Security and Risk Simple (for real)

Gabriel Rovesti

Contents

1. Disclaimer

Given the course has so much content, a complete notes file is definitely something we all need, basically an extended transcript of every set of slides (believe me, it was hell to browse - see for yourself and you will prove me right), here I will give a full revised short summary to avoid the unreadable (and soooo unnecessarily long - understandable given the subject but geez) sets of slides of this course. Hope this could be useful, between all of my other works. I think this was the heaviest file of notes I've ever written (some were 300/400 pages, but not so much notionistic and presented this bad really), literally hoping for the slides to finish or to have something useful. Content very interesting, but keep everything I've written in mind.

The professor of the first part is good in general but not for explaining the course material (many times makes reasonings then goes its own way skipping concepts), definitely boring. The professor of the second part is definitely competent and better, but terribly boring too.

Overall, the course is very very heavy and notional, useful but most of the time with unnecessarily long notions given throughout.

Book references are made across chapters to the "Effective Cybersecurity" made by William Stallings (quoted by course syllabus since it basically contains many things) to help you browse. Consider, lastly, files like "M0" and "M5", given they are basically professors' presentations modules, it's useless for anything related to the exam, so those are not included.

2. M1.1 - Basic concepts

(This here marks the First Part of the Course, made by professor Simone Soderi. On book: §1 - Best Practices, Standards, and a Plan of Action)

2.1. Key terms

Cyberspace

- Consists of:
  - artifacts
  - information
  - interconnections

CyBOK - Cyber Security Body of Knowledge

- It aims to codify the foundational and generally recognised knowledge on cyber security
- It's grouped into five broad categories

Cybersecurity

- Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches used to protect environment and assets
- It's grouped into five broad categories

Asset

- Data contained inside an information system or a system capability
- Generally hardware, software, etc.

Risk

- Possibility that human actions may lead to consequences or have an impact to humans value
- Estimate the likelihood of events, measuring their impact

Threat

- A potential for violation of security, exploiting a vulnerability and getting danger

Vulnerablity

- A flaw or weakness in a system's design that can be exploited violating security policies

Information security

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

2.2. Cybersecurity objectives and dilemmas

Objectives:

- *Confidentiality*: property of data not disclosed to unauthorized entities
- *Integrity*: Property of data not been changed
- *Availability*: Resource or property being accessible or usable upon demand
- *Authenticity*: Property of being genuine and being able to verify that users are who they say they are
- *Accountability*: Property ensuring that the actions of a system entity may be traced uniquely to that entity, which can then be held responsible for its actions

Dilemmas:

- Scale and Complexity of Cyberspace
- Nature of Threat
- User needs vs Security implementation
- Difficulty estimating costs and benefits

2.3. Risk assessment

Risk:

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

Many processes regard risk:

- Risk assessment
  - a process of collating observations and perceptions of the world that can be justified by logical reasoning or comparisons with actual outcomes
- Risk management
  - 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

Risk assessment:

- has to use analytic and structured processes to capture the potential for desirable and undesirable events, and a measure of the likely outcomes and impact
- it involves reviewing information collected as part of the risk (and concern) assessments
- this information forms the basis of decisions leading

It's important for many reasons:

- Identification and, if possible, estimation of hazard
- Assessment of exposure and/or vulnerability
- Estimation of risk combining the likelihood and severity (impact)
- Handle all cases inside the cyberspace
- Number of global standards aiming to formalize that

2.4. Governance structure terms

- Standards
  - Mandatory requirements regarding processes, actions and configurations that are designed to satisfy Control Objectives
- Control Objectives
  - Targets or conditions to be met
- Policies
  - 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
- Procedures
  - Documented set of steps necessary to perform a specific task or process in conformance with an applicable standard
  - There help address the question of how the organization actually operationalizes a policy, standard or control
- Guidelines
  - Recommended practices that are based on industry-recognized secure practices
  - We apply the guidelines where we cannot apply the standard

2.5. Standards and Best Practices documents

A number of organizations, based on wide professional input, have developed best practice types of documents as well as standards for implementing and evaluating cybersecurity (just to quote here)

- 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)
- 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)

2.6. Standard of Good Practice (SOGP)

A security policy:

- is 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, security principles followed by all relevant individuals
- it applies to all employees
- has many different types (e.g., access control, network security, etc.)

SOGP:

- is issued by the Information Security Forum (ISF). The goal of the ISF is the development of best practice methodologies, processes, and solutions
- is a business-focused comprehensive guide to identifying and managing information security risks
- is based on research projects and input from ISF members as well as analysis of the leading standards on cybersecurity
- is of particular interest to business manager or chief information security officers
- has several categories broken down into several topics, consistent with the structure of the standards
- has 3 main activities:
  - planning for cybersecurity
  - managing the cybersecurity function
  - security assessment

2.7. ISO/IEC 27000

The ISO and IEC have developed a growing family of standards in the ISO/IEC 27000 series that deal with ISMS - Information Security Management System.

- Information security management system (ISMS) consists of the policies, procedures, guidelines with the scope of protecting its information assets

- Systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives
- Based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks

ISO 27000 suite has principles which contribute to the successful implementation of an ISMS:

- raising awareness
- assigning responsibilities
- incorporating security
- ensuring a comprehensive approach
- preventing and detecting

It is composed by 4 categories:

- Overview and vocabulary
- Requirements
- Guidelines
- Sector-specific guidelines

2.8. ISO/IEC 27001

ISO 27001 is a management standard initially designed for the certification of organizations. It's composed by:

- Certification Audit
- Qualified individuals to develop and maintain an ISMS
- Obtaining certifications (third-party assessments) to enhance the value
- It can be mapped easily to meet ISF SOGP

2.9. ISO/IEC 27002

It provides the broadest treatment of ISMS topics in the ISO 27000 series and allows for selection of controls for ISMS.

- Allows to choose the controls needed to satisfy ISMS requirements
- Grants specific security controls to protect confidentiality, integrity and availability of information
- Uses a checklist of topics to map ISF SOGP correctly

2.10. IEC 62443

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

- It ensures 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

It's divided into four *parts*:

- General: basic terminologies and concepts
- Policies: required to implement a cybersec system
- System: describes security requirements for systems
- Component: same but for components

Different from normal IT systems given they are rarely patched or changed, but time dependency here is critical, less awareness overall.

It defines also some *roles*:

- product supplier
  - responsible for development and testing of the control system, embedded device and host device
- system integrator
  - responsible for the integration and starting up, with conformance to specific security levels
- asset owner
  - responsible for operational and maintenance capabilities

Let's list some *concepts*:

- Defense in depth
  - Layered security mechanism that enhances security of the whole system
  - Layers to be found here: data, application, host, internal network, perimeter, physical, policies
  - If one layer gets affected, the others will work anyway
- Security zones
  - Physical or logical groupings of assets that share common security requirements
- Conduits
  - Special type of security zone that groups communications that can be logically organized into information flows within and also external to a zone
  - They control access to the zone

Finally, its *security levels*:

- It focuses on the zones, making decisions on the use of countermeasures and can be applied to Defense in Depth
- Different ones to list:

- SL1 = Prevents eavesdropping
- SL2 = Prevents unauthorized disclosure
- SL3 = Prevents information to an entity searching for it using sophisticated means moderate resources
- SL4 = Prevents unauthorized disclosure of information with extended resources

And also *maturity levels*:

- They define the benchmarks
- They are required to identify the maturity level associated with the implementation of each requirement
- Different ones to list:
  - ML1 = Initial
  - ML2 = Managed
  - ML3 = Defined
  - ML4 = Improved

3. M1.2 - Basic concepts

(On book: §2 - Security Governance / §3 - Information Risk Assessment)

3.1. NIST Cybersecurity Framework

NIST is a U.S. federal agency that deals with measurement science, standards, and technology

- Their publications have a worldwide impact and bring an excellent resource on the field, providing prescriptive standards, tutorials and surveys defining for each countermeasures to act against threats
- The NIST Computer Security Resource Center (CSRC) is the source of a vast collection of documents that are widely used in the industry
- In response to the growing number of cyber intrusions at U.S. federal agencies, directed the NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure
- The framework is a collection of best practices that improve efficiency and protect components, used for nongovernment organizations, with the clear goal of continuous improvement while managing supply chain risk

Composed by three *parts*:

- *Core*: cybersecurity activities, desired outcomes, and applicable references
- *Implementation tiers*: Provide context on how an organization views cybersecurity risk
- *Profiles*: Represents the outcomes based on business needs, categories and subcategories

An organization can use the CSF core, profiles, and tiers with the supplementary resources to understand, assess, prioritize, and communicate cybersecurity risks:

- Understand and assess gaps of the organization
- Prioritize actions for managing risks
- Communicate with a clear language inside/outside the organization the risks

Composed by six *key functions*, each divided into specific categories and subcategories, each with sections, practices and standards:

- *Govern*
- *Identify*
- *Protect*
- *Detect*
- *Respond*
- *Recover*

Composed by *tiers*, which define the priority and the level of commitment:

- *Tier 1: Partial*
- *Tier 2: Risk informed*
- *Tier 3: Repeatable*
- *Tier 4: Adaptive*

Composed by *profiles*, selection of categories and subcategories which define a target profile and enable management, needing for maintenance and guidelines with concrete descriptions.

Some important documents of NIST to quote:

- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (this in particular, quoted by many slides sets)
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (2006)
- NIST SP 800-12, Introduction to Information Security, (2017)
- NIST SP 800-55, Performance Measurement Guide for Information Security (2008)
- SP 800-100, Information Security Handbook: A Guide for Managers (2006)

3.2. MITRE Att&ck

The MITRE Corporation is a private, not-for-profit company to provide engineering and technical guidance for the federal government and works in the public interest across all safety and cybersecurity fields.

MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks.

- This is an open framework for implementing cybersecurity detection and response programs
- It's available free of charge and includes a global knowledge base of adversarial tactics, techniques, and procedures (TTPs) based on real-world observations
- ATT&CK mimics the behaviour of real-life attackers, helping IT, security, and compliance organizations efficiently identify security gaps, evaluate risks, and eliminate vulnerabilities
  - Common taxonomy = same language
  - Database = tracking of activities and threat actors
- ATT&CK is largely a knowledge base of adversarial techniques, which focus isn't on the tools and malware but on how they interact, organizing a collection of tactics to efficiently detect and isolate threats
  - Tactics = Why to perform an action & what the adversary is trying to do
  - Techniques = How adversaries achieve their actions

This framework to address four main issues:

- Adversary behaviours: adversary tactics allowing to develop analytics

- Lifecycle models that didn't fit inside existing adversary lifecycle
- Applicability to real environments looking at observed incidents
- Common taxonomy across different types of adversary groups

We can even make a MITRE Att&ck Decomposition in case of enterprises:

- PRE-ATT&CK framework focusses on the preceding preparation phases. Preventing an attack is much cheaper
- A whole matrix is available, describing tactics and procedure examples

3.3. National Framework for Cybersecurity

The National Framework for Cybersecurity and Data Protection ("Framework") represents a tool for measuring an organization's security posture in terms of maturity and completion of activities aimed at reducing cyber risk.

- This is in use in Italy, complying with the GDPR and taking up elements from NIST Framework
- Some key principles:
  - Core
  - Controls
  - Informative references
  - Priorities levels
  - Maturity levels
  - Contextualization
  - Prototype of contextualization
- The following is for the framework methodology:
  - Phase 1 - Contextualization
    - Contextualizing the Framework to the reality of interest, achieving a Target Profile and desired reference to carry out assessments
  - Phase 2 - Measurement
    - In this second phase, the organization's current cyber security posture is identified, done through interviews with relevant individuals
  - Phase 3 - Evaluation
    - The results of the measurement phase are evaluated according to several possible scopes. This operation allows to calculate, starting from the values of coverage and maturity of each subcategory, metrics of interest for the scope itself

The output of the evaluation phase, and therefore the result of the entire assessment, is expressed through the metrics defined in the Framework, aggregated according to different criteria and projected onto different *scopes*, interpreting assessment results:

- Scope framework = assess how far current posture is set by Target Profile
- Risk management scope = how consistent the posture is with risk mitigation
- Compliance scope = align cybersec requirements to organization scopes

3.4. OWASP

Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software, being a source for devs and technologies to secure the web. Some documents to list here:

- OWASP Top 10
  - Standard awareness document for developers and web application security, representing broad consensus about most critical security risks to web apps
  - Risks are ranked based on frequency, severity and impact
- OWASP Cheat Sheet
  - Created to provide a set of simple good practice guides for application developers and defenders to follow
- OWASP Mobile Top 10
  - Consists of the most critical security risks to mobile applications. It represents a broad consensus about the most critical security risks to mobile applications
- OWASP Mobile Application Security (MAS)
  - It provides a security standard for mobile apps (OWASP MASVS) and a comprehensive testing guide (OWASP MASTG)
  - It covers the processes, techniques, and tools used during a mobile app security test, as well as an exhaustive set of test cases that enables testers to deliver consistent and complete results
  - There is a checklist - OWASP Mobile Application Security Checklist - containing links to the MASTG test case for each MASVS requirement, see if they are compliant
- OWASP Risk Rating Methodology
  - Attackers can take a variety of routes through your application to cause damage
  - Procedure of following a path of several steps for the classification of threats: identifying, estimating, determining, deciding and customizing

3.5. Cybersecurity Management Process

- An essential characteristic of cybersecurity provision is that it is not a single end that is attained but an ongoing process

- The goal of effective cybersecurity is constantly receding as management makes an effort to keep up with changes in the cyberspace ecosystem
- Two cyclic processes working at an executive level (organizational) and at a business level (infrastructural)

4. M2.1 - Planning for Cybersecurity - Security Governance/Management and Risk Assessment

(On book: §2 - Security Governance / §3 - Information Risk Assessment / §4 - Security Management)

4.1. Security governance

Governance allows to:

- Establish policies and continuous monitoring of their proper implementation
- Includes the mechanisms required to balance the powers of the members (with the associated accountability) and their primary duty of enhancing the prosperity and viability

Security governance:

- is the process of establishing and maintaining a framework and supporting management structure and processes
  - also, the system by which activities are directed and controlled
- allows to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls
- wants to provide assignment of responsibility, all in an effort to manage risk

To better understand the role of security governance, it is useful to distinguish between *security*:

- *governance*
  - process that develops the security program that adequately meets the strategic needs of the business
  - it communicates the mission priorities and overall risk tolerance
- *management*
  - supervision and making of decisions necessary to achieve business objectives through the protection of the organization's information assets
  - uses information as inputs into the process that realizes the security program and defines the profiles
- *implementation/operations*
  - implementation, deployment and ongoing operation of security controls defined within a cybersecurity framework

  - it integrates into the lifecycle and monitors security performance continuously

The *security program* is the management, operational, and technical aspects of protecting information and information systems

- It consists of policies, procedures, and management structure and mechanism for coordinating security activity

In an ISMS:

- reports help to define the threat and level of risk
- standards and best practices provide guidance on managing risk
- feedback help improve the effectiveness of policies and technical mechanisms

Security governance establishes different principles:

- ITU-T X.1054 establishes as a key objective "the alignment of information security objectives and strategy with overall business objectives and strategy"
- We can list 6 principles:
  1. Establish organization wide information security
  2. Adopt a risk-based approach
  3. Set the direction of investment decisions
  4. Ensure conformance with internal and external requirements
  5. Promote a security-positive environment for all stakeholders
  6. Review performance in relation to business outcomes

Given IT as a whole represent systems which have interest in the context of a business or other enterprise, having interest or concern for others:

- The IT Governance Institute defines five basic outcomes of information security governance that lead to successful integration of information security with the organization's mission
  - Strategic alignment
  - Risk management
  - Resource management
  - Value delivery
  - Performance measurement

NIST SP 800-100 lists the following key activities, or *components* that constitute effective security governances:

- Strategic planning
- Organizational structure

- Establishment of roles and responsibilities
- Integration with the enterprise architecture
- Documentation of security objectives in policies and guidance

4.2. Strategic planning

Let's define three hierarchically related aspects of strategic planning:

- Enterprise strategic planning
  - Involves defining long-term goals and objectives for an organization and the development of plans to achieve, with ongoing oversight
- IT strategic planning
  - Considering development and changes to involve new arrangements with outside providers and use of mobile devices
  - Activities may create unintended barriers to flexibility, introducing risk. IT management must be guarded against that
  - There is a whole process for this one:
    - Two to five years business and technology outlook: look at major trends
    - Strategic deep dive: identify a number of high-impact areas to inform the overall planning process
    - Current-state assessment: analysis of current state of all IT-related systems and policies, bringing sets of recommendations
    - Imperatives, roadmaps and finances: discussion of strategic objectives and a budget for investment plans, reflecting the organization priorities
    - Governance process and decision making: approval of budget, information taken from preceding phases used to guide the governance process
    - Regular reviews: monthly-based reviews culminating in a year-end assessment, continuing to improve into following years, hence modifying inputs and processes
- Information security strategic planning
  - Aligned with enterprise and IT strategic planning
  - A *strategic plan* is a document used to communicate, within the organization, the organization's goals, the actions needed to achieve those goals, and all the other critical elements developed during planning exercises
    - This should be approved by executives and committees, while regularly reviewed

4.3. Organizational structure

The organizational structure to deal with cybersecurity depends on the size of the organization, its type, and the organization's degree of dependence on IT.

- The Information Security Governance Framework includes the governing cycle to direct, monitor, and evaluate the ISMS
- This cycle is in accordance with ISO 27001 that the organization shall establish, implement, maintain, and continually improve an ISMS
- The evaluation function triggers communication with stakeholders in the form of a report, both for accountability and corporate values respect

It has a full cycle to respect:

- Direct: leading strategies, developing a security policy
- Monitor: performances measured with metrics
- Evaluate: assessing and verifying the results of monitoring
- Communicate: reporting stakeholders' requirements

4.4. Security report

Reporting enables stakeholders to ensure that information security is being managed effectively, including policies, evaluation and responses to a system.

