

Security and Risk: Management and Certifications Simple (for real)



Gabriel Rovesti

Summary

[2 Course Introduction (Soderi Part) 3](#_Toc160099515)

[3 M1.1 - Basic Concepts 3](#_Toc160099516)

[4 M1.2 – Basic Concepts 16](#_Toc160099517)

[5 M2.1 – Planning for Cybersecurity 17](#_Toc160099518)

[6 M2.2 – Planning for Cybersecurity 18](#_Toc160099519)

[7 M3.1 – Cybersecurity Operations and Management 19](#_Toc160099520)

[8 M5 – Speaker’s intro and Basic Information (Belli Part) 20](#_Toc160099521)

[9 M6.1 – Information Security Management System & ISO IEC 27001 21](#_Toc160099522)

[10 M3.2 – Cybersecurity Operations and Management 22](#_Toc160099523)

[11 M3.3 – Cybersecurity Operations and Management 23](#_Toc160099524)

[12 M3.4 – Cybersecurity Operations and Management 24](#_Toc160099525)

[13 M3.4.1 – Cybersecurity Operations and Management 25](#_Toc160099526)

[14 M3.5 – Cybersecurity Operations and Management 26](#_Toc160099527)

[15 M4.1 – Cybersecurity Operations and Management 27](#_Toc160099528)

[16 M4.2 – Cybersecurity Operations and Management 28](#_Toc160099529)

[17 M6.2 – Cloud Security 29](#_Toc160099530)

[18 M6.3 – Personal Data Processing 30](#_Toc160099531)

[19 M6.4 – Data center notification, NIST, CINI, law 31](#_Toc160099532)

[20 M7 – Certification of technology 32](#_Toc160099533)

[21 M6.5 – Nist CSF Laboratory 33](#_Toc160099534)

[22 M8.1 – Competencies e-CF NICE Agid 34](#_Toc160099535)

[23 M8.2 – Competencies NICE and DoD Pathways and ENISA 35](#_Toc160099536)

[24 M9 – Certification of people 36](#_Toc160099537)

[25 M10 – Certifications available on the market 37](#_Toc160099538)

[26 ISACA Chapter Presentation 38](#_Toc160099539)

[27 M11.1 – Management Systems audit and techniques 39](#_Toc160099540)

[28 M11.2 – Practical cases. Information Security Management System (ISMS) audit 40](#_Toc160099541)

**Disclaimer**

# Course Introduction (Soderi Part)

The course is mainly divided into two parts (two teachers: Simone Soderi = red / Antonio Belli = blue)

1. Basic Concepts;

2. Planning for Cybersecurity;

3. Cybersecurity Operations and Management;

4. Security Assessment and use cases;

5. Certification and Frameworks for Organizations and management systems;

6. Certification of products and technologies;

7. Frameworks that describe the competencies;

8. Certification of people;

9. Most common Certifications available on the market;

10. Audit techniques and approach examples

About the exam:

* last year, there was a report made about the contents of the course
  + many copied with ChatGPT, so the professor is quite vocal about it
* this year, it’s not defined yet

Basically, the contents of “00-Course Introduction” is a presentation about thesis possible with the teacher and other general content. Move on.

# M1.1 - Basic Concepts

Let’s first talk about the cyberspace (as defined by Nation Research Council in USA) based mainly on:

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

Immagine che contiene testo, cerchio, Dispositivo di archiviazione dati, compact disk

Descrizione generata automaticamenteThe following are the cybersecurity knowledge areas, with figure coming from the CyBOK (Cyber Security Body of Knowledge):

In general, we can say:

* 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
  + Immagine che contiene testo, schermata, Carattere, logo

    Descrizione generata automaticamenteand ultimately some of the structure is relatively arbitrary

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 asset.

We give some useful definition:

* asset
  + Where
    - Software-hardware
  + What
    - *Data contained* in an information system; or a service provided by a system or a *system capability*
      * such as *processing power* or communication bandwidth
      * an item of system equipment
        + such as hardware, firmware, software, or documentation
* risk
  + Where
    - Measure-impact
  + What
    - 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
  + Where
    - Capability-danger
  + What
    - 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
  + Where
    - flaw-design
  + What
    - 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

We discuss also about information security, which is:

* Preservation of *confidentiality, integrity and availability* of information
* In addition, other properties, such as *authenticity, accountability, non-repudiation, and reliability* can also be involved

Immagine che contiene testo, schermata, Carattere, cerchio

Descrizione generata automaticamenteCybersecurity has different objectives:

Immagine che contiene testo, biglietto da visita, schermata, Carattere

Descrizione generata automaticamenteImmagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamenteBut also has different dilemmas:

Risk is the possibility that human *actions* or events *lead to consequences that have an impact* on what humans value. There are different dimensions to consider:

* *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

There are different reasons on why risk assessment is important (analytic process to reduce the risk and possibly mitigate the costs):

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamenteImmagine che contiene testo, schermata, cerchio, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamenteImmagine che contiene testo, schermata, cerchio, Carattere

Descrizione generata automaticamente

Cyber is a special case inside risk management (*cyber risk*):

* Cyber security risk assessment and management
  + fundamental special cases that everyone living and working within the digital domain
  + should understand and be a participant in it
* There are a number of global standards
  + aiming to formalize and provide a common framework
  + for cyber risk assessment and management

