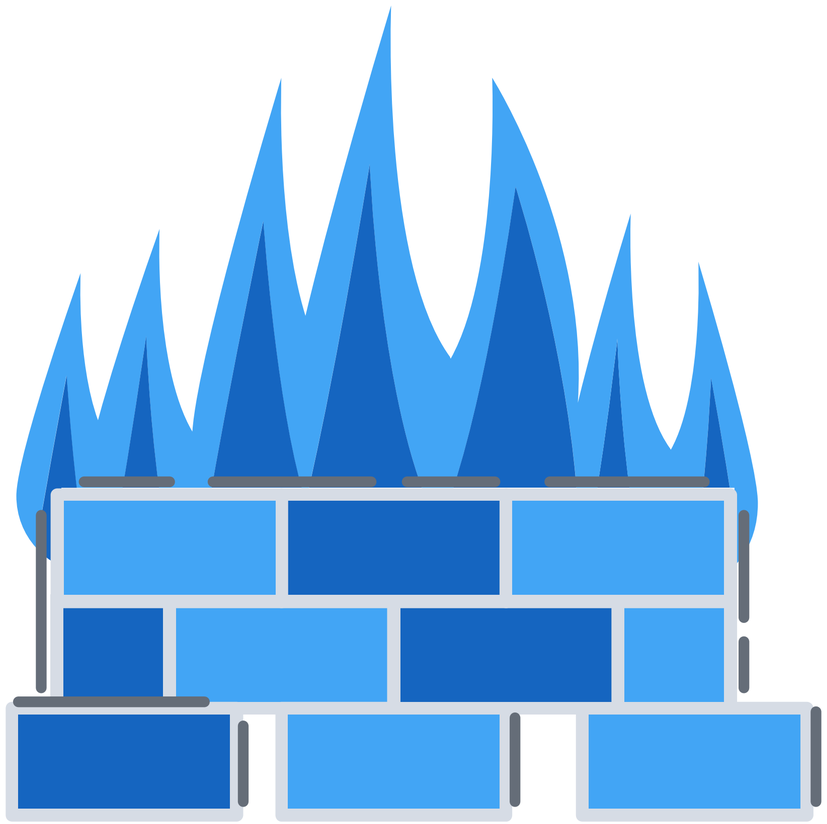


Concept

Defense in depth is a **layered security mechanism that enhances security of the whole system.** The **benefit** of this mechanism is that during an attack, **if one layer gets affected, other layers can keep assisting** to protect against, detect and react to other attacks.

- **Data Layer** is the innermost layer and can be used for **Access Control List** and encryption of data.
- **Application Layer** is the next layer used for installing **antivirus** software and application hardening.
- **Host Layer** is used for the patch implementation of vulnerability detected and authentication of the users.
- **Internal Network** is used for **IPsec** (Internet Protocol Security) for IP communications, authentication and encryption of the packet that takes part in a communication system; **IDS** (Intrusion Detection System) detects the intrusion of every user (authorized or unauthorized).
- **Perimeter Layer** is used for implementing the **firewalls** and **VPN** quarantining.
- **Physical Layer** is the layer where the useful guards, switches, locks, ports and **physical access** are employed.
- **Policies Layer** is the outermost layer where the **security policies and procedures** for the Industrial Automation Control Systems networks are defined.