- Includes costs and benefits
- Value of inventory and information assets
- Economic value of security and information assets
- Risk reduction

A report should include:

- Introduction
- Statis
- Updates
- Significant issues (if any)
- Decisions required (if any)

4.5. Security roles

We can have different roles to consider:

- C-level
  - Refers to high-ranking executives in an organization

  - Officers who hold C-level positions set the company's strategy, make high-stakes decisions, and ensure that the day-to-day operations align with fulfilling the company's strategic goals
- Chief executive officer (CEO)
  - Responsible for the success or failure of the organization
- Chief operating officer (COO)
  - Generally second in command to the CEO. Oversees the organization's day-to-day operations on behalf of the CEO, creating the policies and strategies
- Chief information officer (CIO)
  - In charge of IT strategy and the computer, network, and third-party
- Chief security officer (CSO)/Chief information security officer (CISO)
  - Tasked with ensuring data and systems security
- Chief risk officer (CRO)
  - Charged with assessing and mitigating significant competitive, regulatory, and technological threats to an enterprise's capital and earnings
- Chief privacy officer (CPO)
  - Charged with developing and implementing policies designed to protect employee

It is important to have a structure with clear responsibilities but also metrics to measure the goals

4.6. Security policies

NIST SP 800-53 rev.5 "Security and Privacy Controls for Information Systems and Organizations" defines an information security policy as: "an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information".

- It is an essential component of security governance, providing a concrete expression of the security goals and objectives
- The policies, together with guidance documents on the implementation of the policies, are put into practice through the appropriate selection of controls to mitigate identified risks
- The policies and guidance need to cover information security roles and responsibilities, a baseline of required security controls, and guidelines for rules of behavior for all users of data and IT assets

4.7. Security approach and framework

Effective security governance requires the development of a framework, which is a structured approach for overseeing and managing risk for an enterprise.

- The implementation and ongoing use of the governance framework enables the organization's governing body to set clear direction for and demonstrate their commitment to information security and risk management

- The definition, monitoring, and maintenance of a security governance framework involves a number of tasks:
  - Appoint a single executive to be ultimately responsible for security governance
  - Decide and communicate to top executives the objectives of the security governance framework
  - Ensure integration of the security architecture with the enterprise architecture
  - Include a process that enables the governing body to evaluate the operation of the information security strategy
  - Regularly review the organization's risk willingness to ensure that it is appropriate for the current environment in which the organization operates
  - Formally approve the information security strategy, policy, and architecture

4.8. Security direction, evaluation and best practices

A governing body is responsible for ensuring that there is effective security direction.

- SOGP recommends that effective security direction be provided by a combination of a single individual responsible for information security supported by a governing body
- The single individual is a CISO or equivalent implementing security approach
- The SOGP also recommends that the governing body include the CISO and have a mission to support the CISO
- Other members of the governing body could include human resources
- Governing body assists in the coordination of security activities and ensuring that the CISO has the resources and authority

Those are responsible for enterprise governance and information security governance need to be open to evaluation of their efforts at governance. The metrics fall into three categories:

- Executive management support and security awareness
- Business and information security relationship
- Information protection

Security governance also enlists some best practices:

- Security Governance Framework
- Security Direction
- Information Security Strategy
- Stakeholder Value Delivery
- Information Security Assurance

4.9. Risk assessment

Risk assessment is a complex subject and a good way to begin looking at risk assessment is to consider the terminology.

- These terms are based largely on definitions in ISO 27005 "Information Security Risk Management System Implementation Guidance", but also NIST SP 800-30 "Guide for Conducting Risk Assessments"

Threats and vulnerabilities need to be considered together:

- A *threat* is an agent acting on a vulnerability produces a security violation, or breach
- A *vulnerability* is a weakness in a system's security procedures, design, implementation, or internal controls

The level of risk is a measure that an organization can use in assessing the need for and the expected cost of taking remedial action in the form of risk treatment. This is measured in *impact* on two elements:

- Asset: Develop an inventory of the organization's assets, which includes an itemization of the assets and an assigned value for each asset.
- Threat: For each asset, determine the possible threats that could reduce the value of that asset

Then, for each asset, determine the impact to the business, in terms of cost or lost value, of a threat action occurring.

There is also the *likelihood*, made up of three elements:

- Threat: For each asset, determine which threats are relevant
- Vulnerability: For each threat to an asset, determine the level of vulnerability to the threat
- Controls: Determine what security controls are currently in place to reduce the risk

Then determine how likely it is that a threat action will cause harm, based on the likelihood.

- $\text{Security Risk} = \text{Impact x Likelihood}$
- The level of risk is determined as the combination of the cost of the threat occurring combined with the likelihood of the threat occurring
  - This is especially important in terms of determining a budget allocation

Challenges that an organization faces in determining the level of risk fall into two categories:

- The difficulty of *estimating*
  - Four main elements:
    - Put value on assets
    - Determine the entire range of threats
    - Vulnerabilities one may not be aware of
    - Effectiveness of given controls
- The difficulty of *predicting*
  - Four main elements:
    - Change and impact on assets
    - Assess and determine effect on threats, even without complete knowledge of them
    - Changes within the organization may create unexpected vulnerabilities
    - New technologies may provide opportunities and is difficult to predict the nature of such

4.10. Risk management

NIST Cybersecurity SP 800-37 "Risk Management Framework for Information Systems and Organizations" states that:

- Risk management includes a disciplined, structured, and flexible process for organizational asset evaluation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring
- It also includes enterprise-level activities
- It is an iterative process:
  - Assess likelihood and impact
  - Identify security controls
  - Allocate resources, roles and responsibilities
  - Monitor and evaluate risk treatment effectiveness
- Risk management for large organization use a broader framework (ISO 27005), iterative process made up of continual changes, consisting of separate activities:
  - Context establishment
  - Risk assessment
  - Risk treatment
  - Risk acceptance
  - Risk communication and consultation
  - Risk monitoring and review

4.11. Asset identification

A first step in risk assessment is to document and determine values for the organization's assets:

- An asset is anything of value to the business
  - Key concerns are loss of a device or device malfunction
  - Availability is another key consideration taking into account disruption losses and recovery expenses
- The challenge is to develop a uniform way of documenting the assets
- The input for asset evaluation needs to be provided by owners and custodians of assets

There are different *categories* of assets:

- Hardware
  - Servers, laptops, networking and telecommunications equipment

  - Key concerns are loss of a device, through theft or damage, lack of availability or device malfunction

- Software
  - These include applications, operating systems and other system software
  - Availability is a key consideration here, and asset evaluation must take account of disruption losses and recovery expenses
- Information
  - These comprise the information stored in databases and file systems, both on-premises and remotely in the cloud
  - Asset valuation needs to take into account the impact of threats to confidentiality, privacy, integrity, and authenticity
- Business
  - These include assets that don't fit into the other categories and also intangible ones (know-how, reputation, controls, etc.)

In order to effectively protect assets, an organization needs to provide a systematic method of documenting assets. This is done in an asset register that documents important security-related, including assets features and information ones.

4.12. Threat types and identification

Threat identification is the process of identifying sources with the potential to harm system assets. Threat sources are categorized into three areas:

- Environmental
  - Examples include floods, earthquakes, tornadoes, landslides, avalanches
- Business resources
  - Examples include equipment failure, supply chain disruption
- Hostile actors
  - Examples include hackers, hacktivists

Many efforts have been made to categorize types of threats, and there is considerable overlap in the definition of some common terms. A large category of threat is malicious software, or malware, which is a general term encompassing many types of software threats (e.g., malware, virus, worm, etc.)

- It is difficult to get reliable information on past events and to assess future trends
- Organizations are often reluctant to report security events in an effort to save corporate image and some attacks may be carried out without being detected by the victim until much later
- Three important categories of threat information sources are:
  - In-house experience

  - Already inside the organization

- Security alert services
  - Concerned with detecting threats as they develop to enable organizations to patch code, change practices or react
- Global threat surveys
  - Many available and ranked according to to the volume of security incidents surveyed
  - For each threat, the report provides a kill chain, which is a systematic process used to target and engage an adversary to create desired effects

There is also *SOC - Security Operation Center*, which is a facility that tracks and integrates multiple security inputs, checks risk, determines the targets of an attack, contains the impact of an attack, and recommends and/or executes responses appropriate to any given attack.

4.13. Control identification

Controls for cybersecurity include any process that modifies information security risk. Controls are administrative, technical, management, or legal in nature.

Control identification is defined in ISO 27005 and suggests the following steps:

- (1) Review documents containing information about the control
- (2) Check with the people with responsibility related to information security and the users about which controls are implemented
- (3) Conduct an on-site review of the physical controls, comparing those implemented with the list of what controls should be there
- (4) Review results of audits

NIST SP 800-53 should be consulted in the development of any risk treatment plan, considering it defines multiple families.

- For each control, the catalog provides a description of the control, supplemental guidance on implementation, a description of control enhancements

This NIST Interagency Report (NISTIR) provides guidance on how small businesses can provide security and NISTIR 7621 provides the following useful checklist of controls:

- Identity
- Protect
- Detect
- Recover

4.14. Vulnerability identification and classification

Vulnerability identification is the process of identifying *vulnerabilities*, which are weakness or flaws inside procedures, design or implementation.

There are different categories:

- Technical vulnerabilities
- Human-caused vulnerabilities
- Physical/environmental vulnerabilities
- Operational vulnerabilities
- Business continuity and compliance vulnerabilities

In the area of technical vulnerabilities, it is possible to be more precise and exhaustive:

- National Vulnerability Database (NVD)
  - It provides enhanced information above and beyond what's in the CVE list, including patch availability and severity scores
  - It also provides an easier mechanism to search on a wide range of variables
  - Parameters are related to the vulnerability's level of exploitability and the parameters related to the vulnerability impact metrics
- Common Vulnerability Scoring System (CVSS)
  - Overall score assigned, in a scale from 0.0 to 10.0
- Common Vulnerabilities and Exposures (CVE)
  - Simply a list of all publicly disclosed vulnerabilities with their data

4.15. Risk assessment approaches

Two factors of risk assessment, impact and likelihood, can be treated either quantitatively or qualitatively:

- Impact
  - A quantitative approach we can assign a specific monetary cost
  - Otherwise, qualitative terms, such as low, moderate, and high, are used
- Likelihood
  - The quantitative version of likelihood is simply a probability value
  - The qualitative likelihood can be expressed in such categories as low, medium, and high

For quantitative risk assessment:

- If all factors are expressed quantitatively, then it is possible to develop a formula that measure of the cost of security breaches as follows:
  - Level of risk = (Probability of adverse event) x (Impact value)
  - We can express the residual risk level using the mitigation factor that reflects the reduction in the probability of an adverse event:
    - Residual risk level = (Probability of adverse event)/(Mitigation factor) x (Impact value)
- If factors can be quantified with a reasonable degree of confidence, then previous equations should be used to guide decisions concerning how much to invest in security control
- As new security controls are implemented, cost of security breaches declines, but total cost of security increases
- At the end for the qualitative risk we need to define levels of risk

For qualitative risk assessment:

- It determines a relative risk rather than an absolute risk, usually sufficient for identifying the most significant risks
- It is clear that subjective estimates are inherent in the process, while evaluating between opinions and risks
- Has different impact categories:
  - Low (limited adverse effect)
  - Moderate/medium (serious adverse effect)
  - High (severe adverse effect)
- Ranges of probability are assigned to qualitative likelihood categories, usually Low/Medium/High, both based on estimates on number per year an event occurs
- The vulnerability to a particular threat is a function of the capability, or strength which can be expressed by a likelihood matrix, basically a function of frequency classifying impact
- A coarse analysis must be subject to judgment
- On average, each type of breach may be expected to yield the same amount of annual loss
  - Deal with low-likelihood, high- impact breach or with the high-likelihood, low-impact breach: is for management to decide
- A simple approach to risk assessment is to use a risk analysis worksheet, which is a table with one row for each potential threat/vulnerability pair. It has the following columns:
  - Security issue
  - Likelihood
  - Impact
  - Risk level

  - Recommended security controls
  - Control priorities
- Compliance requirements include those imposed by the organization's security policy. It should be rated as follows:
  - 0 = not implemented
  - 1 = partially implemented
  - 2 = implemented but not yet documented
  - 3 = implemented and documented

4.16. Factor Analysis of Information Risk (FAIR)

For purposes of risk assessment, it is useful to group security controls in a manner that reflects the risk assessment process.

- FAIR is an important contribution to risk assessment first introduced in 2005 and has been standardized by the Open Group, providing a methodology for analyzing risk
- The standards is probabilistic rather than predictive, understanding "the probable frequency and magnitude of future loss"
- It provides a more detailed set of guidelines than ISO 27005, providing definitions more specifically tied to risk analysis and based on a belief that subjective qualitative analysis is inadequate

The FAIR (Factor Analysis of Information Risk) risk analysis document, groups controls into four categories:

- (1) Avoidance controls
- (2) Deterrent controls
- (3) Vulnerability controls
- (4) Responsive controls
- FAIR adopts a top-down approach
  - based on historical data, to develop an estimate of loss event frequency, simply on the basis of how frequently a loss event has occurred in the past
- FAIR has different Risk Assessment Levels:
  - If the organization's management or security analysts do not have confidence that a good loss event frequency can be directly estimated: estimating threat event frequency and estimating vulnerability
  - The assessment of threat event frequency involves two aspects:
    - determining frequency of contact with assets
    - probability of acting against assets

- Contact can be physical or logical
  - Physical access is possible for employees and outside actors
  - Logical access is via a network
- Contact can be unplanned, or random, or it can be regular
  - Can have five levels of frequency: VH, H, M, VL, L (L=Low / M= Medium / H = High)
- Determine the probability that the threat agent will take action
- The two dimensions of vulnerability are the threat capability and the control strength and estimating capability involves looking at two factors:
  - Skill
  - Resources

4.17. Likelihood assessment

- The process of developing some sort of agreed-upon likelihood score that estimates the chance of a threat action
- The assessment considers the presence, tenacity, and strengths of threats as well as the presence of vulnerabilities and the effectiveness of security controls already in place
- This assessment is applied to each identified potential threat action and likelihood assessment for a given threat is shown in the following steps:
  - Step 1. Determine the likelihood that a threat event will occur
  - Step 2. Determine the degree of vulnerability
  - Step 3. Determine the likelihood that a security incident will occur
- This analysis needs to be repeated for every threat to every asset

4.18. Impact assessment

The process of developing some sort of agreed-upon impact score or cost value that estimates the magnitude or the adverse consequence of a successful threat action.

- The essence of impact assessment is that, for a given threat to a given asset, you determine the impact on the asset if the threat were to become an actual security incident
- Detailed guidance on how to characterize impact and depends on two categories of loss:
  - primary loss
    - occurs directly as a result of the threat agent's action upon the asset
    - the owner of the affected assets is considered the primary stakeholder in an analysis
    - this event affects the primary stakeholder in terms of productivity loss, response costs, and so on

  - there are two aspects: asset and threat
  - next step is determining what threat action might apply to this asset: access/misuses/disclosure/modification/deny access
- secondary loss
  - occurs as a result of secondary stakeholders reacting negatively to the primary event
  - here, magnitude and loss event frequency are measured

Once the loss magnitude is estimated and the loss event frequency derived, it is a straightforward process to derive an estimate of risk, done separately for primary/secondary, then combining them to determine an overall risk.

- This is done, for example, via risk assessment matrices

4.19. Risk evaluation and treatment

Evaluation process:

- Once a risk analysis is done, senior security management and executives can determine whether to accept a particular risk and if not determine the priority in assigning resources to mitigate the risk

NIST SP 800-100 provides some general guidance for evaluating risk and prioritizing action:

- High
  - Strong need for corrective measures
- Moderate
  - A plan must be developed to incorporate these actions
- Low
  - Corrective actions must be determined in impact and understood if still required to accept the risk

ISO 27005 lists these options for treating risk:

- Risk reduction or mitigation
  - Done by implementing security controls, changing likelihood/consequences and removing threat sources
- Risk retention
  - Also called risk acceptance, it's a conscious decision to to pursue an activity despite the risk presented or to abstain from adding to the existing controls
  - This treatment is acceptable if the risk magnitude is within the risk tolerance level
- Risk avoidance
  - If the risk in a certain situation is considered too high and the costs of mitigating the risk down to an acceptable level exceed the benefits, the organization may choose to avoid the circumstance

- Risk transfer or sharing
  - Sharing or transferring risk is accomplished by allocating all or some of the risk mitigation responsibility or risk consequence to some other organization

5. M2.2 - Planning for Cybersecurity - Security management and models

(On book: Concepts extended of §4 - Security Management)

5.1. Threat modelling

A strategic process aimed at considering possible attack scenarios and vulnerabilities within a proposed or existing application environment for the purpose of clearly identifying risk and impact level.

- Think and find security issues
- Understand security requirements
- Develop and deliver better products
- Four step process
  - What are you building
  - What can go wrong
  - What should you do if things go wrong
  - Was analysis a good job
- Useful to create diagrams, giving an overview and identifying trust boundaries and Data Flow Diagrams (DFD)
  - made of data, processes, external entities, data store and trust boundaries themselves

5.2. STRIDE (Threat Modelling)

STRIDE is a threat classification system developed by Microsoft that is a useful way of categorizing attacks that arise from deliberate actions. This allows to see how different threats affect each other using previous tools.

- Spoofing identity
  - Illegally accessing authentication information
  - Area of authentication
- Tampering with data
  - Involves the malicious modification of data and unauthorised changes
  - Area of integrity
- Repudiation
  - Deny performing a malicious action
  - Area of non-repudiation (users who deny performing an action)

- Information disclosure
  - Threats that involve the exposure of information to individuals who are not supposed to have access to it
  - Area of confidentiality
- Denial of Service (DoS)
  - Attacks that deny service to valid users
  - Area of availability
- Elevation of privilege
  - An unprivileged user gains privileged access and has sufficient access to compromise or destroy the entire system
  - Area of authorization

5.3. DREAD (Risk Classification)

DREAD is part of a system for risk-assessing computer security threats that was formerly used at Microsoft. Its categories are:

- Damage Potential
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Evaluation of the threats that will be subject to security analysis, carried out the following methodology through:

- a rating defined on ten levels and applied to five risk categories
- levels are grouped into three categories, corresponding respectively to a High (8-10), Medium (4-8), and Low (0-4) risk levels
- this is a qualitative risk assessment

Mitigation is the point of threat modelling:

- Address each threat
- Redesign/Apply standard/Use software/Invent mitigations
- Accept vulnerability
- Address each threat

A model then needs to be checked (completely/accurately/covered/enumerating) and updating the diagram accordingly.

