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) 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 or remotely interesting. 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. I advise to study this file on your own and in case you want to do the report to participate in the laboratory held in May usually. I found as many reports as I could in order to have some reference of any kind, see our MEGA for reference.

Overall, the course is very very heavy and notional, useful but most of the time with unnecessarily long notions given throughout - like, it would literally take much much less to explain some parts, so verbose.

Book references are made across chapters to the "Effective Cybersecurity" made by William Stallings (quoted by course syllabus since it basically contains many things of the first part of it) 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. Do I suggest to see the book? It's good, but in any case, refer to this material, is good enough and brought to you summarized and in a readable form which does not kill your eyes (am I right, slides?)

Consider titles of sections (given the slides have basically all misleading or not complete titles, apart from some of the second part) were refined to give you immediately the idea of said concepts. Given how sparse these concepts are, I felt necessary to revise multiple times the slides to ensure subsections are as much as needed without feeling too much to cover and divide logically all the content present in the course. No recording or anything of this "very useful subject" will be present anyway.

Feel free to reach me to feedback about the contents of this file; also to thank me, it doesn't kill me that much.

2. Course program

Prof. Simone Soderi will do the following:

1. Basic Concepts
2. Planning for Cybersecurity
3. Cybersecurity Operations and Management
4. Security Assessment and use cases

Prof. Antonio Belli will do the following:

5. Certification and Frameworks for Organizations and management systems
6. Certification of products and technologies
7. Frameworks that describe the competencies
8. Certification of people
9. Most common Certifications available on the market
10. Audit techniques and approach examples

3. M1.1 - Basic concepts - Terms, Governance, SOGP and ISO Standards

(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)

3.1. Key terms

Cyberspace

- Consists of:
  - Artifacts (e.g., hardware, software)
  - 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 (e.g., human aspects, risks, attacks and defense)

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 and ensures *achievement* and *maintenance* of assets *connected*, *stored* and *transmitted*

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 (e.g., malware, hackers)

Vulnerability

- A flaw or weakness in a system's design that can be exploited violating security policies (e.g., outdated software, misconfiguration)

Information security

- Preservation of confidentiality, integrity and availability of information
- Additional properties: authenticity, accountability, non-repudiation, and reliability

3.2. 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*: considering *many devices and individuals* and *technologies advance*
- *Nature of threat*: *evolving threat* and *evaluating* security risks
- *User needs vs security implementation*: technology with the most modern and *powerful features* to implement *effective security*
- *Difficulty estimating costs and benefits*: *total costs* of cybersec and achieving *consensus*

3.3. Risk assessment

Risk:

- 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*

Going deeper for risk assessment:

- Uses *analytic and structured processes to capture the potential for desirable and undesirable events*, and measure *likely outcomes and impact*
- Involves *reviewing collected information*, forming the *basis for decisions leading*
- Estimates the different *levels* of risks:
  - Intolerable: risk needs to be abandoned or replaced
  - Tolerable: risks have been reduced with reasonable methods
  - Acceptable: risk reduction is not necessary

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

3.4. Governance structure terms

Source of these terms here:

- 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
  - These help address the question of how the organization actually puts into operation a policy, standard or control

- Guidelines
  - Recommended practices that are based on industry-recognized secure practices
  - This can be applied where we cannot apply the standard

3.5. Standards and Best Practices documents

Organizations and industry groups have developed best practices, guidelines, and standards for implementing and evaluating cybersecurity, including:

- 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)

3.6. Standard of Good Practice (SOGP)

A security policy:

- *Set of rules and practices* that specify or regulate *how a system or organization provides security services to protect sensitive and critical system resources*
- Includes associated responsibilities, security principles followed by all relevant individuals
- *Applies to all employees* and is applied by CISO and Security Manager
- Has many different types (e.g., access control, network security, etc.)