IEC 62443 Concepts: Zones



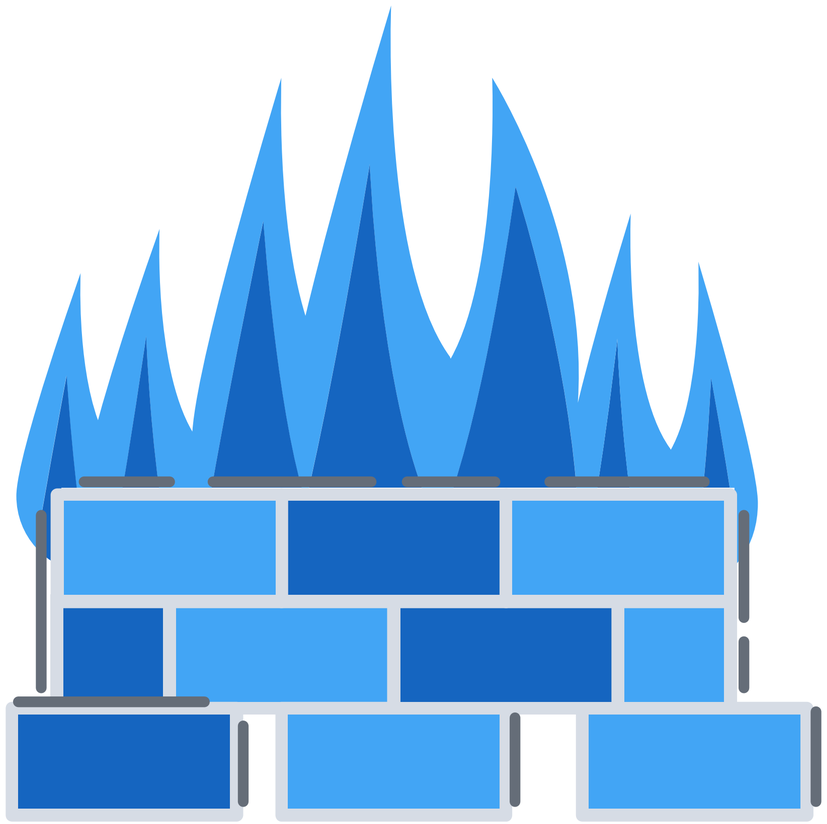
Security Zones

Security zones are **physical or logical groupings of assets** that **share common security requirements** and isolate the critical control systems components.

A special type of security zone is the demilitarized zone (DMZ), which segments the external network with the internal IACS network with help of security components (e.g., firewall).

This concept provides a **layered security** approach, with a **“defense in depth”** approach being taken into account.

IEC 62443 Concepts: Conduits



Conduits

"**Conduits** are the special type of security zone that groups communications that can be **logically organized into information flows** within and also external to a zone. It can be a single service (i.e., Ethernet network) or be a multiple data carrier."

Conduits control access to the zone by resisting several attacks like denial of service and malware attacks, and protects the integrity and confidentiality of the network traffic.

IEC 62443 Security Levels (SL)

ON THE BASIS IEC 62443 3-3 AND IEC 62443-4-2

- **Security Level (SL) concept focus on the zones** of the IACS. SLs provide a frame of reference for **making decisions on the use of countermeasures** and devices with different inherent security capabilities.

- The SL may also be used to **identify layered Defense-in-Depth strategy** for a zone that includes hardware and software base **technical countermeasures.**

IEC 62443 Security Levels (SL) (1/2)

ON THE BASIS IEC 62443 3-3 AND IEC 62443-4-2

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No objective
SL2	Capability to protect against intentional violation using simple means with low resources, general skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL4	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical damage	Industrial specific	High	Aggressive

IEC 62443 Security Levels (SL) (2/2)

ON THE BASIS IEC 62443 3-3 AND IEC 62443-4-2

- **SL1 -** Prevents the unauthorized disclosure of information via **eavesdropping** or casual exposure.

- **SL2 -** Prevents the unauthorized disclosure of information **to an entity actively searching for it using simple means** with low resources, generic skills and low motivation.

- **SL3 -** Prevents the unauthorized disclosure of information **to an entity actively searching for it using sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation.

- **SL4 -** Prevents the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with **extended resources**, IACS specific skills and high motivation.

IEC 62443 Maturity Levels (SL) (1/2)

ON THE BASIS IEC 62443 2-4 AND IEC 62443-4-1

These levels **define the benchmarks** that are requirements defined by the standards IEC 62443 2-4 and IEC 62443 4-1. Each level is progressively more advanced than the previous level.

The **service providers** and the **asset owners** are required **to identify the maturity level associated with the implementation of each requirement.**

IEC 62443 Maturity Levels (SL) (2/2)

ON THE BASIS IEC 62443 2-4 AND IEC 62443-4-1

Maturity Level	Category	Description
ML1	Initial	Capability of performing a service without a documented process that is poorly controlled
ML2	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel
ML3	Defined	Capability of performing ML2 level, including evidence of practicing the process (e.g., documented process) plus list of participants in the training of personnel
ML4	Improved	Capability of performing ML3 level, including demonstration of continuous improvement (e.g., internal audit report)

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

simone.soderi@unipd.it

M1.1 - Basic Concepts

Thanks for your attention!