5.4. OCTAVE (Risk Management)

OCTAVE (Operationally, Critical, Threat, Asset, and Vulnerability Evaluation) is an approach to identify, assess, and manage risks to IT assets.

- This process identifies the critical components of information security and the threats that could affect their confidentiality, integrity, and availability
- This helps understand what information is at risk and design a protection strategy to reduce or eliminate the risks to IT assets
- Define essential components for a context-driven, self-directed information security risk evaluation

There aree three main methods:

1. The original OCTAVE method, (forms the basis for the OCTAVE body of knowledge)
   - Was designed for larger organizations with 300 or more users
   - The method was also designed to allow for tailoring by organizations adopting it
   - Made up of three phases:
     - Phase 1: Identify important information-related assets
     - Phase 2: Integrate threat analysis and inform mitigation decisions
     - Phase 2: Perform risk identification and develop risk mitigation
2. OCTAVE-S
   - For smaller organizations of about 100 users or less
   - Performed by an analysis team that has extensive knowledge of the organization and made up of three phases similar to the previous one
   - Does not rely on formal knowledge conducting workshops to gather information because it is assumed that the analysis team has working knowledge
3. OCTAVE-Allegro
   - A streamlined approach for information security assessment and assurance
   - This approach differs from previous OCTAVE approaches by focusing primarily on information assets and how are they used/stored/transported/processes, using workshops and questionnaires
   - Well suited for use by individuals who want to perform risk assessment without extensive organizational involvement, expertise, or input

5.5. Security management

The security management function entails establishing, implementing, and monitoring an information security program, under the direction of a senior responsible person.

- It involves multiple levels of management
  - Chief Information Security Officer (CISO)

  - Has overall responsibility for the enterprise information security program
  - Should designate and individual or a group to monitor and reflect changes on all organization environment, signaling violations with reporting mechanisms
  - The relation between executive management and the information security program, communicating and coordinating closely
  - Different roles and key security program areas:
    - Security and capital planning
      - This process enables to CISO to oversee all security projects throughout the organization
      - It involves three steps:
        - Identify
        - Analyze
        - Select
      - Also, the cost planning is applied and identified between different categories
    - Awareness and training
    - Information security governance
    - System development life cycle
    - Security products and services acquisition
    - Risk and configuration management
    - Contingency planning
    - Performance measures
- Information Security Manager (ISM)
  - Has responsibility for the management of information security efforts

NIST SP 800-18 "Guide for Developing Security Pans for Federal Information Systems", indicates that the purpose of a system security plan is to provide an overview of the security requirements of the system.

- The system security plan also delineates responsibilities and expected behaviour
- The system security plan is basically documentation of the structured process for a system
- It recommends that each information system in an organization have a separate plan document with different elements, basically categorizing everything

6. M3.1 - Cybersecurity Operations and Management - People/Information/Asset Management

(On book: §5 - People Management - §6 - Information Management - §7 - Physical Asset Management)

6.1. Human Resource Security

- Includes hiring, training, monitoring and handling employees
- Not only a technical challenge, but also employees also have to be aware of incidents and problems
- Harmful behaviors can occur, being both malicious and non-malicious

6.2. Hiring process

- ISO 27002 specifies "the hiring process ensures employees and contractors understand their responsibilities, suitable for their roles"
- They should be fully capable of perform the intended job, without making unfounded claims and avoiding "negligent hiring"
- Ask applicants as much detail as possible and in case get even criminal/credit record check, according to the country's law
- Employees should agree and sign the terms and conditions of contracts, including non-disclosure agreement and ensuring assets are confidential, agreeing to respect both the policy and confidentiality

6.3. During and after employment

- Each job should have specific cybersec tasks associated
- Employers and contractors should be aware of responsibilities, policy and training programs
- Several principles for personnel security:
  - Least privilege
  - Separation of duties
  - Mandatory vacations
  - Limited reliance on key employees
  - Dual operator policy
- During the termination of employment phase, organization's interests should be protected and all data/accounts/codes/assets regarding specific individuals will be removed

6.4. Security awareness

- Having a good security awareness and appropriate security training is as important as any other security countermeasure or control
- Activities that explain and promote security should develop into secure practices according to the specific role, accompanying good education/certification
- All employees have security responsibilities which the awareness program should constantly push, being focused on all people and categories
- A good program should include all aspects (e.g., communication, responsibility, help, security culture)
- According to ENISA we should have:
  - Plan/Assess/Design
  - Execute/Manage
  - Evaluate/Adjust
- Good communication materials should be available:
  - both in-house
  - and externally obtained
- Good education/certification programs should be also available, considering specialized training
- Role-based training also should encompass:
  - Manage
  - Design
  - Implement
  - Evaluate

6.5. Hardware management

- Hardware = any physical asset used to support corporate information or systems, including the software embedded within them and the operating systems
- Hardware Asset Management (HAM) deals specifically with hardware portion of IT assets, managing the physical components
- Its lifecycle is composed by:
  - Planning
  - Acquiring
  - Deploying
  - Managing

  - Disposing
- Destruction is important to handle data safely

6.6. Office equipment

- Every hardware inside an office, containing sensitive information processed by or stored inside of it
- Could be also multifunction devices (MFD)
- Each contains some processing power, and each is an asset to protect opportunities for threat and protection
- Could be exposed to several threats:
  - Network services
  - Information disclosure
  - DoS attacks
  - Physical security
  - OS security
- They can have a checklist containing organization measures

6.7. Equipment disposal

- SOGP recommends sensitive information should be securely destroyed
- Three main actions:
  - Clear = sanitize storage locations
  - Purge = apply logical/physical techniques to destroy encryption key on devices
  - Destroy = renders target data recovery infeasible

6.8. Industrial Control System (ICS) security

- Used in control industrial processes, including Supervisory Control and Data Acquisition (SCADA)
- Consists of a combination of control components used to achieve industrial objectives
  - HMI - Human-Machine Interface
  - Remote diagnostics and maintenance
  - Sensors
  - Actuators
  - Control
- They are distributed in insecure locations, often with microcontrollers with limited processing power

- There could be several threats:
  - Blocked/delayed flow of information
  - Unauthorized changes to instructions
  - Inaccurate information
  - ICS software or settings modified
  - Interference with operation of equipment protection systems, safety systems and system settings

6.9. Mobile device security

- Mobile device = Portable computing and communications device
- Prior to the use of smartphones, user devices were clearly confined over defined perimeters
- Now devices are constantly connected and there's always the need for more
- Each has a full stack, from hardware/firmware/mobile OS/application, being an entire ecosystem
- Millions of apps are available and each should conform to the organization security requirements; some examples
  - Rooting/Jailbreaking
  - Sideloading
- Many vulnerabilities to list, given they are outside of the corporate perimeter
- *Bring Your Own Device (BYOD)* - many organizations find convenient to have such a policy, inspecting devices and their features
  - configuring devices in such a way it's possible to access, protect and wipe data from them safely, even remotely

7. M3.2 - Cybersecurity Operations and Management - System Access

(On book: §10 - System Access)

7.1. System access and its functions

- Capability that restricts access to business applications, denying or limiting access to specific users
- *Functions*:
  - Authentication
    - Verifying the identity of user
  - Authorization
    - Granting of access by a security administrator, based on a security policy
  - Access control
    - Granting or denying specifying access requests
- Functions to establish rules and privileges and moderate access to an object in the system
- Each user has to be authorized properly, defining access privileges

7.2. Authentication factors and means

- Simplest way to access, including an identification and verification step
- Authentication factors are methods
  - The user has (possession factor) - tokens/smart cards/wireless tags
  - The user knows (knowledge factor) - passwords/PINs/tokens
  - The user is or does (inherence factor) - biometrics

7.3. Authenticators

- Means used to confirm a user/process/device
- Can be:
  - Multi-factor: use of one or more authentication means
  - Password-based: use of an ID and a password

7.4. Vulnerability of a password

- Instead of using a file retrieved by ID, to avoid storing password one can use a one-way hash function of the password
- Different kinds of attacks exist

  - Dictionary attacks
  - Specific account
  - Popular password
  - Password guessing
  - Hijacking
  - Monitoring/Exploiting
- Rely on hardware/SSO/password managers to avoid problems
- Select password not too short or easy to guess, eliminating guessable passwords

7.5. Hashed password and salt

- Combine the password with a fixed length salt value using an hashing algorithm
- In verification, the ID is used to see if result matches, therefore password is accepted
- Salt usage
  - prevents duplicate password
  - increases difficulty for attacks
  - nearly impossible to use same password for more systems
  - is non-deterministic

7.6. Password cracking

- Process of recovering secret password stored in a system
- Many approaches like developing a dictionary to crack all words or precomputing hash values

7.7. Password file access control

- Deny the attacker access to the password file
- Allowing it only for a privileged user
- File can become readable or physical security might be a problem, to use a policy to force users selecting passwords difficult to guess

7.8. Possession-based authentication

- Object the user possess for user authentications = hardware tokens
- *Memory cards*: have an electronic memory, store but do not process data, used for physical access alone
  - May require specific requirements and can be lost

- *Smart tokens*: have some specific physical characteristics, user interface, electronic interface and authentication protocol
  - Have a smart card, a microprocessor and a processing circuit
- *Electronic identity cards*: also called eID, they provide stronger proofs of identity, given thy are verified by a government
- *One-Time Password (OTP) device*: it generates one time passwords, using a seed embedded

7.9. Biometric authentication

- Based on the specific individual characteristics
- Technically complex and expensive
- Nature and requirements should be considered, being universal, distinct, permanent and collectable
- Should meet some criteria:
  - Performance and accuracy
  - Difficulty of circumventing
  - Acceptability by users

7.10. Access control

- Gaining the ability to communicate or interact with a system. In other words, the process of granting or denying specific requests, via specific services and mechanisms
- $\text{ACCESS CONTROL} = \text{AUTHENTICATION} + \text{AUTHORISATION}$
- Has different *inputs*
  - Who issued the request
  - What is required
  - What rules apply
- *System access* deals with moderating access to system objects via authentication (establishing user identity) and authorisation (defining user privileges)

7.11. Access control elements

- *Subject*
  - Entity capable of accessing objects
  - Typically considered accountable for their actions
  - Can be creators of resources, groups of users or every user possible to access

- *Object*
  - Resource which access is controlled and used to contain and/or receive information
- *Access rights*
  - The ways in which a subject can access an object

7.12. Access control policies

- Dictates what types of access are permitted
- Different categories exist:
  - *Discretionary access control (DAC)*
    - Based on requestor identity and on access rules, granting specific permissions
  - *Mandatory access control (MAC)*
    - Comparison between security labels (sensitiveness of resources) with security clearances (which resources to access)
    - Has to be mandatory, so not to enable user wishes
  - *Role-based access control (RBAC)*
    - Access control based on user roles
    - Role permissions can be inherited through an hierarchy
    - Can apply to a single or several individuals
  - *Attribute-based access control (ABAC)*
    - Access control based on attributes associated with and about subjects and objects, combining attributes under which an access takes place

7.13. Access control structures

- Access matrix = using access control lists (ACLs) or capability tickets
- Governed by a set of rules granting the subject access

7.14. Customer access

- Each customer needs to be uniquely approved and identified, both individual and in groups, responding to organization's business requirements
- Each one should be aware and trained
- Balance between customer satisfaction and meeting security requirements
- Subject to the same types of technical controls, defining access privileges and selecting an appropriate authentication procedure

8. M3.3 - Cybersecurity Operations and Management - System and Security

(On book - §11 - System Management)

8.1. Computer Security Incident Response Team (CSIRT)

- Responsible for rapidly detecting incidents
- Minimizing loss and destruction
- Mitigating the weaknesses that were exploited
- Restoring computing services
- Calculates the added value to invest in safety resources
- In small organizations can be the security team, in large ones they are two separate entities

8.2. Security Incidents

- Any action that threatens one or more of the classic security services
- Unauthorized access or modification
- Procedures to manage them
  - Sorting, detecting, identifying, documenting

8.3. Managing, detecting and responding to incidents

- Should be detected and reported
  - Manually (reports)
  - Automatically (with integrity/log tools)
- Triage
  - find the single point of contact for services and request additional information to categorize the incident and notify parts of the enterprise
- Documentation to respond to them
  - Detail/Describe/Identify categories, personnel, circumstances
  - Should immediately follow a response to the incidents
    - What
    - How
    - Details
    - Impact

  - Allows for reviewing the risk assessment and strengthening controls
- Once an incident is opened, has to go through a number of states until no further action is required and is considered closed

Security controls are in place throughout:

- Hardware
- Software
- Firmware

8.4. Malware and protection

- Program inserted into others compromising confidentiality, integrity, availability
- Many types and should be protected against them as much as possible
  - Clickless
  - Fileless
  - Adwares
  - Worms/Viruses, etc.
- Businesses are experiencing more and more
- Practical steps to take, avoiding attack and defending against different attack surfaces
- Protection software to use to protect against them, automating actions as much as possible, verifying all defenses and collecting results from all points of attack
  - Scanning
  - Monitoring
  - Identifying
  - Disinfecting
- Software has to be accompanied by other measures like whitelist, firewalls and virtualization

8.5. Intrusion Detection

- The sooner the intrusion is detected, the less damage can be done
- When an intrusion happens, confidentiality is lost on all levels and collecting information can help assessing risks and other means of security
- No exact distinction between an attack and normal use of resource: some overlap might happen
- Identification between legitimate and new user

- Approaches
  - *Misuse detection*: take the strange behaviour and consider it as normal attack, via usage of patterns and signatures. It cannot detect novel/unknown attacks
  - *Anomaly detection*: detect activities different from normal behavior and be able to detect previously unknown attacks, having a trade-off between false positives and false negatives
- Intrusion Detection System
  - Sensors: collecting data and inputs
  - Analyzers: receive data from sensors and support evidence
  - User interface: give user output
- Techniques
  - Host-based
    - Layer of security to detect intrusions, events and send alerts
    - Detect thresholds and profiles
  - Network-based
    - Monitor the traffic on the networks and see if packets match signatures
    - Can use sensors to gather data and feed information
    - It can see data inside the network but also outside of firewalls

8.6. Data Loss Prevention

- Information leakage can happen in an untrusted environment
- Monitor, and protect data in use and data at rest through deep content inspection
- Often includes unencrypted content
- Sensitive data should be precisely identified in an enterprise via different means
  - rule-based/fingerprinting/exact-partial file matching
- Data states
  - Data at rest = big risk with info stored throughout the enterprise
  - Data in motion = data transmitted over enterprise networks, subject to active/passive monitoring of information across enterprise networks
  - Data in use = part of media and saved physically somewhere, controlling the movement in end-user systems

9. M3.4 - Cybersecurity Operations and Management - Network and Communication

(On book: §12 - Network and Communications)

9.1. Network models

There are (as you know at this point I hope) two main network models, both with layered architecture and packet switching technology:

- ISO/OSI made up by 7 levels: application, presentation, session, transport, network, data link, physical
  - This is mainly used as reference
  - Each level creates data units
  - Lower levels encapsulate higher levels' data, adding headers and trailers (encapsulation)
- TCP/IP made up by 4 levels: application, transport, internet, network access
  - It's simpler than OSI and also widespread
  - Each level creates data units, also doing encapsulation
  - At destination, there is decapsulation

There are so many protocols one can see between the different levels of the two.

9.2. Network types, topologies and devices

- LAN/WLAN
  - Commonly used to describe a network of devices in a limited area
  - Most LAN networks use TCP/IP to communicate
- WAN
  - Used to describe a network that spans multiple geographic locations
- SOHO (Small-Office / Home-Office LAN) LAN
  - Usually built of one Ethernet switch, one router, and one wireless AP using Ethernet
  - Devices easy to set up and ready to go after unboxing
- Enterprise networks
  - Much larger in scale, with devices used enterprise-grade
  - Clients typically connect the access switches, connecting them all with aggregation switches

Understanding the network topology is important for an effective network traffic monitoring.

We can distinguish different devices:

- Hub (Layer 1)
  - Security issue: with hubs the traffic is forwarded to all ports, traffic is sniffable
  - It simply connects devices and broadcasts anything received
- Bridge (Layer 2)
  - Each incoming Ethernet frame is inspected for destination MAC address and forwards packets to other destinations to which it is intended
- Switch (Layer 2)
  - Inspect received traffic and make forwarding decisions
  - Build address table listening to incoming frames
  - It breaks up collision domain
- Router (Layer 3)
  - Routers packets from one network to another
  - IP routing allows to send packets to different hosts on the network, using routing tables to determine paths and gateways to communicate remotely
  - Breaks up both collision and broadcast domains

9.3. Network protocols

- IP Addressing (IPv4)
  - Dedicated to everything, from unicast to broadcast and multicast
- Address Resolution Protocol (ARP)
  - Used to find out hardware addresses of devices from IP addresses
  - All OSes maintain caches and works by sending requests and receiving messages and reply
- Transmission Control Protocol (TCP)
  - Connection-oriented, uses handshake, if data is lost is retransmitted
- User Datagram Protocol (UDP)
  - Uses much less resources than TCP, is connection-less
- Network Address Translation (NAT)
  - Process of changing the source and Network Fundamentals IP addresses and ports (16-bit number to identify apps/services), used to extend number of addresses of IPv4

- Access Control Lists (ACL)
  - Sets of rules used most commonly to filter network traffic, used with packet filtering in mind and applied to all network
- Dynamic Host Configuration Protocol (DHCP)
  - Used to assign various network parameters to a device, done by discovers, requests, offers and acknowledgements
- Domain Name System (DNS)
  - Network protocol used to translate hostnames into IP addresses, working with requests and replies
- Telnet & SECURE SHELL (SSH)
  - Both used to communicate remotely, using ports and addresses
  - SSH uses public key encryption

9.4. Network management system

Effective management requires a network management system that includes a comprehensive set of data and has different functions: fault/configuration/accounting/performance/security management.