Specifically, about the Standard of Good Practice (SOGP):

- Issued by the Information Security Forum (ISF). The goal of the ISF is the *development of best practice methodologies, processes, and solutions*
- A business-focused comprehensive *guide to identifying and managing information security risks*
- *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/IT managers, auditors and vendor management teams

- Consists of 17 categories, each with 2 areas and 132 topics addressing good practice controls, being consistent with the ISO/IEC 27000 standards structure
  - Main ones are:
    - Security management
    - Critical business applications
    - Computer installations
    - Networks
    - Systems development
    - End user environment
- Has three *main activities*:
  - *Planning* for cybersecurity: developing approaches/requirements/policies
  - *Managing* the cybersecurity function
  - *Security assessment*: assuring continuity, assessing and improving the suite of cybersec controls

3.7. ISO/IEC 27000 - Information security management

ISO and IEC have developed the ISO/IEC 27000 series of standards dealing with Information Security Management Systems (ISMS).

- 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 and societal values
- Preventing and detecting, while always reassessing

It is composed by 4 *categories*:

- Overview and vocabulary
- Requirements

- Guidelines
- Sector-specific guidelines

3.8. ISO/IEC 27001 - Information Security Management Systems - Requirements

ISO 27001 is a management standard initially designed for the *certification* of organizations. It specifies the *requirements* for establishing, implementing, maintaining, and continually improving an ISMS within the context of an organization. It's composed by:

- *Certification Audit*
- *Qualified individuals* to develop and maintain an ISMS
- Obtaining *certifications* (third-party assessments) to enhance the value, provided by independent bodies
- It can be mapped easily to meet ISF SOGP, providing a far more detailed description of the controls able to satisfy requirements

3.9. ISO/IEC 27002 - Code of Practice for Information Security Controls

ISO 27002 provides the broadest treatment of ISMS topics in the ISO 27000 series and *allows for selection of controls for ISMS*. It provides guidelines and best practices for implementing controls and measures to address specific information security risks identified by the organization. Specifically:

- 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, given ISF SOGP is far more detailed but selects even more controls

3.10. IEC 62443 - Industrial Cyber Security

It 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: describes security requirements for systems for components

Differs from IT systems due to infrequent patching, critical time dependency, and lower awareness.

It defines *roles*:

- *Product supplier*: responsible for *development* and *testing* of control systems, *embedded* devices, and *host* devices
- *System integrator*: responsible for *integration* and *starting up*, conforming to *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 can keep *assisting*
- *Security zones*
  - *Physical* or *logical* groupings of assets that share *common security requirements*
  - Applies with the previous the concept of defense in depth
- *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* by resisting several attacks

Finally, its *security levels*, which help in making decisions and categorize and prioritize cybersecurity requirements based on the criticality of assets and potential impact of security breaches:

- Focus on *zones*, making *decisions on countermeasures*
- Applicable to *defense in depth*
- Different *security levels* 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*
- Service providers/asset owners 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

4. M1.2 - Basic concepts - Cybersec frameworks

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

4.1. NIST Cybersecurity Framework

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

- 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
  - For example, NIST SP 800-53 provides state-of-the-art practice security controls and control enhancements
- The *NIST Computer Security Resource Center (CSRC)* is the source of a vast collection of documents that are widely used in the industry (more here)
- 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. The document itself is *used for nongovernment organizations*, with the clear goal of continuous improvement while managing supply chain risk
- Useful for final report, so start reading this one here but also here

Composed by three *parts*:

- *Core*: Cybersecurity *activities*, desired *outcomes*, and applicable *references*
- *Implementation tiers*: Provide *context* on how an organization views cybersecurity risk
- *Profiles*: Represent 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*

Each subcategory provides a list of informative references with sections, standards and guidelines.

Composed by tiers, which define the *priority* and the *level of commitment*. These describe increasing *degrees of rigor* of practices and *extent* of business needs information and *integration*:

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

Composed by profiles, which are a selection of categories and subcategories which define a *target profile* and enable management, needing for maintenance and usage of referenced guidelines with concrete descriptions. The cybersec posture of an organization is called *current profile*.