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamenteConsider the *difference* between the level of analysis inside systems (source [here](https://complianceforge.com/grc/policy-vs-standard-vs-control-vs-procedure)):

Immagine che contiene testo, schermata, cerchio, design

Descrizione generata automaticamenteStandards and Best Practices documents have different dimensions of value:

Immagine che contiene testo, Carattere, numero, schermata

Descrizione generata automaticamenteFollowing here, some *important standards and best practices documents*:

We define what is an effective security policy, made by a CISO and a Security Manager:

* A *set of rules and practices* that specify or regulate *how 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

There are different *security policy types*:

* *Access control:* How information is accessed
* *Contingency planning*: How availability of data is provided 24/7
* *Data classification*: How data are classified
* *Network securi*ty: How network systems are secured
* *Incident response*: How incidents are reported and investigated
* *Encryption*: How data are encrypted, the encryption method used
* *Physical access*: How access to the physical area is obtained
* *Cloud computing*: Security aspects of using cloud computing resources
* Immagine che contiene testo, schermata, diagramma, grafica

  Descrizione generata automaticamente*Security awareness*: How security awareness is carried out

The Standard Of Good Practice (SOGP) for Information Security is issued by the Information Security Forum (ISF), which develops best practices for large/small businesses, agencies and 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

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamenteThe SOGP is of particular *interest* to the following *individuals*:

Immagine che contiene testo, schermata, Carattere, menu

Descrizione generata automaticamenteThe SOGP organization gives good practice controls for hundreds of security topics:

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamenteSOGP has also different *activities*, according to how its process works:

The ISO and IEC have developed a growing family of standards in the ISO/IEC 27000 Suite of Information Security Standards that deal with ISMSs:

* *Information Security Management System*
  + which 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 organization’s risk acceptance levels designed to effectively treat/manage risks
  + analyzing requirements for the protection of assets, as required, contributes to the successful implementation of an ISMS

We immediately precisely clarify the *standardization bodies*:

* ISO
  + *International agency for the development of standards* on a wide range of subjects
  + to facilitate international exchange of goods and services and for cooperation
* IEC
  + Develops standards in a joint effort with ISO
  + in the areas of data communications, networking, and security

There are different principles inside ISO 27000, which contains the fundamental *principles contributing 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

Immagine che contiene testo, Carattere, numero, linea

Descrizione generata automaticamenteISO 27000 has a *family of standards* to consider:

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamenteThere are many ISMS requirements inside ISO 27001, mainly for ISMS certification:

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamenteAlso, inside ISO 27002, there is the Code of Practice for Information Security Controls, defining precise requirements to *satisfy ISMS requirements*:

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamenteWe also consider the *mapping from the two ISOs considered to ISF SOGP*:

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, Pubblicità online

Descrizione generata automaticamenteIEC 62443 deals with security of the industrial control system, popularly known as *the Industrial Automation and Control System (IACS)*, ensuring key aspects of safety, as shown here:

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

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

IEC 62433 has a specific *structure*:

* *General*
  + explains the basic terminologies, concepts, and abbreviations used in the series
* *Policies and procedures*
  + describes the policies and procedures that are required and used to implement a cyber-security management system
* *System requirements*
  + describes the security requirements for a system in an IACS environment
* *Component Requirements*
  + describes the security requirement of a component in an IACS environment

There are different roles inside IEC 62443:

* *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.
* *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.
* *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

We come to a key concept: defense in depth.

* Immagine che contiene testo, schermata, Carattere, linea

  Descrizione generata automaticamenteDefense 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

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

There are also two other concepts inside IEC 62443:

* 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 considered
* Conduits
  + 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 DoS and malware attacks, and protect the integrity and confidentiality of the network traffic

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*

We can characterize them as follows:

* SL1 - Prevents unauthorized disclosure of information via *eavesdropping* or casual exposure
* SL2 - Prevents 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
* Immagine che contiene testo, schermata, Carattere, numero

  Descrizione generata automaticamenteSL4 - 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

There are also IEC 62443 maturity levels:

* 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
* Immagine che contiene testo, schermata, Carattere, numero

  Descrizione generata automaticamenteThe service providers and the asset owners are *required to identify the maturity level associated with the implementation of each requirement*

# M1.2 – Basic Concepts

# M2.1 – Planning for Cybersecurity

# M2.2 – Planning for Cybersecurity

# M3.1 – Cybersecurity Operations and Management

# M5 – Speaker’s intro and Basic Information (Belli Part)

# M6.1 – Information Security Management System & ISO IEC 27001

# M3.2 – Cybersecurity Operations and Management

# M3.3 – Cybersecurity Operations and Management

# M3.4 – Cybersecurity Operations and Management

# M3.4.1 – Cybersecurity Operations and Management

# M3.5 – Cybersecurity Operations and Management

# M4.1 – Cybersecurity Operations and Management

# M4.2 – Cybersecurity Operations and Management

# M6.2 – Cloud Security

# M6.3 – Personal Data Processing

# M6.4 – Data center notification, NIST, CINI, law

# M7 – Certification of technology

# M6.5 – Nist CSF Laboratory

# M8.1 – Competencies e-CF NICE Agid

# M8.2 – Competencies NICE and DoD Pathways and ENISA

# M9 – Certification of people

# M10 – Certifications available on the market

# ISACA Chapter Presentation

# M11.1 – Management Systems audit and techniques

# M11.2 – Practical cases. Information Security Management System (ISMS) audit