A network management system:

- is a collection of tools for network monitoring and control
- consists of incremental hardware and software additions implemented among existing network components
- is designed to view the entire network as a unified architecture
- the term element refers to network devices

The principal components of a network management system:

- Each network node contains a collection of software devoted to the network management task
  - Network Management Entity (NME)
- At least one host in the network is designated as the network control host, or manager
- The network control host includes a collection of software called the network management application (NMA)
  - Used to allow an authorized user to manage the network
- Every other node in the network that is part of the network management system includes an NME, referred to as an agent

We can differentiate the configurations this way:

- In a traditional centralized network management scheme:
  - one host in the configuration has the role of a network management station

- In a decentralized network management scheme:
  - there can be multiple top-level management stations, which are referred to as management servers
  - for many of the agents, the management server delegates responsibility to an intermediate manager, which plays the role of manager

Network management has the following architecture:

- The element management layer provides an interface to the network devices
- The network management layer (NML) provides a level of abstraction that does not depend on the details of specific elements
- The service management layer is responsible for adding intelligence and automation to filtered events

9.5. Security management

Security management:

- is concerned with generating, distributing, and storing encryption keys
- is concerned with monitoring and controlling access
- is involved with the collection, storage, and examination of audit records and security logs
- provides facilities for protection of network resources and user information
- has the purpose to support the application of security policies, including:
  - creation, deletion and control of security services/mechanisms
  - distribution and reporting of security-related information and events

There are two main data types to consider:

- in motion
- stored

Security has three main objectives: *CIA*.

- Confidentiality: Only authorized individuals can access
- Integrity: Changes made to data are done only by authorized individuals/systems
- Availability: Applies to systems/data/network

Security analysis follows these ones:

- Asset = anything valuable to an organization
- Vulnerability = exploitable weakness
- Threat = potential danger
- Risk = potential that a threat happens

- Countermeasure = safeguard to mitigate risks

Network threats can be of all kinds: reconnaissance, social engineering, backdoors, privilege escalation, password attacks, etc.

Between different systems and networks, borders are slowly dissolving, and logical boundaries are established: end zones, data centers, the Internet itself.

We want to maintain control over data loss and contain it, considering data can be:

- in transit
- at rest
- encryption

9.6. Network perimeter security

Network administrators create zones and policies.

- By default no traffic is allowed between interfaces in different zones
  - Zones are trusted inside and outside the network (demilitarized)
- The Admin must create policies for traffic
  - They should be taken on the traffic itself
- The perimeter will filter traffic based on the range of IP addresses, enabling access control to some services and preventing network reconnaissance by providing a buffer or ACLs

There are also two main kinds of controls to apply:

- Network Intrusion Prevention System (NIPS)
  - Designed to inspect traffic and remove/redirect malicious traffic using sensors for traffic
  - It detects and mitigates malicious activity but uses more resources, add delays and possibly false positives/negatives
- Network Intrusion Detection System (NIDS)
  - Attempt to detect malicious network activities monitoring constantly traffic and sending copies of packets
  - Only a limited number of these is necessary, add no delay and have no negative impact if sensors go down, but can only detect malicious activities, while promiscuous modes cannot see original packets

9.7. IP security (IPSec)

The principal feature of IPSec is that it encrypts and/or authenticates all traffic at the IP level.

- All distributed applications are secured
- It provides three main facilities:
  - An authentication-only function referred to as Authentication Header (AH)
  - A combined authentication/encryption function called Encapsulating Security Payload (ESP)
  - A key exchange function

The last two are used for Tunnel mode:

- which provides protection for the entire IP packet
- and is used when one or both ends of a security association (SA) are a security gateway, such as a firewall or router that implements IPSec
- if a packet from host A to host B requires IPSec, the firewall performs IPSec processing and encapsulates the packet with an outer IP header

9.8. Virtual Private Network (VPN)

A VPN is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted and prevents eavesdropping.

For VPNs, both authentication and encryption are generally desired because it is important both to:

1. ensure that unauthorized users do not penetrate the virtual private network
2. ensure that eavesdroppers on the Internet cannot read messages sent over the VPN

There are different types of VPNs:

- Remote-access
- Site-to-site

They have several benefits:

- Data Tunnelling/Traffic Flow Confidentiality
- Data integrity
- Data Origin Authentication
- Anti-replay

Some examples of VPN protocols to quote: OpenVPN, Wireguard, IPSec.

An organization maintains LANs at different locations. Insecure IP traffic is conducted on each LAN. For traffic offsite, through some sort of private or public WAN, IPsec protocols are used.

- These kinds of devices typically encrypt and compress all traffic going into the network and decompress it, using also authentication
- These operations are transparent to workstations and servers on the LAN and secure transmission is also possible, using IPsec protocols and must implement high security

A logical means of implementing IPsec is in a firewall.

- If IPsec is implemented in a separate box behind the firewall, then VPN traffic passing through the firewall in both directions is encrypted
- In this case, the firewall is unable to perform its filtering function or other security functions
- IPsec can be implemented in the boundary router, outside the firewall

Some clues about security:

- Managed switch can provide a basic, yet effective security layer to combat a variety of network attacks, like DHCP snooping, ARP inspection, IP guard, port security and protection
- Today's router can be equipped with firewall modules, IDS, malware scanners, using ACLs, content filtering and firewalls

9.9. Firewall

The firewall is an important complement to host-based security services such as intrusion detection systems.

- Typically, a firewall is inserted between the premises network and the Internet to establish a controlled link
- The aim of this perimeter is to protect the premises network and to provide a single point where security and auditing are imposed
- A firewall provides an additional layer of defense

Firewall has the following goals:

- All traffic from inside to outside, and vice versa, must pass through the firewall
- Only authorized traffic, as defined by the local security policy, is allowed to pass
- The firewall itself is immune to penetration

Firewalls use four *techniques* to control access and enforce the site's security policy:

- Service control
  - Determines the types of Internet services that can be accessed — inbound/outbound
- Direction control
  - Determines the direction in which particular service requests are initiated and allowed

- User control
  - Controls access to a service according to which user is attempting to access it
- Behavior control
  - Controls how particular services are used

Capabilities within the scope of a firewall:

- A firewall defines a single choke point that keeps unauthorized users out of the protected network
- A firewall provides a location for monitoring security-related events
- A firewall is a convenient platform for several Internet functions that are not security related
- A firewall serves as a platform for implementing virtual private networks

Firewalls have limitations, including the following:

- A firewall cannot protect against attacks that bypass the firewall
- A firewall does not fully protect against internal threats
- An improperly secured wireless LAN can be accessed from outside the organization
- A laptop or portable storage device can be used and infected outside the corporate network and then attached and used internally

There are different methods applied by firewalls:

- Static packet filetring (Layer 3 - Layer 4)
- Application Layer gateway (Layer 3 - higher)
- Stateful packet filtering
- Application inspection (Layer 7)
- Transparent (Layer 2)
- Circuit-Level Gateway

The firewall should:

- Be resistant to attacks
- Be the only transit point
- Enforce the access control policy of the organisation
- Implement the network address translation (NAT)

A firewall acts as a packet filter. Depending on the type, a firewall can examine one or more protocol headers.

Next-generation firewalls, which are implemented in either software or hardware, are capable of detecting and blocking complicated attacks by enforcing security measures at the protocol, port, and application levels.

- The difference between a standard firewall and a next-generation firewall is that the latter performs more in-depth inspection and in smarter ways
- Common functionalities present in traditional firewalls are also present in next-generation firewalls
- Next-generation firewalls are more capable of detecting application-specific attacks

A firewall may be an internal or external firewall.

- An external firewall is placed at the edge of a local or enterprise network
- One or more internal firewalls protect the bulk of the enterprise network
- Between these two types of firewalls are one or more networked devices in a region referred to as a demilitarized zone
- Systems that are externally accessible but need some protections are usually located on DMZ networks
- An internal firewall provides two-way protection with respect to the DMZ

9.10. Remote maintenance

Maintenance activities conducted by individuals who are external to an information system's security perimeter.

- Principal security objective in this area is to prevent unauthorized access to critical systems

The U.S. Department of Homeland Security has compiled a list of requirements for remote maintenance of industrial control system. There are different requirements for an organization:

- authorization, monitoring and use of remote maintenance, maintaining records and terminating all sessions
- maintenance personnel, implementing cryptographic mechanisms, employing disconnect verifications

We conclude this run with Voice Over IP (VOIP) Networks:

- VoIP involves the transmission of speech across IP-based networks
- VoIP works by encoding voice information into a digital format
- VoIP has two main advantages over traditional telephony:
  - It's usually cheaper to operate than an equivalent telephone system with a PBX and conventional telephone network service
  - It readily integrates with other services

The following are some specific threats to the use of VoIP:

- Spam over Internet telephone (SPIT)
  - Undersired/pre-recorded bulk telephone calls to cause disturbance to victims
- Eavesdropping
  - Listening to the communication without consent
- Theft of service
  - Theft of goods and services without having lawful rights to do so
- Man-in-the-middle attack

10. M3.5 - Cybersecurity Operations and Management

(On book: §15 - Threat and Incident Management)

10.1. Technical vulnerability management

A technical vulnerability is:

- A hardware, firmware, communication, or software flaw that leaves an information processing system open to potential exploitation

Technical vulnerability management is designed to proactively mitigate or prevent the exploitation of technical vulnerabilities.

Five key steps involved in vulnerability management:

- Plan
- Discover
- Scan
- Log and report
- Remediate

10.2. Plan, discovery and scan for vulnerability

Effective management of technical vulnerabilities begins with planning. Key aspects of the planning process include the following:

1. Risk and process integration
   - Technical vulnerability review and vulnerability analysis must consider the relative risk impacts. These risks must also have a clear reporting
2. Integration with asset inventory
   - Asset identification is an integral part of risk assessment. An enterprise can prioritize high-risk systems where the impact of technical vulnerabilities can be greatest
3. Establishment of clear authority to review vulnerabilities
   - An enterprise needs to have in place a policy and approval from top management before performing vulnerability assessments.
   - There is also a need for policies and ethical guidelines for those who have access to data from vulnerability scans
4. System and application life cycle integration
   - The review of vulnerabilities must be integrated in system release and software development planning

The *discover* step involves monitoring sources of information about known vulnerabilities. Key sources of information are the following:

- NIST National Vulnerability Database (NVDB), Common Vulnerability Scoring System (CVSS), and Common Vulnerabilities and Exposures (CVE)
- Computer Emergency Response Team (CERT): team collects information about system vulnerabilities
- Packet storm
- Security focus
- Internet Storm Center

Enterprises need to regularly scan software, systems, and networks. The Center for Internet Security (CIS) recommends the following scanning regimen:

- Run automated vulnerability scanning tools against all systems on the network on a weekly basis
- Perform vulnerability scanning in authenticated mode
- Compare the results from back-to-back vulnerability scans to verify that those were addressed

There are some challenges involved in scanning that an enterprise needs to address:

- Scanning can cause disruptions, because it can impact performance, especially true with legacy systems
- Scanning can generate huge amounts of data and numerous false positives
- The vulnerability prioritization plan must be aligned with the IT infrastructure

10.3. Log, report, patch

When a vulnerability scan is completed, the organization should *log* the results. Discovered vulnerabilities should be ranked reflecting:

- The skill required to exploit the vulnerability
- The availability of the exploit to potential attackers
- The privilege gained upon successful exploitation
- The risk and impact of this vulnerability if exploitation is successful

The reporting process includes keeping track of the number and risk levels and event logs be correlated with information from vulnerability scans. Issues to consider related to performing *patch* management:

1. The relationship between timing, prioritization, and testing
2. Availability of resources involved in testing need to be taken into account
3. The impact of a patch on operational systems
4. Special care should be taken if multiple automated means of patching are used

10.4. Security logging

In the information security field, a distinction is commonly made between events and incidents:

- Security event
  - An occurrence considered by an organization to have potential security implications to a system or its environment. Security events identify suspicious or anomalous activity
- Security incident
  - An occurrence that actually or potentially puts in danger the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation

The objectives of security event logging are:

- To help identify threats that may lead to an information security incident
- Maintain the integrity of important security-related information
- Support forensic investigations

Log: a record of the events occurring within an organization's systems and networks.

- Effective logging enables an enterprise to review events, interactions, and changes that are relevant to security
- With a record of events such as anomalies, unauthorized access attempts, and excessive resource usage, an enterprise can perform an analysis to determine the cause

A wide variety of sources of security events can be logged, including the following:

- Server and workstation operating system logs
- Application logs (for example, web server, database server)
- Security tool logs (for example, antivirus, change detection, intrusion detection/ prevention system)
- Outbound proxy logs and end-user application logs
- Firewalls and other perimeter security devices for traffic between local user and remote database or server (referred to as north–south traffic)
- Security devices between data center storage elements that communicated across a network, which may involve virtual machines and software-based virtual security capabilities

Potential security related events that could be logged:

- Operating system logs
  - Successful user logon/logoff; failed user logon; service started/stopped
- Network device logs
  - Traffic allowed through firewall; traffic blocked by firewall; administrator access

- Web servers
  - Code seen as part of the URL; failed user authentication

10.5. Security Event Management (SEM)

Security event management (SEM) is the process of identifying events.

- The objective of SEM is to extract from a large volume of security events, which qualify as incidents. It is analyzed with security algorithms and statistical computations.

There are different SEM functions:

- The first phase of event management is the collection of event data
- As event data are generated, they are generally stored in logs local to the devices that generate them
- A number of steps need to be taken at this point:
  - Normalization
  - Filtering
  - Aggregation

The objective of the next steps is to analyze the data and generate alerts of security incidents:

- Pattern matching
- Scan detection
- Threshold detection
- Event correlation

10.6. Threat intelligence and analysis

Threat intelligence (cyber threat intelligence (CTI) or cyberintelligence) is the knowledge established as a result of analyzing information about potential or current attacks that threaten an organization.

The information is taken from a number of internal and external sources. There are different to consider:

- Adversarial: Individuals that seek to exploit
- Accidental: Erroneous actions
- Structural: Failures of equipment or software due to aging
- Environmental: Failures or critical infrastructures

The primary purpose of threat intelligence is to help organizations understand the risks:

- Threat intelligence includes in-depth information about specific threats
- Threat intelligence enables a security team to become aware of a threat well before the point of typical notification

- Threat intelligence reduces the time it takes to discover that an attack

Gathering threat intelligence requires having:

- external sources
  - subscribe to a regular feed of threat data
  - cyberintelligence vendors
  - many of the sources of vulnerability information
- internal sources
  - event logs from technical infrastructure
  - alerts from security systems such as firewalls
  - direct feeds from security event management utilities
  - dedicated teams

Threat analysis includes the task of describing the type of possible attacks and an organization should carry this analysis as a regular part of risk management. It involves the following:

- Identifying the vulnerabilities of the system
- Analyzing the likelihood of threats aimed at exploiting these vulnerabilities
- Assessing the consequences that would occur if each threat were to be successfully carried out
- Estimating the cost of each attack
- Costing out potential countermeasures
- Selecting the security mechanisms

An application or set of tools that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

- One of the most important incident management tools is a SIEM (Security Information and Event Management)
- Capabilities of a typical SIEM include data collection, aggregation, correlation

10.7. Incident management, response and handling

It is essential that an incident management policy is established for appropriate incident management. The policy should also cover the strategy for dealing with incidents:

- Identification of an incident and response
- Acquisition of volatile and static data
- Retention and analysis of data
- Remediation

- References to law enforcement
- Handling of forensic data
- Escalation of incidents
- Reporting of findings
- Definition of the learning process from incidents to upgrade ystems and processes

Many organizations react in an ad-hoc manner:

- Because of the potential cost of security incidents, it is cost-beneficial to develop a standing capability for quick discovery and response to such incidents
- This capability also serves with a view to improving the ability to prevent and respond to incidents

Making the right planning and implementation decisions is fundamental. Tasks involved in preparing for incident response include:

- Develop an organization-specific definition of the term incident so that the scope of the term is clear
- Create an incident response policy
- Develop incident response and reporting procedures
- Establish guidelines for communicating with external parties
- Define the services that will be provided by the Incident Response Team (IRT)
- Select an organizational structure and staffing model for incident response
- Staff and train the IRT
- Establish and maintain accurate notification mechanisms
- Develop written guidelines for prioritizing incidents
- Have a plan for the collection, formatting, organization, storage, and retention of incident data

Once an incident is detected, there needs to be the removing of threat and recovery from any damage. Typical actions include:

- Determine the magnitude of the impact
- Assess the severity
- Assess the urgency of the event

The analysis also needs to determine whether immediate action is needed to remove the vulnerability or to block the action that enabled the incident to occur.

Most incidents require some sort of *containment*:

- The objective is to prevent the spread of the effects of the incident
- Strategies for dealing with various types of incidents must be planned well in advance

- The nature of the strategy and the magnitude of resources devoted to containment depends on criteria developed ahead of time

During recovery, IT personnel restore systems to normal operation to the extent possible and, if applicable, harden systems to prevent similar incidents. Possible actions include the following:

- Restoring
- Rebuilding
- Replacing
- Installing
- Changing
- Locking network perimeter security

An incident handling checklist involves different operations:

- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident Activity

10.8. Emergency classification and best practices

Security incident emergencies must be handled with a greater sense of urgency than other security incidents. An emergency response may make an emergency fix to temporarily eliminate ongoing damage until a more permanent response is provided.