There was a significant *revision* of NIST CSF with version 2.0:

1. It introduced a new function called "*Govern*", which emphasizes the significance of organizational governance in cybersecurity
2. It emphasizes the importance of *managing supply chain risk*, which is a growing concern for organizations
3. It encourages organizations to *adopt a mindset of continuous improvement*

Given approaching a document such as the ISF SOGP or the ISO 27002 can be *intimidating* and even overwhelming because of the large body of knowledge inside, this framework is an *excellent resource* to help in use of more detailed documents.

- For this reason, *NIST has produced a large number of FIPS publications and SPs* that are enormously useful to security managers, designers, and implementers
- Some of these documents are *prescriptive standards*, but many of them are *tutorials* or *surveys* - describing *countermeasures* = actions reducing threats/vulnerabilities/attacks

Some important NIST *documents* to quote:

- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations - state-of-the-art practice security controls and control enhancement
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (2006)
- NIST SP 800-12, Introduction to Information Security, (2017) - introduction to the topic of information security
- NIST SP 800-55, Performance Measurement Guide for Information Security (2008)
- SP 800-100, Information Security Handbook: A Guide for Managers (2006) - overview of information security program elements to assist managers in understanding/implementing security programs

4.2. 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 (*Adversarial Tactics, Techniques & Common Knowledge*) 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 against adversary behaviours, adapting lifecycle models which didn't fit, observing incidents and bringing a common taxonomy
- It's available *free of charge* and includes a global knowledge base of adversarial tactics, techniques, and procedures (TTPs) based on real-world observations
- It's organized into *matrices* to represent different types of adversaries, platforms, and environments. The most well-known matrix is the *Enterprise ATT&CK matrix*, which focuses on tactics and techniques observed in enterprise networks
- 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
    - These describe *what* the adversary is trying to do (e.g., steal credentials)
  - *Techniques* = *How* adversaries achieve their actions and *what* an adversary gains performing actions
    - These can be organized into a series of tactics to help practitioners detect and remediate threats
    - They describe the actions the adversary takes to achieve their goals (e.g., brute force methods)

This framework was designed to address four main *issues*:

- *Adversary behaviours*: adversary tactics allowing to develop analytics
- *Lifecycle models that didn't fit* inside existing adversary lifecycle
  - Cyber Kill Chain = model describing what the attacker needs to do to succeed
- *Applicability to real environments* looking at *observed incidents*
- *Common taxonomy* across different types of adversary groups all speaking the same language
- It includes a *Group database* that *tracks the activities*

The above matrix can be used to 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* than having to repair damages
- A whole matrix is available, describing tactics and procedure examples and containing steps once the attack is launched (see here)

4.3. 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 and integrating elements from NIST Framework*
- Its *key principles*:
  - Core: structured list of requirements
  - Controls: sets of actions
  - Informative references: tieing each subcategory to known security practices
  - Priorities levels: priority of implementation
  - Maturity levels: implementation
  - Contextualization: process of selecting subcategories
  - Prototype of contextualization: templates to implement contextualization
- There is a specific framework *methodology*:
  - *Phase 1 - Contextualization*
    - Contextualizing the Framework *to the reality of interest*, achieving as outcome a *Target Profile* and *desired reference* to aim and 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*
    - This allows for results of the assessment to be *analyzed from different points of view*

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 for the organization:

- *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

4.4. 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 (in case, see all projects here):

