

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



Gabriel Rovesti

Summary

[2 Course Introduction (Soderi Part) 3](#_Toc159959663)

[3 M1.1 - Basic Concepts 3](#_Toc159959664)

[4 M1.2 – Basic Concepts 8](#_Toc159959665)

[5 M2.1 – Planning for Cybersecurity 9](#_Toc159959666)

[6 M2.2 – Planning for Cybersecurity 10](#_Toc159959667)

[7 M3.1 – Cybersecurity Operations and Management 11](#_Toc159959668)

[8 M5 – Speaker’s intro and Basic Information (Belli Part) 12](#_Toc159959669)

[9 M6.1 – Information Security Management System & ISO IEC 27001 13](#_Toc159959670)

[10 M3.2 – Cybersecurity Operations and Management 14](#_Toc159959671)

[11 M3.3 – Cybersecurity Operations and Management 15](#_Toc159959672)

[12 M3.4 – Cybersecurity Operations and Management 16](#_Toc159959673)

[13 M3.4.1 – Cybersecurity Operations and Management 17](#_Toc159959674)

[14 M3.5 – Cybersecurity Operations and Management 18](#_Toc159959675)

[15 M4.1 – Cybersecurity Operations and Management 19](#_Toc159959676)

[16 M4.2 – Cybersecurity Operations and Management 20](#_Toc159959677)

[17 M6.2 – Cloud Security 21](#_Toc159959678)

[18 M6.3 – Personal Data Processing 22](#_Toc159959679)

[19 M6.4 – Data center notification, NIST, CINI, law 23](#_Toc159959680)

[20 M7 – Certification of technology 24](#_Toc159959681)

[21 M6.5 – Nist CSF Laboratory 25](#_Toc159959682)

[22 M8.1 – Competencies e-CF NICE Agid 26](#_Toc159959683)

[23 M8.2 – Competencies NICE and DoD Pathways and ENISA 27](#_Toc159959684)

[24 M9 – Certification of people 28](#_Toc159959685)

[25 M10 – Certifications available on the market 29](#_Toc159959686)

[26 ISACA Chapter Presentation 30](#_Toc159959687)

[27 M11.1 – Management Systems audit and techniques 31](#_Toc159959688)

[28 M11.2 – Practical cases. Information Security Management System (ISMS) audit 32](#_Toc159959689)

**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*:

# 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