Classification scheme for security incidents suggested in ISO 27035:

- Emergency
- Critical
- Warning
- Information

Example of incident category and severity class includes both:

- Incident categories/Technical attacks/Malware
- Severity classes according to what was written here

The SOGP breaks down the best practices in the threat and incident management category into two areas. The areas and topics are as follows:

- Cybersecurity resilience
  - The objective of this area is to manage threats and vulnerabilities acting on threat intelligence, and protecting information against targeted cyber attacks

- Security incident management
  - The objective of this area is to develop a comprehensive and documented strategy for managing security incidents

10.9. Physical and Infrastructure Security

We must distinguish *three elements* of information system security:

- Logical security
  - Protects computer-based data from software-based and communication-based threats.
- Physical security
  - Also called infrastructure security, it must prevent any type of physical access or intrusion that can compromise logical security
- Premises security
  - Also known as corporate or facilities security. Protects the people and property within an entire area and is usually required by laws and regulations
  - It provides perimeter security, access control, smoke and fire detection

We can distinguish the following categories of threats:

- Physical threats
  - There are a number of ways in which such threats can be categorized. It is important to understand the spectrum of threats to information systems
  - These can be organized into:
    - Environmental
    - Technical
    - Human-caused
  - Technical threats
    - Electrical power is essential to run equipment
    - There can be power utility problems or electromagnetic interferences (EMI)

10.10. Prevention and mitigation

Standards including ISO 27002 “Code of practice for information security management” and NIST SP 800-53 “Recommended Security Controls for Federal Information Systems” include lists of controls relating to physical and environmental security.

- One prevention measure is the use of cloud computing
- Inappropriate temperature and humidity

- Fire and smoke
- Water
- Other threats

There should be *mitigation* measures:

- Critical equipment should be connected to an emergency power source
- To deal with electromagnetic interference (EMI) a combination of filters and shielding can be used

Most essential element of recovery is redundancy:

- Provides for recovery from loss of data
- For critical situations a remote hot-site that is ready to takeover operation instantly can be created

Physical equipment damage recovery:

- Depends on nature of damage and cleanup
- May need disaster recovery specialists

Physical security involves numerous detection and prevention devices, being effective if there is central control. Integrate automated physical and logical security functions is made via a wide range of vendors, being conform to standards and covering smart card protocols.

The *Personal Identification Verification (PIV)* front end defines the physical interface to a user who is requesting access to a facility.

- The PIV front end subsystem supports up to three factor authentication; the number of factors used depends on the level of security required
- The front end makes use of a smart card
- The other major component of the PIV system is the PIV card issuance and management subsystem. This subsystem includes the components responsible for identity proofing and registration
- The PIV system interacts with an access control subsystem, which includes components responsible for determining a particular PIV cardholder's access to a physical or logical resource

If the integration of physical and logical access control extends beyond a unified front end to an integration of system elements, a number of benefits grow:

- Employees gain a single, unified access control authentication device
- Auditing and forensic groups have a central repository for access control investigations
- Hardware unification can reduce the number of vendor purchase-and-support contract

10.11. Business continuity management

A couple of *definitions* first:

- Business: the operations and services performed by an organization in pursuit of its objectives, goals, or mission
- Business continuity: The capability of an organization to continue delivering products or services at acceptable predefined levels following a disruptive incident
- Business continuity management (BCM): A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats for building organizational resilience with the capability of an effective response
- Business continuity plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
- Business continuity program: An ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management

Enterprises engage business continuity planning to reduce the consequences of any disruptive event.

- Continuity of Operations (COOP) must be guaranteed
  - An effort in an organization to ensure that it can continue to perform the essential business functions and technological or attack-related emergencies
  - In essence, business continuity management is concerned with mitigating the effects of disasters
  - When a disaster occurs, the worst-case scenario is that it has the potential to bring some business processes or functions to a complete halt
  - A business continuity plan also calls for the implementation of capabilities and procedures rapidly

An organization's resilience is directly related to the effectiveness of its business continuity capability. This is based on the following components:

- Management
  - Continuity of management is critical to ensure continuity of essential functions. An organization should have a detailed contingency plan
- Staff
  - All staff should be trained accordingly
- ICT Systems
  - An organization should identify critical IT systems and have backup and rollover capabilities tested and in place

- Buildings and equipment
  - This component includes the buildings where essential functions are performed. Organizations should have separate backup locations available

A business continuity strategy involves considering the costs/benefits of any proposed strategy.

- There is a trade-off that management needs to consider
  - The cost of disruption derives from the business impact analysis and risk assessment
  - Against that is the cost of resources to implement a business continuity program
  - For example, for short recovery times, an organization may require a mirror data site that is always active and updated
  - Recovery time objective (RTO): the target time set for recovery after an incident

Resilience of the infrastructure improves the organization's ability to withstand and recover from disruptive events.

- Elements of business resilience (common strategies):
  - Recovery
  - Hardening
  - Redundancy
- Offensive measures that go beyond traditional approaches to resilience:
  - Accessibility
  - Diversification
  - Automation

11. M4.1 - Security Assessment and use cases

11.1. Communication Systems in Transportation

Communication systems are widely used in transportation and play a significant role in operating these critical infrastructures.

- Technological advances in the telecommunications industry have brought significant advantages in management and performance

Railway systems have evolved overtime:

- Fully connected systems and interoperable, many times driverless
- Safety through electromechanical devices

One of the sectors that have greatly enhanced this technological evolution is the railway industry where signaling systems are fully computerized.

- Such interconnected systems have a greater surface area exposed to cyber-attacks

11.2. Cybersecurity for the Rail Industry

There is a lot of attention on cybersecurity issues for critical infrastructure.

- National governments have defined specific laws to control security requirements for these systems
- New rail industry systems are fully connected to the railway network, and this makes the railway market vulnerable to hackers
- Transportation companies must deal with cyber events, potentially damaging the systems and compromise their safety

11.3. Critical Infrastructures

Critical infrastructures are those considered essential to maintaining the vital functions of society.

- In this category there are the electrical grid, the transportation network
- To reduce the vulnerability of critical infrastructure, EU has launched the European programme for critical infrastructure protection (EPCIP)
- E.g. Italy has defined by law the national cybersecurity perimeter (first law to define which assets which need to be protected), giving precise cybersec obligations for public and private companies

Critical rail infrastructure refers to railway systems that provide high safety and reliability of public transportation services.

- Many systems are designed to make everything work together in an organized way
- As transportation railways prepare to digitize their processes, rail companies look for ways to protect their systems from cyber-attacks

- Rail services are critical infrastructure and should be protected against cyber attacks to ensure their safety and reliability

If critical rail infrastructure is significantly disrupted or damaged, rail operations could be affected, potentially leading to fatalities.

- The cyber risk to the railways is diverse, including compromised infrastructure, cyberattacks on stations, equipment, and potential damage to the rail network
- E.g., service unavailable, safety critical system unavailable, railway incident safety issues

We can make several *security remarks*:

- A rail system offers a broad attack surface
- Attacks can propagate even to the subsystems not directly connected to the computer network
- Guaranteeing the security of such complex systems is a challenging task
- As rail systems go through the modernization process, we need people who understand how cybersecurity must be integrated into the rail sector

Railway transportation is a complex system that involves and interlinks many different engineering fields (*railway as a system*). It's useful here to use metalanguages/schemas to represent situations (e.g., SysML).

- The rail transportation system transfers passengers and goods on wheeled vehicles running on rails located on tracks. It is a complex system consisting of the railway infrastructure, vehicles (rolling stock), and operation
- The operation and maintenance data digitalization expanded the railway systems' attack surface
- The security assessment must consider and manage various cyber and physical, internal, and external threats

11.4. Use case: railway signalling systems

- The wayside systems comprise electrification, signalling, and telecommunications systems and level crossings
- The railway signalling is a system used to ensure safe movements
- Modern railway signalling systems, e.g., the ERTMS/ETCS (European Rail Traffic Management System/European Train Control System) and communications-based train control (CBTC), implement the automatic train protection (ATP) function.
  - safe train separation and protection against excessive speed based on continuous wireless communication
- The main subsystems within the railway systems are the *interlocking (IXL)* and *automatic train control (ATC)*:
  - The IXL is responsible for granting a train exclusive access to a sequence of railway track elements named route

  - The ATC, instead, controls and protects the train movement by regulating the distance of trains and verifying that they comply with the speed limit

Given the many interconnections and the ways of signaling, interconnected computers control all these systems, expanding the attack surface towards the railway systems.

11.5. Safety and security standards

Railways systems are considered safety-critical applications, i.e., systems whose failure can result in human disaster of various kinds.

- Safety-critical applications are focused on ensuring safety, i.e., avoiding physical harm to people or property, and not on their (cyber)security
- The safety standards used as references for railway infrastructure design do not consider cybersecurity

Safety standards:

- define the safety integrity levels (SILs) for safety-related functions, depending on the maximum tolerable hazard rate
- to achieve a given SIL, specific design rules and test procedures must be implemented

Cybersecurity standards:

- Until recently, railway system designers and operators addressed cybersecurity by following ISA/IEC 62443 or more general norms
- Other generally applicable norms and frameworks include the Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 27001, and NIST Cybersecurity Framework (CSF)
- ENISA mapped the security requirements and measures for the operators of essential services (OES), including those of the rail transportation sector, to some of the standards and framework
- It is particularly complicated to achieve the safety certification of components that include security modules which are usually not designed according to safety standards
- The brand new technical specification CENELEC TS 50701, “Railway Applications – Cybersecurity”, will create a new standard that includes safety and security areas
  - This future standard is based on ISA/IEC 62443

Historically, since 2003, many cybersec incidents have involved railway sectors.

- The major confirmed cybersecurity incidents that have affected the transportation operations or have endangered or had the potential to compromise transportation safety
- The most recent attacks involving ransomware have not impacted railway safety systems but significantly disturbed the transportation services

Modern industrial control systems (ICSs) use ICT to control electromechanical systems and automate industrial processes and operations in various applications.

- Main components of an ICS might include programmable logic controllers (PLCs), data communication systems (DCSs), and supervisory control and data acquisition (SCADA)
- The increasing number of security vulnerabilities in industrial systems want to create more advanced systems
- The ICT systems and ICSs have a different emphasis on confidentiality, integrity, and availability (CIA)

11.6. Radio-based Data Communication System (DCS)

At present, the ERTMS and CBTC are the prevailing radio-based control systems:

- CBTC systems use radio frequency DCSs for train control and traffic management using V2I/V2V (vehicle-to-vehicle/infrastructure)
  - It has increased its popularity with rail operators due to its ability to maximize the capacity of the railway
- ERTMS is a European standard that enhances the interoperability of the signaling equipment on mainline railways
  - It has three operating levels, and it implements a standard solution jointly created by different manufacturers at each level

A CTBC and an ETCS system might also include an interlocking (IXL) to monitor the status of the objects in the railway yard.

- Railway IXL systems are those systems that are responsible for granting a train exclusive access to a route
- Cyber-criminals can attack these systems through the same interfaces the IXL uses to monitor and manipulate objects

Greater reliance on wireless technology increases complexity during development and exposes wireless systems to security threats.

- These affect the DCS directly through the wired wayside network and indirectly via vehicles' onboard network and wireless V2I and V2V communications

11.7. Cybersecurity Assessment for Railways

The railway companies that manage the signalling systems must ensure high safety and security standards.

- The rail transportation sector can no longer treat cybersecurity and physical protection separately
- Risk management methodologies and security standards usually incorporate controls of both natures, cyber and physical
- ENISA identified ISO/IEC 27001 and IEC 62443 as the most commonly applicable security standards for railways

Even when doing network cybersecurity assessment:

- Any assessment process includes information gathering to have a detailed picture of the system under investigation
- It's useful to map then all the information learned on each network component and interface during the architecture modeling
- Then, it's important to validate assumptions, policies, and security requirements during risk scenarios analysis
- The core stage is threat examination, in which we try to identify any event that potentially might affect the network under test
- The threat analysis stage comprises three steps:
  - After identifying threats in the first step
  - finding vulnerabilities in software, protocols, and architecture is preliminary for determining the associated risks in the last step
  - each vulnerability has associated risk to that, deriving probabilities of threat events and their impact

11.8. Cyber ranges as tools

Cyber ranges (or threatres) have attracted considerable attention in the cybersecurity ecosystem due to their ability to mimic realistic situations.

- They can contain several interconnected components (physical or virtual - with these ones understanding how the original system works in more detail)
- Scenarios represent particular settings of a theatre, specifying the active elements, applicable rules
- Simulation environment mimes the essential characteristics of the physical system but neglects low-level implementation details
- Emulation environment reproduces most physical system peculiarities

The workflow that uses a cyber range to evaluate network security during the reconnaissance can consider the following:

- Emulate the network (or a part of it) using the actual configurations
- Research the vulnerabilities
- Enumerate the vulnerabilities

12. M4.2 - Security Assessment and use cases

12.1. Cyber risk management for railway sector

In EU, significant directives were implemented:

- NIS (2016): In the EU, the Network and Information Systems (NIS) Directive was a significant step in improving the security of computer networks
- NIS2 (2020): Proposed modernization of the NIS Directive aiming at increasing resilience to cyber threats for essential service operators in a global Internet scenario

In general:

- Addressing cyber risks in the railway sector can raise entirely new challenges for railway companies who often lack the internal expertise
- European railway companies and infrastructure managers use a combination of good practices, approaches, and standards to perform cyber risk management for their organisations

Existing risk management approaches are multiple and varying across the railway companies:

- For the risk management of railway IT systems, the most cited approaches were the requirements of NIS Directive, NIST framework and the ISO 2700s

It is crucial to make an *identification on railway assets and services* that need to be protected.

- Identify who is responsible for the infrastructure, assets and services
- The identification of all interdependencies of the systems can be a real challenge
- OT (Operative Technology) and IT have different levels of maturity in terms of cybersecurity

TS50701 breaks down the list of asset and service in 5 areas:

- Service
- Device
- People
- Physical equipment
- Data

12.2. Cyber threat, safety and security for railway sector

In railway sector compromised OT systems can affect passengers' safety, cause a train accident, or interrupt traffic. OT systems are usually more vulnerable than IT system.

- OT systems are now more and more interconnected with classic IT systems, which makes them even more vulnerable and exposed to cyber threats

A possible *architecture* that can combine safety and security might use a security shell protects the safety function.

- This leaves the designer free to apply any relevant standard to design each internal component but imposes that all communications
- This architecture is implicitly resistant, for instance, to a DoS attack, given only functioning components can be compromised
- The designers only have to worry about maintaining the (reciprocal) compatibility between the I1 and I2 interfaces that connect the two controllers

12.3. Cyber risk scenarios

Cyber risk scenarios can assist railway stakeholders when performing a risk analysis.

- *Scenario 1*: Compromising a signalling system or automatic train control system, leading to a train accident
  - Attacker gathers physical information, builds a device/software, takes control of junctions/trains and false signaling information is injected
  - This scenario requires high motivation of the attacker and in-depth knowledge of railway systems and networks. It is considered a low likelihood scenario
- *Scenario 2*: Sabotage of the traffic supervising systems, leading to train traffic stop
  - An ICS malware propagates into OT systems, the attacker obtains remote access to traffic supervision systems and disrupts them, resulting in emergency stop
  - This scenario is a targeted attack using a specific Industrial Control System (ICS) malware to disrupt the trafficsupervising systems, thus leading to an urgent stop of train traffic
- *Scenario 3*: Ransomware attack, leading to a disruption of activity
  - An attacker infitrates via credential theft, identifies vulnerable systems, takes control of IS components, ransomware is deployed and systems become unusable, unless there is a ransom exchange
  - Ransomware attacks are considered the top threat scenario and are targeting the transport sector
- *Scenario 4*: Theft of clients' personal data from the booking management system
  - An attacker steals the credentials of booking system admins, obtains privileged access and downloads clients' personal data, proceeding to leak it
  - This scenario is a targeted attack, where the attacker steals the identity of an administrator and is therefore able to connect to a cloud-based booking management system and exfiltrate customer data
- *Scenario 5*: Leak of sensitive data due to unsecure, exposed database
  - A public/unprotected database is found, its content is exfiltrated and social engineering attacks are performed

  - This scenario is also related to data leakage, but the starting point here is a supplier with a low cybersecurity level. The attacker uses this third-party weakness to exfiltrate sensitive data

- *Scenario 6*: Distributed Denial of Service (DDoS) attack, blocking travellers from buying tickets
  - An attacker creates a botnet to launch DDoS, targeted devices are unable to handle incoming results and passengers are unable to book tickets
  - This scenario is a targeted attack, where the prerequisite for the attacker is to have created a botnet network. The attacker can then use the botnet to flood devices with requests and make them unavailable
- *Scenario 7*: Disastrous event destroying the datacentre facility, leading to disruption of IT services
  - A physical event occurs, affecrs the datacenter with permanent damage and IT-related activies are disrupted
  - This scenario is the consequence of a disastrous event which leads to disruption of activity, for parts or all of them. Depending on the redundancy strategy of the company, disruption can last more or less

12.4. CENELEC TS 50701

CENELEC (Comité européen de normalisation en électronique et en électrotechnique) is one of the three European Standardization Organizations (together with CEN and ETSI) recognized by the European Union and the European Free Trade Association (EFTA) to develop and define standards within Europe.

- The continued lowering of the cost of modern solutions is leading to industrial automation and control systems (IACS) with more adaptable architectures
- The cybersecurity of a rail system is effective when no hardware/software can be modified or corrupted

As its reference architecture:

- assets shall be divided in groups corresponding to physical areas and functional criticality level

For a railway application to operate in a safe and fully functional manner, its *essential functions* need to be protected.

- these are defined as functions or capabilities which are required to maintain the safety and availability of the system
- for railway applications, a loss of protection, of control or of view would be considered as a loss of essential functions. Since attacks on the system can lead to losses, security countermeasures need to be implemented
- the availability of railway applications needs to be ensured when considering security function, guaranteeing continuous security operation

"Defence in depth" is one of the guiding principles to provide appropriate security for the essential functions of all systems.