- *OWASP Top 10*
  - *Standard awareness document for developers and web application security*, representing broad consensus about most critical security risks to web apps
  - Using the OWASP Top 10 is *perhaps the most effective first step towards changing the software development culture*
  - By itself, it's an awareness document that highlights the *top 10 most critical web application security risks* (reference here)
  - Risks are ranked based on frequency, severity and impact
- *OWASP Cheat Sheet Series*
  - Created to *provide a set of simple good practice guides for application developers and defenders to follow*
  - This is intended to provide *useful practices that most developers will actually be able to implement* (more here)
- *OWASP Mobile Top 10* [2016]
  - Consists of the *most critical security risks to mobile applications* with data gathered thanks to *surveys*. 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) defining process/techniques/tools using during mobile security tests
  - 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
    - Key points of this one: Security Assessments / Pentests - Standard Compliance - Learn & practice your mobile security skills - Bug Bounties - (reference here)

- *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 (similar to many things already seen - just wait to see things repeatead ad nauseam for a lot more pages!)

4.5. Cybersecurity management process

A good cybersecurity management process is 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 at work:
  - The first is at an *executive* level (organizational)
    - It focuses on organizational risk, *defining* priorities, levels of tolerance and determining available resources
  - The second one is at a *business* level (infrastructural)
    - It focuses on infrastructure risk management, *translating guidelines into controls*

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

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

5.1. 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:

- The *process* of establishing and maintaining a framework and supporting management structure and processes
  - Alternatively, as a complementary definition, the *system* by which activities are directed and controlled - another definition, same meaning
- 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 different levels of *security*:

- *Governance*
  - Process that develops the *security program* that adequately meets the strategic needs of the business
    - *Security program* is the management, operational, and technical aspects of protecting information and information systems
      - It *consists in* different policies/procedures for coordinating activities
  - 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
  - *Management* is expressed through *formulation and use of information security policies, procedures and guidelines*
  - Uses the information as inputs into the risk management process that *realizes* the security program and *define* the cybersecurity *profiles*

- *Implementation/operations*
  - *Implementation, deployment* and ongoing operation of security controls defined within a cybersecurity framework
  - *Integrates* into the *life cycle* and *monitors* security performance continuously

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 (Information security, cybersecurity and privacy protection - Governance of information security)* establishes as a *key objective* "the alignment of information security objectives and strategy with overall business objectives and strategy"
- Before that, very brief definitions:
  - IT (Information Technology) = Applied computer systems, both hardware and software usually in the context of a business or other enterprise
  - Stakeholder = A person, a group, or an organization that has interest or concern in an organization
- We can list 6 *principles*:
  1. Establish organization wide information security at all levels ensuring serving of business objectives
  2. Adopt a risk-based approach based on the risk readiness of an organization
  3. Set the direction of investment decisions, ensuring it is integrated with existing organization processes
  4. Ensure conformance with internal (goals/objectives) and external requirements (legislations/regulations)
  5. Promote a security-positive environment for all stakeholders, responsive to their expectations and promoting a positive information security culture
  6. Review performance in relation to business outcomes and checking precisely their measurements

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
    - Security strategy and policy have to be aligned with business strategy

- Risk management
  - The principal driving force, which involves mitigating risks and reducing or preventing potential impact on information resource
- Resource management
  - A key goal of information security governance is to align information security budgets with overall enterprise requirements
- Value delivery
  - Information security investments need to be managed to achieve optimum value
- Performance measurement
  - The enterprise needs metric against which to judge information security policy

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

5.2. Strategic planning

A strategic plan is a document used to communicate, within the organization, the organization's goals and the actions needed to achieve those goals. This should be approved by executives and committees, while regularly reviewed.

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 a *strategic plan with ongoing oversight of the implementation*
- *IT strategic* planning
  - It is the alignment of IT management and operation with enterprise 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 *small 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* and paying attention to the *key drivers*
  - Imperatives, roadmaps and finances: discussion of strategic objectives and a budget for investment plans, *reflecting IT's highest priority items*
  - 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 and is a document approved by executives

5.3. 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 effects

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*

5.4. 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

X.1054 provides an example of detailed contents a report should include:

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

5.5. Security roles

A *key aspect* of security governance is defining the *roles and responsibilities* of executives related to information security:

- All of the following positions refer to the "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 (e.g., governance/business drivers, roles and responsibilities, metrics/audit).