- when applying this one, integrity and availability are to be considered as highest priority
- it reduces the susceptibility of systems to attacks by eliminating single points of failure
- layered security mechanisms increase the security of the system as a whole

There is a whole methodology based on Zoning and Conduits:

- The TS 50701 describes a seven-step process (each called "Zone and Conduit Requirements" (ZCR)) to improve the security posture of railway systems
- The regulation demands one to identify the so-called System under Consideration (SuC), which will be further divided into zones according to the context
- Different zones communicate with each other through the use of conduits that define how communications can occur. At this stage, we perform an initial risk evaluation in which the threat landscape and the corporate risk matrix are evaluated
- The initial zoning is further refined to individuate the most critical parts of a SuC and to draw the communications avenues (the conduits) between different zones or SuC

The specifications detail the following:

- ZCR 1: Identify assets and basic process demands
- ZCR 2: Identify global corporate risks through an initial risk assessment
- ZCR 3: Perform zoning
- ZCR 4: Perform high-level risk assessment with the high-level zone model and the designated SL for exceeding risk
- ZCR 5: Check threats
- ZCR 6: Document all information and results
- ZCR 7: Get approval from all stakeholders

In principle there are only three different conduits necessary to connect zones:

- Conduit implementing a transparent gateway
- Filtering conduit as firewall appliance
- Unidirectional conduit as data diode

Some final remarks:

- A rail system offers a broad attack surface
- Attacks can propagate even to the subsystems not directly connected to the computer network
- Guaranteeing the security of such complex systems is a challenging task

- Human factor: as rail systems go through the modernization process, we need people who understand how cybersecurity must be integrated
- The new standard for cybersecurity (TS 50701) of rail systems will greatly improve security management in this critical infrastructure

13. M6.1 - Certification and Frameworks for Organizations and management systems

(This here marks the Second Part of the Course, made by professor Antonio Belli)

13.1. Information Security Management System (ISMS): Definition and Usefulness

Firstly, define *information security*:

- Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

Then, define an *Information security management system (ISMS)*:

- Management system designed to protect the information assets of the Organization at the required level of security, through the definition and maintenance of a series of policies, procedures, control / governance tools and best practices
- ISO/IEC 27001:2022 defines a set of rules to run an ISMS
- The part of the management system that follows a riskbased approach with the aim of establishing, implementing, making effective, monitoring, reviewing, maintaining and improving the security of information within the context of the Organization (ISO 27001, Section 1)

The certification of the management system derives from an audit carried out by an independent third party (Certification Body).

- Certification is voluntary, having a scheme for improving information security
- In some cases, it is mandatory, such as to participate in some tenders or to provide specific services to certain categories of customers

ISMS is useful for:

- Protect information assets
- Give a competitive advantage (e.g. tenders, when certified)
- Enhance profitability
- Improve legal compliance (e.g. privacy law)
- Improve the image of the company
- Enhance security
- Manage the risk

And also, some other benefits:

- It gives an excellent list of security controls to apply
- It gives a tangible demonstration of having adopted adequate measures to everybody (customers/ users/auditors, etc.)

- Lays the foundation for the definition of an Information Security policy
- Risk defined controls means they're not oversized, but not underdimensioned as well
- Takes climate change into consideration, both for internal and external (stakeholders) needs

Knowing the context, the scope and the criteria of risk management is the premise for risk assessment.

- This is true for both ISO / IEC 27001 and ISO 31000
- It's important to acknowledge what is risky, for who/why and what is the reach

Risk assessment and treatment lead to the achievement of information security goals. ISO 31000s allow for risk identification/analysis/evaluation/treatment and definition of information security goals.

Specifically, consider the alignment with ISO 31000 (Risk Management):

- a) ISO 27001 risk assessment principles are aligned with the indications provided in ISO 31000
- b) There are benefits for organizations operating with integrated management systems as the risk assessment methodology itself can be used in various standards
- c) Identification of internal and external "problems"

13.2. Assets, threats, risk analysis and risk treatment

The asset is a factor to which the organization assigns a value and which needs to be protected. Assets can be:

- Information, Paper documents, Computer, Media, People, Know how, Other valuable things

The Information can be classified (e.g.) as:

- Top Secret
- Secret
- Confidential
- Public (no restriction)
- Other schemes

Information must be classified in relation to its value, mandatory requirements and harm in the event of unauthorized disclosure or modification.

Once again, some definitions, following here the specified ISO standards:

- Vulnerability is a *weakness* in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
- Threat is any *circumstance* or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access

- Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
  - (i) the adverse impacts that would arise if the circumstance or event occurs; and
  - (ii) the likelihood of occurrence

The procedures relating to the identification and analysis of *risks* must consider:

- Ordinary and non-ordinary activities
- The activities carried out by all staff who have access to workplaces, including suppliers and visitors
- The equipment present in the workplace, whether provided by the organization itself or by other parties
- This analysis must be carried out (in the input and output phase) with the owners of the risks

Risk analysis also defines:

- Normal and planned operations
- Operations carried out outside the normal range, like start-up, shutdown and maintenance
- Accidental or emergency situations

What risks are tolerable?

- Legal or other requirements
- Needs of stakeholders
- Company policy
- Can they go beyond defined tolerance thresholds?

We define risk treatment as "a process and (approved) risk treatment plan should be defined that takes into account the results of the risk assessment, determining all the controls necessary to treat the risk"

13.3. ISO/IEC 27001 and ISO/IEC 27002: Overview

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 167 national standards bodies,improving the management of business processes (I know you know, but just to give you context). Here, we talk of course about:

- ISO/IEC 27001:2022 is the standard that provides the rules for the operation of the information security management system (ISMS)
  - It contains an annex "A", which is a list of security controls that an Organization can adopt. This standard is certifiable
- ISO/IEC 27002:2022 is a standard that provides guidelines for implementing those controls (from Annex "A" of the ISO/IEC 27001)
  - This standard is not certifiable itself (but auditing an ISMS follows these guidelines)

Here we define the key concepts:

- *Context*
  - This is given by factors that can be internal and external to the Organization, which affect its purposes and may affect the relative ability to achieve the objectives set for the Information Security Management System
- *Stakeholders*
  - Employees
  - Shareholders
  - Customers
  - Society (citizens)
  - Others (Third parties who have interest in the success of the ISMS)
- *Documented information*
  - Whenever we read in the text of an ISO standard that information must be available as a *set* of documented information or *stored* asdocumented information (and similar)
  - We refer to the fact that the Organization must guarantee written evidence, in its processes / policies, or in any case in its document management systems, of such information
  - The "Deming" Cycle (or "PDCA")
    - Planning (Plan) define the objectives that a management system must achieve
    - Insurance (Do) trust that the requirements will always be met and then pursue them
    - Check (Check) identify the performances which are different from those expected
    - Continuous Improvement (Act) has the purpose to increase performance
  - High Level Structure (HLS) common to Management Systems is the following:
    1. Purpose and field of application
    2. Normative requirements
    3. Terms and definitions
    4. Context of the Organization
    5. Leadership
    6. Planning
    7. Support
    8. Operating activities
    9. Performance evaluation

10. Improvement

About the structure of ISO/IEC 27001:2022:

- Introduction
  - 1 - Scope
  - 2 - Normative references
  - 3 - Terms and definitions
  - 4 - Context of the organization
    - The scope must be available as documented information
    - These chapters are mostly reading indications and specifications about (e.g.) variations with respect to the previous version of the standard
    - Specifically:
      - 4.1 - Understand 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
        - E.g. the country where the organization is located, the laws it must take into account …
  - 5 - Leadership
    - Obtain the commitment of the Management (budget, definition of roles and responsibilities, promote improvement …)
      - The information security policy must be available as documented information
      - Specifically:
        - 5.1 - Leadership and commitment
        - 5.2 - Policy
        - 5.3 - Roles, responsibilities and organizational powers
  - 6 - Planning
    - The main “premise” of risk analysis
    - Based on the context, the Organization must establish how to identify risks and opportunities
    - Guarantee the Result, establishing evaluation criteria and ensuring «rigor»
    - Information on the risk assessment process, ‘SoA’, Risk Treatment Plan and information security objectives must be available as documented information

    - SOA = Statement of Applicability: it identifies the objectives and controls applicable to the needs of the organization. This is mentioned in the certificate
  - Specifically:
    - 6.1 - Actions to address risks and opportunities
    - 6.2 - Information security goals and planning to achieve them
- 7 - Support
  - The Organization determines and provides competent, knowledgeable resources, establishing the rules for communicating and documenting information
  - Specifically:
    - 7.1 - Resources
    - 7.2 - Competence
    - 7.3 - Awareness
    - 7.4 - Communication
    - 7.5 - Documented Information
- 8 - Operation
  - The information certifying the operation of the processes, the results of the risk analysis and the risk treatment plan must be documented and stored
  - Specifically:
    - 8.1 - Planning and operational control
    - 8.2 - Information security risk assessment
    - 8.3 - Treatment of information security risks
- 9 - Performance Evaluation
  - Evaluate the performance and effectiveness of the ISMS
  - The Organization must keep appropriate documented information as evidence of monitoring and measurement results, as well as the results of the management review
  - Documented information must be kept as evidence of the audit program and internal audit results
  - Specifically:
    - 9.1 - Monitoring, measurement, analysis and evaluation
    - 9.2 - Internal audit
    - 9.3 - Management Review

- 10 - Improvement
  - The Organization must react to the non-compliance: check it and correct it. Face the consequences and make sure it won't happen again.
  - It must also understand the causes and document the nature and results of corrective actions as documented information.
  - Specifically:
    - 10.1 - Continual improvement
    - 10.2 - Nonconformity and corrective action

13.4. ISO/IEC 27001 and ISO/IEC 27002: Security controls and implementations

These are 93 countermeasures that can mitigate the information security risk.

- They are based on best practices recognized internationally as methods to reduce risk
- Those proposed by ISO27001 are optional, but necessary to justify both the adoption and the exclusion of controls

There is a relationship between ISO/IEC 27001:2022 annex "A" and ISO 27002:2022:

- The Annex "A" of the ISO/IEC 27001:2022 standard contains a list of controls that the ISO/IEC 27002:2022 describes in detail, one by one, proposing a guidance for implementing each control within the context of the Organization.
- They're very useful to guide Organizations writing their information security policies
- Each control reduces risk in a specific area. There are 4 areas of controls (themes):
  - 5. Organizational controls
  - 6. People controls
  - 7. Physical controls
  - 8. Technological controls

ISO 27002 also defines attributes as a new tool for sorting, filtering and showing controls. An Organization can create their own attributes.

- They are based on tags "#" to make them searchable by different criteria:
  - Control type (preventive, detective, corrective)
  - Information security properties (Confidentiality, Integrity, Availability)
  - Cybersecurity framework concept (Identify, Protect, Detect, Respond and Recover) from ISO/IEC 27110
  - Operational capabilities (area of the control, useful for the operative staff)

- Information security domains (4 categories / sets of information security areas)

Organizational controls are measures based on general policy choices that can be strategical in terms of operation and efficiency for information security.

- We have, for example, indications on the existence of a security policy, the separation of roles, responsibility management, assets, … for including the right amount ofinteraction with external context
- Some examples of organization controls:
  - List of controls: 5.1 Policies for information security 5.2 Information security roles and responsibilities 5.3 Segregation of duties 5.4 Management responsibilities 5.5 Contact with authorities 5.6 Contact with special interest groups 5.7 Threat intelligence …

People controls have the objective to reduce the risk associated with the area of human resources. We think about hiring staff, the risks of careless screening, NDAs, remote work, what can happen when the employment terminates.

- Some examples of people controls:
  - List of controls: 6.1 Screening 6.2 Terms and conditions of employment 6.3 Information security awareness, education and training 6.4 Disciplinary process 6.5 Responsibilities after termination or change of employment …

Physical controls are controls related to the physical world, according to ISO / IEC 27002: 2022, help organizations to be aware of their spaces, which must be protected against intrusions

- But also with respect to simple disorder, as well as with respect to the risk of accidents (fires, floods, …) safe disposal of equipment and more
- Some examples of physical controls:
  - List of controls: 7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 Physical security monitoring …

Technological controls offer specific countermeasures for systems and applications.

- The Organization that applies them can have a reduction in the risk associated with malware, or for example rely on backups made according to the best practices for having adequate redundancy of information
- But also know how to manage changes, patching and logging of events
- Some examples of technological controls:
  - List of controls: 8.1 User endpoint devices 8.2 Privileged access rights 8.3 Information access restriction 8.4 Access to source code 8.5 Secure authentication

14. M6.2 - Cloud security

14.1. Cloud computing

Cloud computing:

- is the data processing delivered as a service over a network, typically the Internet
- provides shared computer resources on demand
- can be also defined as a “paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources"

14.2. Benefits of cloud computing

The Cloud model introduces significant advantages over traditional hardware solutions, which allow you to:

- carry out continuous updates of the infrastructure and applications
- use the applications from any device in any place via internet access
- have greater flexibility in trying new services or making changes, with minimal costs;
- reduce the risks associated with the management of the security (physical and logical) of IT infrastructures
- have important savings in the use of software, as it is possible to pay for resources as services on a consumption-based basis (“pay per use”), avoiding initial investments in the infrastructure
- reduce the overall costs associated with the location of the data centers (electricity consumption rents, non-ICT personnel)

14.3. Key terms of cloud computing

- Cloud service provider
  - The party which makes cloud services available
  - Public cloud service provider is the party which makes cloud services available according to the public cloud mode
- Cloud service customer (or consumer)
  - A person or organization that is a customer of a cloud
  - A cloud customer may itself be a cloud and that clouds may offer services to one another

14.4. Key terms of cloud services

There are mainly three different types of cloud services that a CSP can provide, which entail a different division of responsibilities among the actors (following definitions from NIST SP 800-145):

- IaaS (Infrastructure as a Service)
  - Provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications
  - The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
- PaaS (Platform as a Service)
  - Deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
  - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment
- SaaS (Software as a Service)
  - Use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface
  - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings

Consumers and Cloud Service Providers (CSPs) security responsibilities are dependent on the cloud service model procured. Understanding this shared responsibility model is fundamental to ensuring the appropriate allocation of security compliance responsibilities (i.e., impact level, security controls).

- Responsibility moves from customer to provider
- In the SaaS, Customer is usually only responsible for information (data)
- Specific standards, frameworks and certifications can represent a valid tool, even for cloud services

14.5. ISO Standards on cloud computing

- ISO / IEC 27002:2022 - Information security, cybersecurity and privacy protection
  - Control 5.23, "Information security for use of cloud services"
  - There are several controls that impact cloud services. The one described by ISO/IEC 27002:2022 in particular, states that the processes for acquiring, using, managing and terminating cloud services must be established in accordance with the organization's information security requirements

The following two standards define a series of additional controls for information security, for management systems based on the ISO/IEC 27001:2013 standard (which has been recently re-edited to adapt to the new ISO/IEC 27002:2022). They only "extend" the ISMS, expanding the control area of the management system already existing with cloud services specific controls.

- ISO/IEC 27017:2015 - Security Controls for Cloud Services
  - Gives guidelines for information security controls applicable to the provision and use of cloud services by providing:
    - additional implementation guidance for relevant controls specified in ISO/IEC 27002
    - additional controls with implementation guidance that specifically relate to cloud services (which do not follow the scheme of annex "A" of ISO 27001)
  - This Recommendation / International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers
  - Some important areas of controls:
    - Shared responsibilities and roles in the cloud computing environment
    - Removal and return of cloud services customer assets upon termination of contract
    - Protection and separation of a customer's virtual environment from that of other customers
    - Virtual machine hardening requirements to meet business needs
    - Procedures for administrative operations of a cloud computing environment
    - Monitoring of relevant customer activity in a cloud computing environment
    - Alignment of security management for virtual and physical networks
- ISO/IEC 27018:2019 - Data protection standards for cloud services
  - Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment
  - In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services
  - It is an international Code of Practice for privacy in the cloud
  - Substantially aligned with European Union data protection laws, it provides specific guidelines for cloud service providers (CSPs) processing personal information (PII) for risk assessment and implementation of state-of-the-art controls to protect such information

- Some important areas of control:
  - Management of data breach involving PII;
  - Agreements on the processing of personal data;
  - definition of a contact point for the customer;
  - legitimate use of personal data (e.g. commercial purposes must be declared and accepted);
  - Localization of PII (where data centers are located);
  - secure deletion and return of customer personal data;

These are the most common information security risks:

- multi-tenancy: creating multiple virtual environments logically distinct present on the same physical component, allowing multiple customers (tenants) to work independently, increases the risk of attacks that can compromise this separation and therefore the *confidentiality* of the data
- the increasingly international location of computational and storage systems makes the place of processing and storage of data often unidentifiable, giving the sensation of *losing control*
  - the non-homogeneity of laws and regulations between states in which the Datacenters of Cloud suppliers are present, in particular outside the EU, can cause problems of non-compliance and / or sanctions
- the ways in which Cloud services and immaturity is scarce adoption of tools, standards and interoperable data formats often make it difficult to *migrate* from a provider to another, as well as the simple *recovery* of their data

14.6. AGID (The Agency for Digital Italy)

- AGID Marketplace - How to join the Cloud model of the PA (Public Administrations)
  - The Department for Digital Transformation, in collaboration with the Agency for Digital Italy (AgID), has developed a cloud enabling program that defines the set of activities and resources useful to administrations for migration of digital services and infrastructures to the PA Cloud
  - The Cloud Marketplace
    - Since 1 April 2019, Public Administrations can only acquire IaaS, PaaS and SaaS services qualified by AgID and published in the Cloud Marketplace
    - To fully exploit the benefits of the cloud, public administrations should first evaluate the presence of SaaS services in the Cloud Marketplace that meet their needs and, only second, consider PaaS and finally laas solutions

14.7. Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) is a world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

- The CSA "SECURITY GUIDANCE For Critical Areas of Focus In Cloud Computing" is an Official Study Guide for the CSSK certificate (cloud security knowledge)

- The Cloud Control Matrix (CCM) is a powerful tool for improving cloud security

CSA Cloud security process wants to identify necessary security and compliance requirements, and any existing controls.

- Select your cloud provider, service, and deployment models
- Define the architecture
- Assess the security controls
- Identify control gaps
- Design and implement controls to fill the gaps
- Manage changes over time

14.8. CSA – Cloud Control Matrix / CAIQ - Consensus Assessments Initiative Questionnaire

CSA is made up of 197 controls over 17 domains, each control describing a domain, a title, an ID and a specification.

- It defines typical control applicability and ownership, describinmg responsibility models and specified roles
- Domains can be whatever thing: audit/assurance, security, governance, identity, etc.
- Each control has guidelines related to it

Each control from the previous matrix has a question associated (CAIQ) to that - from control to question.

14.9. STAR Certification

Security Trust Assurance and Risk (STAR) encompasses key principles of transparency, rigorous auditing, and harmonization of standards.