5.6. 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

5.7. 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

5.8. 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:

- Strong executive management support and security awareness
- Business and information security relationship with goals and objectives
- Information protection, with good level of awareness and training to deal with attacks

Security governance also enlists some best practices, enabling the organization to set clear direction and demonstrate their commitment to information security and risk management:

- Security governance framework: *checklist of action*
- Security direction: *outline of a recommended top-down management structure*
- Information security strategy: *checklist of security*
- Stakeholder value delivery: *value delivered by each stakeholder*
- Information security assurance: *discuss actions so to adequately assess risks*

5.9. Risk assessment

Risk assessment is a complex subject; 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.

- Security Risk = 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
  - Both factors are *necessary 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:
    - Asset: Put value on assets
    - Threat: Determine the entire range of threats
    - Vulnerability: Vulnerabilities an organization may not be aware of
    - Controls: Effectiveness of given controls
- The difficulty of *predicting* future conditions
  - Four main elements:
    - Asset: Change and impact on assets
    - Threat: Assess and determine effect on threats, even without complete knowledge of them
    - Vulnerability: Changes within the organization may create unexpected vulnerabilities
    - Controls: New technologies may provide opportunities and is difficult to predict the nature of such

5.10. 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, so *results are fed back into the next iteration*:
  - *Assess* and *determine* likelihood and impact
  - Identify *security controls to be reduced and prioritized*
  - *Allocate* resources, roles and responsibilities and *implement* controls

  - *Monitor* and *evaluate* risk treatment effectiveness
- *Risk management for large organization use a broader framework (ISO 27005)*, iterative process made up of *continual changes* given it's an ongoing activity, consisting of separate activities:
  - Context establishment
  - Risk assessment (with identification/analysis/evaluation)
  - Risk treatment
  - Risk acceptance
  - Risk communication and consultation
  - Risk monitoring and review

5.11. 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*
    - E.g., what would happen if information were made public, if was incorrect or cannot be accessed

- *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.

5.12. Threat types and identification

Threat identification is the process of *identifying sources with the potential to harm system assets*. Such 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*, given *threats continue to evolve overtime*
- Thus, keeping informed on threats in an *ongoing and never-ending battle*
- Three important *categories* of threat information sources are:
  - *In-house experience*
    - Experiences already had inside the organization on identifying attacks
  - *Security alert services*
    - Concerned with *detecting threats as they develop* to enable organizations to patch code, change practices or react
  - *Global threat surveys*
    - Many are available (e.g. Cisco, ENISA, Verizon, Fortinet, Trustwave) 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*.

- *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
- In some cases, an organization establishes a SOC itself, in other cases, SOC services are outsourced

5.13. 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 really implemented*
- (3) *Conduct an on-site review of the physical controls*, comparing those implemented with the list of what controls should be there and *see if they work correctly/effectively*
- (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 (e.g., AC = Access Control, AU = Audit and Accountability, etc.).

- *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

5.14. Vulnerability identification and classification

Vulnerability identification is the process of identifying *vulnerabilities*, which are *weaknesses 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)* - here
  - It is a comprehensive *list* which 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)* - here
  - It indicates the *severity* and each level assigns a *numeric value in a scale from* 0.0 *to* 10.0, producing an *aggregate base security score*
  - Calculator related to vulnerability's level of exploitability with relative parameters here
- *Common Vulnerabilities and Exposures (CVE)* - here
  - Simply a *list* of *all publicly disclosed vulnerabilities* with their data

5.15. 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:

- Uses numerical values to measure risk in terms of probability and impact
- If all factors are expressed *quantitatively*, then it is possible to develop a *formula that measures the cost of security breaches* as follows:
  - Level of risk = (Probability of adverse event) x (Impact value)
  - We can express the *residual risk level*, equivalent to *the expected cost of security breaches with the implementation of controls*:
    - Residual risk level = (Probability of adverse event)/(Mitigation factor) x (Impact value)

- If various *factors can be quantified*, previous equations should be *used to guide decisions*, for example in understanding *how much to invest in security controls*
- As new controls are implemented, cost of breaches *declines*, but total cost of security controls *increases*
- The *optimal* cost point represents a *level of risk that is tolerable*

For qualitative risk assessment:

- It determines a *relative risk rather than an absolute risk*. Evaluates risk-based on *relative estimates and subjective judgments rather than precise numerical values*
- It is *usually sufficient for identifying the most significant risks*
- Uses descriptive *categories, levels or scales* to measure risk:
  - *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*

Inside of matrices determining risk:

- 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
- The *impact* is determined as a function of asset class and exposure to loss
- The *likelihood* of an adverse security event is a function of the frequency/likelihood
- And finally the *risk* can be expressed as a function of the impact and likelihood

Results of 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: brief statement of each security issue
  - Likelihood: estimate likelihood of occurrence
  - Impact: estimate impact for threat/vulnerability pair
  - Risk level: risk level based on matrices like showed before
  - Recommended security controls: used for particular issues

  - Control priorities: relative priority for recommended controls
  - Comments: any other information considered relevant
- *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

Any issue with a compliance score of less than 3 should be included in the worksheet with a risk level of high.

5.16. Factor Analysis of Information Risk (FAIR)

FAIR (Factor Analysis of Information Risk) 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": combination of Loss Event Frequency and Loss Magnitude
- It provides a *far more detailed set of guidelines than ISO 27005*, giving *definitions less vague and more specifically tied to risk analysis*
- It is based on a belief that *subjective qualitative analysis is inadequate* in most situation of risk analysis
- ISO 27001 describes a general process, ISO 27005 defines the approach for managing risk, *FAIR provides a methodology for analyzing risk*

FAIR risk analysis documents groups *controls* into four *categories*:

- (1) Avoidance controls: frequency and likelihood of *encountering threats*
- (2) Deterrent controls: affect the *likelihood of a threat acting*
- (3) Vulnerability controls: probability a *threat's action will result in loss*
- (4) Responsive controls: affect *the amount of loss*
- It 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*
- It has different *risk assessment levels*:
  - FAIR provides *detailed guidance on how to systematically characterize event likelihood*, documented as *loss event frequency*

- The *assessment* of threat event frequency involves two *aspects*:
  - Determining *frequency* of *contact* with assets
  - *Probability* of *acting* against assets
- *Contact* can be of two *types*:
  - *Physical* access is possible for employees and outside actors
  - *Logical* access is via a network
- Contact may vary on the *frequency*: can be *unplanned*, *random*, or it can be regular
  - *Five levels of frequency*: VH (V = Very), 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*
- Estimating *threat capability* involves looking at two factors:
  - *Skill*: knowledge and experience in severity of threat actions
  - *Resources*: people and finance to be used in threat agents
- *Five levels of resistance strength: VL, L, M, H, VH*

5.17. Likelihood assessment

The likelihood assessment is 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*

5.18. Impact assessment

The impact assessment is 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 (analysis needs to be repeated for every threat to every asset):
  - *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 factors
    - 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*
    - Reactions of secondary stakeholders may act as new threat agents (e.g., reputation, legal fees)
    - Here, magnitude and loss event frequency are measured to be *expected to materialize*

Once the loss magnitude/loss event frequency are derived, it's *straightforward to derive an estimate of risk*. This is helped by using *predefined criteria* or *matrices*, so to prioritize risks and guide treatment decisions.

- A common approach is to use a risk matrix that maps likelihood and impact ratings to corresponding risk levels, done separately for primary and secondary losses
- The two risks are then combined to determine an overall risk
- The following is a good example to consider.