- Level 1: Self-Assessment
  - At level one organizations can submit one or both of the security and privacy self-assessments. For the security assessment, organizations use the Cloud Controls Matrix to evaluate and document their security controls
  - The privacy assessment submissions are based on the GDPR Code of Conduct
  - Who should pursue level one?
    - Organizations should pursue this level if they are
    - Operating in a low-risk environment
    - Wanting to offer increased transparency around the security controls they have in place
    - Looking for a cost-effective way to improve trust and transparency

- Level 2: Third-Party Audit
  - Level 2 of STAR allows organizations to build off of other industry certifications and standards to make them specific for the cloud
  - Organizations looking for a third-party audit can choose from one or more of the security and privacy audits and certifications. An organization's location, along with the regulations and standards it is subject to will have the greatest factor in determining which ones are appropriate to pursue
  - Which organizations should pursue level 2?
    - Organizations should pursue this level if they are
      - Operating in a medium to high risk environment
      - Already hold or adhere to the following: ISO 27001, SOC 2, GB/T 22080-2008, or GDPR
      - Looking for a cost-effective way to increase assurance for cloud security and privacy

15. M6.3 - Personal data processing

15.1. Personal data and definitions

- Privacy
  - The state of being alone, or the right to keep one's personal matters and relationships secret
  - The right of an entity (normally a person or an organization), acting on its own behalf, to determine the degree to which the confidentiality of their private information is maintained
  - The value of the information we have is something which we have to protect at all costs

15.2. Privacy law

- Why is privacy so important?
  - The protection of natural persons in relation to the processing of personal data is a fundamental right
  - Everyone has the right to the protection of personal data concerning him or her

How ISO/IEC 29100:2011 can help by giving some basic definitions:

- privacy principles
  - set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems
- privacy risk
  - effect of uncertainty on privacy
  - risk is defined as the "effect of uncertainty on objectives"
  - uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood
- sensitive PII (personally identifiable information)
  - category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal
  - please note: "PII" ("personally identifiable information'), "personal data', "personal information', are usually used as synonymous
  - in some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life or criminal convictions, as well as others defined as sensitive

Why is it important, for organizations, to protect PII?

- Almost everyone these days deals with compliance functions within the organization bundaries, whether it is finance law, tender law, etc.

- Privacy law is becoming of vital importance nowadays for various businesses
- It imposes some rules that are relevant for reducing not only the risk of compliance itself (penalties and/or brand image damage), but also a substantial risk of compromising people's life, at many different levels

15.3. Privacy laws and certification

- Europe
  - *Reg. (UE) 2016/679 European General Data Protection Regulation - GDPR* (which basically applies to european citizens personal data)
    - is one of the most famous examples of rules set to achieve an ambitious but necessary objective in the current digital era: protecting natural persons when their personal data is processed
- World
  - The *California Consumer Privacy Act of 2018 (CCPA)* gives consumers control over the personal information that businesses collect about them and the regulations provide guidance on how to implement the law
  - Some rights here
    - The right to know about the personal information a business collects about them and how it is used and shared
    - The right to delete personal information collected from them (with some exceptions)
    - The right to opt-out of the sale of their personal information
    - The right to non-discrimination for exercising their CCPA rights
- Various to quote around the world
  - LGPD: Brazilian General Data Protection Law
  - POPI: Protection of Personal Information Act (often called the POPI Act or POPIA) for South Africa
  - The Data Protection Act 2018: the UK's implementation of the General Data Protection Regulation (GDPR)
  - The Privacy Act 1988 (Privacy Act): the principal piece of Australian legislation protecting the handling of personal information about individuals

15.4. GDPR definitions

GDPR reports, in various articles, the following statements:

- "Personal data" means any information relating to an identified or identifiable natural person
  - an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, etc.

- Processing of special categories of personal data
  - Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, etc. shall be prohibited
- Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context oftheir processing could create significant risks to the fundamental rights and freedoms

There are some exceptions to the processing of such information, including, for example, the danger of life or the explicit consent given by the data subject.

Other definitions given by GDPR:

- "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, etc.
  - Having data doesn't mean you are not processing data, both preserving and using are parallel aspects one between the other
- "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, etc.
- "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Information to be provided where personal data are collected from the data subject (GDPR, art. 13) and when personal data haven't been obtained from the data subject.

- Please note: Privacy policy / notice is the way the document that contains these information is commonly known

This information must be provided to the interested party, so that he or she can be aware, among other things, especially of:

- why data is collected
- what is the legal basis of the processing (Consent? Contract? Public interest, or a legal obligation?)
- what are the categories of recipients of the data (to whom it will be transmitted and why)
- data retention period
- transfer personal data to a third country or international organization
- the existence of the rights of data subject (articles 15 to 22)

Consdier "security of processing" (GDPR, art. 32):

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms, implement appropriate technical and organisational measures
   - (a) the pseudonymisation and encryption of personal data

- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring thesecurity of the processing

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller

15.5. Privacy standards and certifications

According to the GDPR, Art. 42, about certifications in particular:

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the establishment of data protection certification mechanisms for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors

GDPR, Art. 43 specifies this:

- Certification bodies [=accredited companies that issue the certificates]

  1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall where necessary, issue and renew certification.

  ▸ Member States shall ensure that those certification bodies are accredited by one or both of the following:

    – a) the supervisory authority which is competent pursuant to Article 55 or 56; [e.g. Garante per la Protezione dei dati personali, in Italy]

    – (b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and with the additional requirements established by the supervisory authority

Some considerations:

- Currently, through accredited certification, companies and professionals cannot demonstrate compliance with EU Regulation 679/2016, but can exhibit the independent certification of a third-party body and obtain advantages in terms of safety, effectiveness and competitiveness
- But the compliance assessment sector has activated a series of privacy certifications that have been recognized as a guarantee, and an act of diligence towards the interested parties, of the voluntary adoption of a system of analysis and control of the principles and of the rules of the GDPR

Public and private companies and professionals can request them from accredited certification bodies based on international standards:

- ISO / IEC 17065 for the certification of products and services
- ISO / IEC 17021-1 for the certification of management systems
- ISO / IEC 17024 for the certification of people

15.6. Some ISO standards on the topics

- ISO/IEC 27701:2019 - Security techniques and PIMS (Privacy Information Management System) extension
  - This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a PIMS
  - It specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing
  - It is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS
  - The structure follows different levels of security, additional guidance for PII processors, context of the organization analyzed and planning
  - It is essential to consider the external context. In particular, for personal data, the Organization must take into account the legislation that can have impacts on the achievement of its purposes. In planning the risk analysis, the organization must take into account the risk of loss of integrity, confidentiality and availability of personal information
- ISO / IEC 27018:2019
  - «Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors»
- ISO/IEC 29100 - Privacy framework
  - It provides a privacy framework which:
    - specifies a common privacy terminology
    - defines the actors and their roles in processing personally identifiable information (PII)
    - describes privacy safeguarding considerations; and provides references to known privacy principles for information technology
  - It is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, etc. of systems and services where privacy controls are required for the processing of PII
  - Its structure follows different actors, controls, roles, policies and privacy, describing choices and accuracy the good way

15.7. Other privacy certifications

- ISDP 10003 - Protection of personal data
  - The accredited certification is issued on the basis of the ISDP 10003 private scheme, which follows EU Reg. 679/2016
  - The scheme specifies the requirements for the correctness, security and compliance management of the personal data with specific reference to the correct management of risks
  - The certification covers all types of organizations that want to demonstrate their accountability through the voluntary adoption of a system of analysis and control of the principles and standards of reference on the subject of data protection
- SGCMF 10002 - Compliance of the files of healthcare operators
  - The accredited certification is issued on the basis of the private SGCMF 10002 scheme which concerns the processing of personal data of healthcare professionals of pharmaceutical companies
  - Through the instrument of certification, the pharmaceutical company can keep internal strategic variables under control, rationalize processes and operate in accordance with the law
- UNI / PDR 43 - Management of personal data in the ICT field
  - It's designed for all organizations that process data with electronic tools, in particular to small and medium-sized enterprises
  - The PdR consists of two sections: the first provides the guidelines for the definition and implementation of the processes relating to the processing of personal data, using electronic tools (ICT); the second provides a set of requirements that allows organizations
  - Through the certification, the organization aims to demonstrate the management of personal data in the ICT field in line with the provisions of the GDPR, in terms of security and correctness of the management of the personal data processing process by the owners and responsible
- UNI 11697 - Data Protection Officer (DPO)
  - The standard defines the professional profiles relating to the processing/protection of personal data in accordance with the definitions provided by the EQF (European Qualifications Framework) and provides a series of specialized figures for business management of all privacy-related aspects

16. M6.4 - Data center certification, NIST, CINI, law

16.1. Data center certification and TIER certifications

Data centers and facilities play an important role in protecting information security, its continuity and, in particular, availability of information.

- In some cases, in order to be competitive, organizations need to signal to investors, customers and the market that their data center and facilities have high functional capabilities
  - as demonstrated in the design documents
  - but also verify that the system design itself is consistent with uptime goals
- Certification helps align infrastructure design with corporate mission
  - ensuring that the organization's significant capital investment produces the desired result

We can define a Tier Certification:

- developed by Uptime Institute, the Tier Certification is a measure of data center infrastructure's capability to meet the performance level the business depends on
- A data center's tier certification can be based on Tier Standards, based on an unbiased set of infrastructure and operating criteria

Let's list some key features of Tier Standard:

- Tier Standards are performance-based
- Any design solution that meets the requirements for availability, redundancy, and fault tolerance is acceptable
- This latitude allows you to incorporate a wide variety of infrastructure and system solutions to best meet the organization's goals for IT operations
- They are technology neutral, given tier classification does not require or rely on any fixed set of technologies
- The Standards are able to encompass specific solutions for data center systems and engineering
- Tier Standard criteria is vendor-neutral and unbiased (it does not relate to specific brands)
- The performance-based nature of the Tier standards gives organizations flexibility to comply with local statutes, codes, and regulations
- The Tier Standard has the organization covered in all of its lifecycle
- The Standard is administered by the author of the standard itself, given the usage of a certain certification

Uptime Institute data center classifications are divided into four Tiers that match a particular business function and define criteria for maintenance, power, cooling and fault capabilities.

- The Tiers are progressive, so each Tier incorporates the requirements of the lower Tiers

- This progression does not mean that a Tier IV data center is better than a Tier II — it means that these levels fit differing business operations

Operational sustainability is the second essential component of data Tier classification.

- It refers to the behaviors and risks apart from infrastructure design that determine the ability of the data center to meet long-term business goals
- Data center owners can align their management style to a Tier to achieve these goals, as management behavior is essential to operational sustainability

Together, topology and operational sustainability establish the performance criteria for data centers to follow.

- Data center owners may also want to consider other factors, such as building codes, regional weather, security and property usage
- Uptime institute topology and operational sustainability standards do not cover these factors because they vary in every case. It is ultimately up to the owner to determine which Tier is best for their business needs

The data center Tier definitions define criteria, but not specific technology options or design choices to meet the Tier.

- Tiers are flexible enough to allow for many solutions that meet performance goals and compliance regulations.
- Each data center can decide the best way to meet the Tier criteria and business goals

Let's list all of the different tiers:

- Tier 1 - Basic capacity
  - A Tier I data center is the basic capacity level with infrastructure to support information technology for an office setting and beyond. The requirements for a Tier I facility include:
    - An uninterruptible power supply (UPS) for power sags, outages, and spikes
    - An area for IT systems
    - Dedicated cooling equipment that runs outside office hours
    - An engine generator for power outages
  - Tier I protects against disruptions from human error, but not unexpected failure or outage.
  - Redundant equipment includes chillers, pumps, UPS modules, and engine generators
  - The facility will have to shut down completely for preventive maintenance and repairs, and failure to do so increases the risk of unplanned disruptions and severe consequences from system failure

- Tier 2 - Redundant capacity
  - Tier II facilities cover redundant capacity components for power and cooling that provide better maintenance opportunities and safety against disruptions
  - These components include engine generators, energy storage, chillers, cooling units, UPS modules, pumps, heat rejection equipment, fuel tanks, fuel cells.
  - The distribution path of Tier II serves a critical environment, and the components can be removed without shutting it down. Like a Tier I facility, unexpected shutdown of a Tier II data center will affect the system
- Tier 3 - Concurrently maintanable
  - A Tier III data center is concurrently maintainable with redundant components as a key differentiator, with redundant distribution paths to serve the critical environment.
  - Unlike Tier I and Tier II, these facilities require no shutdowns when equipment needs maintenance or replacement
  - The components of Tier III are added to Tier II components so that any part can be shut down without impacting IT operation
- Tier 4 - Fault Tolerant
  - A Tier IV data center has several independent and physically isolatedsystems that act as redundant capacity components and distribution paths.
  - The separation is necessary to prevent an event from compromising both systems. The environment will not be affected by a disruption from planned and unplanned events
  - However, if the redundant components or distribution paths are shut down for maintenance, the environment may experience a higher risk of disruption if a failure occurs
  - Tier IV facilities add fault tolerance to the Tier III topology.
  - When a piece of equipment fails, or there is an interruption in the distribution path, IT operations will not be affected
  - All of the IT equipment must have a fault-tolerant power design to be compatible. Tier IV data centers also require continuous cooling to make the environment stable

16.2. NIST Framework

NIST framework publication is the result of an ongoing collaborative effort involving industry, academia, and U.S. government.

- The National Institute of Standards and Technology (NIST) launched the project by convening private/public-sector organizations and individuals in 2013
- This Framework for Improving Critical Infrastructure Cybersecurity has relied upon public workshops, multiple Requests for Comment or Information, and thousands of direct interactions with stakeholders from across all sectors

- The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes
- The advntage is having a common language adaptable to many technologies, risk-based, guided by many persepctives and being a living document
- The Framework consists of three parts:
  - the Framework Core
    - a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure
  - the Implementation Tiers
    - provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk, which will help in prioritizing and achieving cybersecurity objectives
  - the Framework Profiles
    - through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources

Particularly:

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction
- It does so by having different functions, categories and references
- Matrices represent implementation tiers pretty well
- The Govern function makes process controlling easier

16.3. CINI – Consorzio interuniversitario nazionale per l'informatica

CINI has improved the Framework Core by introducing:

- new categories and subcategories dedicated to data protection topics (Section 4.1)
- Contextualization Prototypes, a new tool that support and facilitates the denition of contextualizations (Section 4.2)

Goals of the CINI Italian National Framework for cybersecurity and data protection are the following:

- design a cybersecurity framework
- that uses a risk-based approach

- easily adaptable to the heterogeneous characteristics of the Italian context
- coherent with national/international regulations
- aligned to existing standards
- that takes into account data protection

Lead to the Italian national framework for cybersecurity and data protection. It inherits the core structure and contents from NIST CSF 1.1 and has a hierarchically organized collection of 117 enabling activities.

Applying the framework to a given organization requires an appropriate contextualization:

- Selection of core subcategories applicable to the target domain of interest
- Identification of implementation priority levels for all the selected subcategories
- Definition of appropriate controls for subcategory implementation, possibly associated to maturity levels

Parts of a contextualization may be applicable to several realities that share some requirements (e.g. compliance to common regulations, adoption of the same best practices, etc.).

Contextualization prototypes allow the definition of "templates" that can be used to embed specific requirements during the contextualization process.

Prototypes can be used, for example, to capture through the Framework requirements defined by:

- regulations that impose specific requirements linked to cybersecurity or data protection aspects
- technical documents that include specific controls for cybersecurity or data protection processes
- best practices
- for each core subcategory defines an implementation class:
  - mandatory / recommended / free
- for each core subcategory it may define a suggested priority level
- it includes an implementation guide, a document that describes:
  - the domain of interest for the prototype
  - further constraints on subcategory selection (if any)
  - a list of optional controls for the considered subcategories

The Framework is experiencing a growing adoption among Italian organizations of various sizes.

- large organizations already use the NIST CSF => straightforward mapping
- italian NIS authorities published their guidelines for OESs using the Framework as a common baseline Next steps:
  - improve internationalization (currently the core is only available in EN)

- alignment with other frameworks (NIST Privacy Framework, ISO 27701/29100)
- implementation of a quantitative security assessment methodology on top of the Framework

16.4. EU strategies and NIS directives

Regarding cybersecurity, different EU strategies exist:

- EU Cybersecurity Strategy (2013)
- European Agenda on Security (2015)
- Digital Single Market Strategy (2015)
- Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016)

In 2013 the Commission proposed the Directive on security of network and information systems (NIS - Network and Information Security Directive) aiming at ensuring a high common level of cybersecurity in the EU. After an approval process, the Directive entered into force in August 2016.

The Directive builds on three main pillars:

1. ensuring Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority
2. ensuring cooperation among all the Member States
   - by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States
   - and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks
3. ensuring a culture of security across sectors which are vital for our economy and society and moreover rely heavily on information and communications technologies (ICT)
   - businesses with an important role for society and economy that are identified by the Member States as operators of essential services under the NIS Directive will have to take appropriate security measures and to notify serious incidents to the relevant national authority
   - these sectors include energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure
   - also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive
   - similar requirements already apply to telecom operators and internet service providers through the EU telecoms regulatory framework

Cyber security is one of the interventions envisaged by the National Recovery and Resilence Plan (P-NRR) transmitted by the Government to the European Commission on 30 April 2021.

- At EU level, Directive (EU) 2016/1148 of 6 July 2016 sets out measures for a high common level of security of networks and information systems in the Union (so-called NIS – Network and Information Security “)
  - in order to achieve a “high level of security of the network and information systems at national level, helping to increase the common level of security in the European Union”
- The directive was transposed into Italian law with legislative decree no. 65 of 18 May 2018
  - which therefore dictates the legislative framework of the measures to be adopted for the security of networks and data information systems
  - and identifies the competent subjects to implement the obligations established by the NIS directive

Directive (UE) 2022/2555 (also known as ‘NIS 2’) has the purpose to step up action against the “deterioration of the security environment following Russia’s aggression against Ukraine and strengthen the EU’s ability to protect its citizens and infrastructure” and moves towards the full definition of the cyber strategy of the European Union.