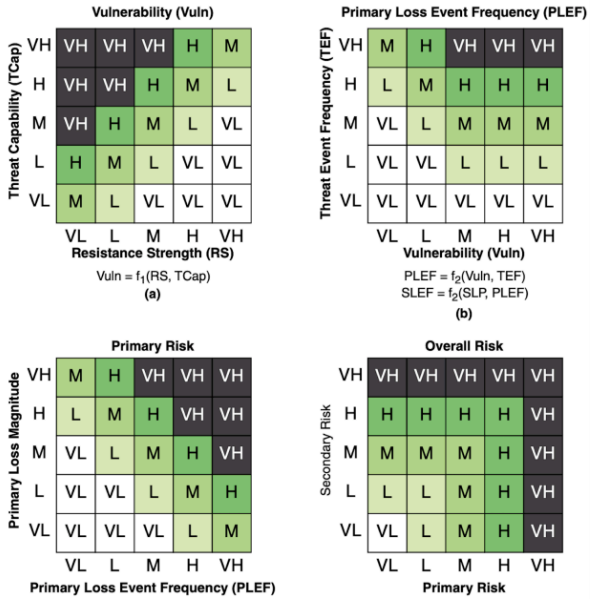

Figure 1: Risk assessment matrix to know for exam

5.19. Risk evaluation and treatment

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 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*

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

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

6.1. Threat modelling

Threat modelling is 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 levels.*

- *Think* and *find* security issues
- *Understand* security requirements
- *Develop* and *deliver* better products
- Four step process
  - What are you building? (System model/diagram)
  - What can go wrong? (Identify/find threats)
  - What should you do if things go wrong? (Mitigate/address threats)
  - Was analysis a good job? (Validate)
- Useful to create diagrams, going to the *whiteboard*, giving an *overview* and identifying *trust boundaries* and *Data Flow Diagrams (DFD)*
  - These are made of data, processes, external entities, data store and trust boundaries themselves (an example of such tool here)

6.2. 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.

- **S**poofing identity
  - *Illegally accessing* authentication information
  - Area of *authentication*
- **T**ampering with data
  - Involves the *malicious modification of data* and unauthorised changes
  - Area of *integrity*
- **R**epudiation
  - *Deny performing a malicious action*

  - Area of *non-repudiation* (users who deny performing an action)
- **I**nformation disclosure
  - Threats that involve the *exposure of information to individuals who are not supposed to have access to it*
  - Area of *confidentiality*
- **D**enial of Service (DoS)
  - Attacks that *deny service to valid users*
  - Area of *availability*
- **E**levation of privilege
  - An *unprivileged user gains privileged access* and has sufficient access to compromise or destroy the entire system
  - Area of *authorization*

Different threats affect each element type, so the threats evaluation will be subject to security analysis.

6.3. DREAD (Risk Classification)

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

- **D**amage Potential
- **R**eproducibility
- **E**xploitability
- **A**ffected users
- **D**iscoverability

Each component of DREAD is typically assigned a numerical score (e.g., on a scale of 0 to 10), and the overall risk severity is calculated based on the combined scores.

- 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 *similar software*/Invent *mitigations*
- *Accept vulnerability*

- *Address each threat*

The threat model needs to be *checked* (completely/accurately/covered/enumerating) and to be *updating the diagram* accordingly.

6.4. OCTAVE (Risk Management)

OCTAVE (Operationally, Critical, Threat, Asset, and Vulnerability Evaluation) developed by the Software Engineering Institute (SEI) at Carnegie Mellon University 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
- *Defines* essential components for a *context-driven, self-directed information security risk evaluation*

There are three variations of OCTAVE 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
   - The method is performed in a *series of workshops* conducted and facilitated by an *interdisciplinary analysis team*
   - Made up of three phases:
     - Phase 1: Identify *important information-related assets* and *threats that can interfere*
     - Phase 2: *Integrate threat analysis of previous step* and *inform mitigation decisions*
     - Phase 3: 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*
   - It is *consistent* with the OCTAVE criteria and is made up of *three similar phases* 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*