- It aims to increase the cooperation between EU Members, reducing costs and increasing effectiveness of cybersecurity measures
- Operators of essential and digital services remain subject to the current regime of the NIS Directive until 2024

Other important sources of European law on cybersecurity include Regulation (EU) 2022/2554 Digital Operational Resilience Act - (DORA) and the Cyber Resilience Act - CRA, the proposed regulation on IT security requirements for products with digital elements.

16.5. New challanges for ICT and cybersecurity law

The most recent reports on information policy sent to Parliament (such as the Annual Report to Parliament and the National Security Document) highlight the significant impact they have had:

- on the life of individuals, as well as on the political-economic balance and on the same way of “playing the democratic game”

The rapid, massive diffusion of new technologies and the consequent, instant accessibility on a global level of news and data, and therefore of knowledge:

- but also of mystified or tout court unfounded representations and distorted or falsified narratives

The current health and geopolitical situation have confirmed the importance of protecting IT and information systems, making data and IT protection a key element for the security of any organization regardless of the reference sector.

- Consequently, never like today the existing laws and regulations on network and system security become a point of reference for all companies that intend to increase their level of security and awareness regarding cyber threats and risks

- In 2020, the European Commission revised the NIS (Network and Information Technology) Directive, questioning the efficiency of the measures adopted
- In the same year, the National Cyber Security Perimeter was first implemented, a plan for the protection of national computer networks and system

The new Commission proposal aims to address the deficiencies of the previous NIS Directive, to adapt it to the current needs and make it future-proof.

- To this end, the Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap
- At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.
- The proposal also eliminates the distinction between operators of essential services and digital service providers
- Entities would be classified based on their importance, and divided respectively in essential and importantcategories with the consequence of being subjected to different supervisory regimes

The proposal strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied.

- The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines
- Furthermore, the Commission proposes to address security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships
- At the European level, the proposal strengthens supply chain cybersecurity for key information and communication technologies
- Member States in cooperation with the Commission and ENISA, will carry out coordinated risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks

The proposal introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

- The proposal also enhances the role of the Cooperation Group in shaping strategic policy decisions on emerging technologies and new trends, and increases information sharing and cooperation between Member State authorities
- It also enhances operational cooperation including on cyber crisis management
- The Commission proposal establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creating an EU registry on that operated by the ENISA

17. M6.5 – Nist CSF Laboratory

17.1. How to read the NIST CSF

17.2. How to use the Framework in the laboratory assessment

18. M7 - Certification of products and technologies

An effective security system can be described as the following:

- “The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff” - FIPS PUB 140-2

18.1. ISO / IEC 15408 - Common Criteria (CC)

- Technology assessment and certification
  - The evaluation of technologies and IT products (hardware, software or firmware) is a difficult problem to solve, as it is not easy to find universal rules
  - However, there are methods to demonstrate reliability that can be placed in the security measures of an IT product
  - One of the best known refers to the so-called Common Criteria, currently considered the most reliable (they are also known as “CC” and the ISO / IEC 15408 standard has transposed them)
  - Specifically, use the following:
    - “secure" to do what (security goals)
    - “secure” in which context (security environment)
    - “secure" against which checks (assurance requirements)
  - It has the following structure:
    - Part 1 - Introduction and general model is the introduction to the CC
      - It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation
    - Part 2 - Security functional components establishes a set of functional components that serve as standard templates upon which to base functional requirements for TOEs (Targets of Evaluation)
      - CC Part 2 catalogues the set of functional components and organises them in families and classes
    - Part 3 - Security assurance components establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs
      - CC Part 3 catalogues the set of assurance components and organisesthem into families and classes
      - It also defines evaluation criteria for PPs (Protection Profiles) and STs (Security Targets) and presents seven predefined assurance packages which are called the Evaluation Assurance Levels (EALs)

The standard provides for seven increasing levels of assurance:

- from EAL1 (Evaluation Assurance Level) to EAL7, which depend on the extent and formality of the documentation used during the analysis and development phases, but also on the development methods

The Common Criteria contain a grouping of security functional requirements divided in classes, which can be represented as diagram flows:

- this grouping allows specific classes of requirements to be evaluated in a standard way in order to meet an Evaluation Assurance Level

Something to be careful about:

- The onerousness of the assessment can lead a manufacturer to choose to certify only part of the security functions of their product
- A dishonest seller, however, could use the same system to mask the presence of security functions for some reason "weak", by having only the functions evaluated sufficiently robust

For instance, if for some reason a specific function of some device has not been included in the evaluated configuration (perhaps because it is vulnerable to some type of attack or because it is deliberately obsolete), the enabling of one of these functions would pose a serious risk to the system.

- The sense of trust that is placed in the certification may lead us not to consider its actual 'perimeter'. This is not always known
- It is necessary to have trained personnel who adopt the appropriate procedures to configure the product correctly even at the cost of limiting its functionality

ISO/IEC 15408-5 called "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements" has been published on 2022-08.

- It provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders

18.2. Federal Information Processing Standard (FIPS) 140-2

Federal Information Processing Standard (FIPS) 140-2 is one of the main standard for validating the effectiveness of cryptographic modules.

- If a product has a FIPS 140-2 certificate, you know it has been formally tested and validated by the governments of the United States and Canada.
- Although FIPS 140-2 is a US / Canadian federal standard, FIPS 140-2 compliance has been widely adopted around the world in both government and non-government sectors as a practical safety benchmark and realistic best practice

This standard requires specialized laboratories to identify and test a particular hardware, software or firmware module.

- Cryptographic modules can be produced by the private sector (also by open source community) or public for use by particular sectors (e.g. health, finance) and in general the critical infrastructures that make use of these modules to process sensitive information

There are 11 areas of control:

- Cryptographic module specification (what must be documented)
- Cryptographic module ports and interfaces (what information flows in and out, and how it must be segregated)
- Roles, services and authentication (who can do what with the module, and how this is checked)
- Finite state model (documentation of the high-level states the module can be in, and how transitions occur)
- Physical security (tamper evidence and resistance, and robustness against extreme environmental conditions)
- Operational environment (what sort of operating system the module uses and is used by)
- Cryptographic key management (generation, entry, output, storage and destruction of keys)
- EMI/EMC (Electromagnetic interference/compatibility)
- Self-tests (what must be tested and when, and what must be done if a test fails)
- Design assurance (what documentation must be provided to demonstrate that the module has been well designed and implemented)
- Mitigation of other attacks (if a module is designed to mitigate against, say, TEMPEST attacks then its documentation must say how

Organizations use the FIPS 140-2 standard to ensure that selected hardware meets specific security requirements. The FIPS certification standard defines four increasing quality security levels:

- Level 1: Requires production-grade equipment and externally tested algorithms
- Level 2: Adds requirements for physical tamper evidence and role-based authentication
  - Software implementations must run on an EAL2 level Common Criteria approved operating system
- Level 3: Adds requirements for physical tamper resistance and identity-based authentication
  - There must also be a physical or logical separation between the interfaces according to which "critical safety parameters" enter and exit the module
  - Private keys can enter or exit only in encrypted form

- Level 4: This level makes physical security requirements more stringent, requiring the ability to be tamper-proof, wiping the contents of the device if it detects various forms of environmental attack

Internationally, the equivalent of FIPS 140-2 is ISO / IEC 19790: 2012 with the title 'Security requirements for cryptographic modules'.

- ISO / IEC 24759: 2014 (Information technology -Security techniques - Test requirements for cryptographic modules) is the equivalent of the NIST Derived Test Requirements document

18.3. Federal Information Processing Standard (FIPS) 140-3

While FIPS 140-2 continues on through 2026, development to support and validate FIPS 140-3 modules must be in place by September 2020.

- This project addresses questions concerning the process of migrating from FIPS 140-2 to FIPS 140-3
- The transition process includes organizational, documentation and procedural changes necessary to update and efficiently manage the ever increasing list of security products that are tested for use in the US and Canadian governments
- Changes also support the migration of internally developed security standards towards a set of standards developed and maintained by an international body, while also referencing government standards

18.4. Italian National ICT Security Assessment Scheme

National ICT Security Assessment Scheme ("Schema Nazionale di Valutazione della Sicurezza ICT") collects all the procedures and rules necessary for the evaluation and certification of ICT systems or products or Protection Profiles, in compliance with the European ITSEC or Common Criteria

- The National Scheme does not apply to systems and products that handle classified information

The procedures relating to the National Scheme, described in detail in the Guidelines, must be observed by the Certification Body (OCSI), by the Laboratories for Safety Assessment (LVS)

- as well as by all those (individuals, legal entities and any other subject) that operate within the national scheme

In addition to the OCSI, the following entities operate within the National Scheme:

- Safety Assessment Laboratories (LVS): carry out assessment activities under the control of the OCSI
- the Client: is the person who commissions the evaluation and can coincide with the Supplier
- the Supplier: is the person who provides the Object of the Assessment (ODV)
- the Assistant: is a person trained, trained and authorized by OCSI to provide technical support to the Client or Supplier

18.5. CVCN - Centro di Valutazione e Certificazione Nazionale

With the decree-law n. 105 of 2019, converted into law no. 133 of the same year - which defines the national cyber security perimeter - the National Evaluation and Certification Center (CVCN) - set up at the Ministry of Economic Development

- was entrusted with the task of carrying out the assessment of ICT goods, systems and services intended to be used on ICT infrastructures that support the provision of essential services or essential functions for the State

The subjects included in the national security perimeter, pursuant to article 1 are required to communicate to the CVCN their intention to acquire ICT goods and services to be used on their "strategic" assets belonging to certain categories identified on specific criteria.

- The CVCN, within a maximum time of 60 days from the communication, indicates to the subject included in the perimeter any conditions to which the suppliers must comply and hardware and software tests that must be carried out

Any conditions and tests are included in the calls for tenders and contracts with clauses that condition the contract on compliance with the conditions and the favorable outcome of the tests ordered by the CVCN.

- The tests can be carried out in the CVCN laboratories or in test laboratories accredited by the CVCN itself and must be completed within sixty days
- Since the Ministry of Defense and the Ministry of the Interior can make use of their own Assessment Centers - CVs
- For acquisitions destined for their networks, information systems and IT services, the CVCN will have to liaise with these Assessment Centers to prevent the supplier from carrying out several times the tests on the same product

With the Decree of the President of the Republic February 5, 2021, n. 54, the procedures, methods and terms of operation of the CVCN have been defined, as well as the procedures for verifying compliance with the provisions of decree-law no. 105/2019

- as well as the technical criteria for identifying the categories of goods, systems and ICT services (to be carried out with DPCM) that will be subject to the evaluation of the CVCN in the event that they are intended for "strategic" assets

Recently the regulatory scenario in the field of cybersecurity was revisited with the issue of the decree-law of 14 June 2021, no. 82 converted into law no. 109, which defined the national cybersecurity architecture and established the National Cybersecurity Agency.

- In the new context, the National Assessment and Certification Center (CVCN) has been transferred to the Agency
- The regulatory framework has been completed with the approval of the Prime Ministerial Decree which defined the procedures for the accreditation of the test laboratories and the methods of linking the CVCN with the CVs

The CVCN is the technical structure that, together with a network of accredited laboratories, will be responsible for verifying the security and absence of known vulnerabilities in ICT goods, systems and services

- with the aim of raising the level of cybersecurity and resilience of the infrastructures on which the country's essential functions and services depend
- it has been transferred from the Ministry of Economic Development to ACN (Agenzia per la Cybersicurezza Nazionale) and entered into operation since 30 June 2022
- it will have the task of carrying out preliminary checks on the assignment procedures and may impose conditions and tests aimed at the security analysis of hardware or softwaree particularly sensitive if compromised

18.6. PCI DSS

PCI DSS is a cybersecurity standard first issued in 2006 when the world leading card issuers formed the Payment Card Industry Security Standards Council. Developed to prevent data theft of payment card holders and make transactions through these cards safer, it is a very important tool.

- PCI Security Standards are developed specifically to protect payment account data throughout the payment lifecycle and to enable technology solutions that devalue this data and remove the incentive for criminals to steal it
- They include standards for merchants, service providers, and financial institutions on security practices technologies and processes, and standards for developers and vendors for creating secure payment products and solutions

PCI DSS stands for Payment Card Industry Data Security Standard and is a proprietary standard for cybersecurity managed by the PCI Security Standards Council (PCI SSC).

- This standard applies to organizations that store, process or transmit data relating to credit card holders, such as merchants, buyers, issuers and service providers
- PCI DSS is the gold standard for consumer protection and helps reduce fraud and data breaches across the payments ecosystem
  - It applies to all organizations that accept or process payment cards, therefore, also to structures in the hospitality sector
  - When implemented correctly, PCI DSS can help these organizations secure their own and their customers' data

The Payment Card Industry Security Standards Council is the body that issues the PCI DSS certificate. But how to get PCI DSS certification? It can be done in two ways:

- Through self -certification , by completing an SAQ (Self Assessment Questionnaire) form and an AOC (Attestation of Compliance) form
- By contacting a QSA (Qualified Security Assessor) company that issues the certification

A company must meet certain requirements to be PCI DSS compliant.

- These requirements concern the ways in which cardholder data is stored, processed and transmitted, but also how card data flows, how it is stored and which IT systems are used
- This document, the Payment Card Industry Data Security Standard Requirements and Testing Procedures, consists of the 12 PCI DSS principal requirements, detailed security requirements, corresponding testing procedures, and otherinformation pertinent to each requirement
- The PCI-DSS certification was created to guarantee the protection of credit card holder data and indicates precise requirements for procedures, network architecture and software that must be met by the companies that manage credit card numbers
- Hackers want cardholder data. By obtaining the Primary Account Number (PAN=cardholder data) and sensitive authentication data, a thief can impersonate the cardholder, use the card, and steal the cardholder's identity

Sensitive cardholder data can be stolen from many places:

- Compromised card reader
- Paper stored in a filing cabinet
- Data in a payment system database
- Hidden camera recording entry of authentication data
- Secret tap into a store's wireless or wired network

Cardholder data can be secured where it is captured at the point of sale and as it flows into the payment system. The best step you can take is to not store any cardholder data. This includes protecting:

- Card readers
- Point of sale systems
- Store networks & wireless access routers
- Payment card data storage and transmission
- Payment card data stored in paper-based records
- Online payment applications and shopping carts

19. M8.1 - Frameworks that describe the competencies - e-cF, NICE, AgID

In all advanced economies, work is becoming increasingly knowledge intensive both in terms of specific knowledge and in terms of more general knowledge. The pervasiveness of the use of machines, digital technology and artificial intelligence (AI) requires more and more specific knowledge in the technological field.

19.1. ICT competencies and standardization

This knowledge is now indispensable not only for highly qualified professions, which have always been characterized by a high intensity of knowledge, but also for apparently less qualified professions that actually interact with extremely sophisticated and complex devices, robots and machines.

- The need to observe social distancing also in working activities has led to an exponential increase in smart working and remote working
- The rapid evolution and expansion of ICT labor markets requires a common language to manage the supply and demand for talents, which is particularly critical and complex in a scenario of transnational integration such as the European Union.

Models and *frameworks* are useful tools for this purpose.

- Digital skills frameworks can improve information security in many ways, regardless of whether the focus is on cybersecurity (as in the NICE framework)
- The more the skills can be typified and composited, the more it is possible to search for specific skills in the professional figures that one wants to hire for certain jobs, and the workers can test their skills in the same way against the typed criteria

19.2. e-CF

European e-Competence Framework (e-CF) is a reference framework of ICT competences that can be used used and understood by ICT user and supply companies, ICT practitioners, managers and Human Resources (HR) departments, the public sector, educational and social partners across Europe.

- e-CF was designed to be an empowerment tool for users, and not to define any kind of restrictions and was designed to support understanding, not to make the use of every term used within the framework mandatory
- Please note: Competence should not be confused with technological or process concepts such as ‘Cloud Computing’ or ‘Big Data’. These concepts represent evolving technologies and, in the context of the eCF, can be integrated as examples in the description of knowledge and skills

We give some definitions related to e-CF:

- *Competence* is a demonstrated ability to apply knowledge, skills and attitudes to achieving observable results
  - Consequently, the related e-Competence descriptions embed and integrate knowledge, skills and attitudes

- *Skill* is defined as “ability to carry out managerial or technical tasks”. Managerial and technical skills are the components of competences and specify some core abilities which form a competence
- *Knowledge* represents the “set of know-what” (e.g. programming languages, design tools…) and can be described by operational descriptions as well
- *Attitude* means in this context the “cognitive and relationalcapacity” (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism…). If skills and knowledge are the components, attitudes are the glue, which keeps them together.

19.3. NICE Framework

19.4. AgID guidelines

20. M8.2 - Frameworks that describe the competencies - NICE, DoD Pathways, ENISA

20.1. Cyber Career Pathways Tool

20.2. U.S. Department of Defense (DoD)

20.3. Cyber Career Pathways DoDD 8140/8570

20.4. NIST-NICE Framework and DoDD 8140/8570

20.5. ENISA

20.6. Conclusions

21. M9 - Certification of people

21.1. Accreditation body

21.2. Conformity Assessment Body (CAB)

21.3. IAF and Mandatory Documents

21.4. ISO/IEC 17024:2012 - Conformity assessment

21.5. Certified ISO/IEC 27001 auditor

21.6. Conclusions

22. M10 - Most common Certifications available on the market

22.1. COBIT 5

22.2. IT Governance and Management certifications (ISACA - COBIT)

22.3. IT Security Certification for people

22.4. Certifications and IT security laboratories

23. M11.1 - Audit techniques and approach examples

23.1. Process and definitions

23.2. Purpose of a certification

23.3. Certification, surveillance and recertification

23.4. Audit plan, initiation and preparation

23.5. Preparing audit activities

23.6. Auditing a process and sampling

23.7. Nonconformities

23.8. Closing meeting

23.9. Use cases

24. M11.2 - Practical cases, ISMS audit

24.1. Audit and certification process

24.2. Documentation

24.3. ISO/IEC 27001:2022 - Auditing the ISMS

24.4. Security controls (countermeasures)

24.5. Most common findings