6.5. 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*:
  - *Information Security Manager (ISM)*
    - Has responsibility for the management of information security efforts
  - *Chief Information Security Officer (CISO)*
    - Has overall *responsibility* for the enterprise information security program
    - It should *communicate and coordinate* closely with key business stakeholders to address needs
    - It's the *relation between* executive management and the information security program, communicating and coordinating closely
    - *NISTIR 7359* - "Information Security Guide for Government Executives" provides a useful summary of tasks comprising *key security program areas*:
      - Security and capital planning
        - This process enables the CISO to *oversee all security projects* throughout the organization
        - It *involves three steps*:
          - Identify: *encompasses* the *research* and *documentation activities*
          - Analyze: involves an *analysis* of *requirements* and *capabilities*
          - Select: involves evaluation of *solutions proposed*
        - Also, the *cost planning is typically 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
    - The CISO should *designate* an *individual* or group responsible for monitoring and *this entity should periodically review policies* and make changes

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

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

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

7.1. Human Resource Security

The process includes many steps:

- Includes hiring, training, monitoring and handling employees
- Cybersec is *not only a technical challenge*, but also employees have to be aware of incidents and problems
- Harmful behaviors can occur, *being both malicious and non-malicious, given any action can compromise security*
- Awareness training allows people to learn basic security practice and technical fixes cannot remove vulnerabilities inherent in the workforce itself
- If an organization *doesn't have an effective awareness and training program, a problem could occur*

7.2. Hiring process

- ISO 27002 specifies the following *objective* for the *hiring process*: "to ensure 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*, investigate the accuracy of applicants' details and *arrange for experienced staff members*
- For *highly sensitive positions*, more intensive investigation is needed
- Many checks may be employed (according to the *specific country* of application): have an *investigation agency*, get a *criminal record check*, check the applicant's *credit record*
- *Employees should agree and sign the terms and conditions of their employment contract for information security*
  - The agreement *should include a confidentiality and non-disclosure agreement that accomplishes* specifically that the organization's information *assets are confidential*
  - *Confidentiality agreements put all parties on notice that the organization owns its information*
  - Each employee *has to agree to respect the policy*
  - A key aspect of clarifying the security responsibilities attached to a particular job description *is to specify the cybersecurity tasks associated with each type of job*

7.3. During and after employment

- Each job should have specific cybersec tasks associated
- Employers and contractors should be aware of responsibilities, policy and training programs - using acceptable documents and having a good ongoing awareness and training program
- Several principles for personnel security:
  - Least privilege
  - Separation of duties
  - Mandatory vacations
  - Limited reliance on key employees
  - Dual operator policy
- ISO 27002 recommends the following: "To protect the organization's interests as part of the process of changing or terminating employment"
  - In the termination process, delete all data, codes, accounts of the specific person

7.4. 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
- Cybersecurity learning continuum should be guaranteed: awareness, cybersecurity essentials, role-based training, education/certification
- All employees have security responsibilities, awareness is a program continually pushing the security messages reaching all employees, and the program must be ongoing
- Security awareness program should imclude: education/communication/security culture/behavior/responsibility/help
- According to ENISA we should have:
  - Plan/Assess/Design: must be designed with the organization mission in mind
  - Execute/Manage: activities necessary to implement an information security
  - Evaluate/Adjust: evaluation of critical components of any security awareness program

- Good communication materials should be available:
  - Both in-house
  - And externally obtained
- Communication materials and methods used to convey security awareness are at the heart of an awareness training program
  - Two options for the awareness program: use in-house materials and use externally obtained materials
- An education and certification program is targeted at those who have specific security responsibilities, often provided by outside sources and specialized training programs
- Role-based training also should encompass:
  - Manage
  - Design
  - Implement
  - Evaluate

7.5. 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
- IT hardware is disposal, which can be destruction, recycling or redistribution - it is important to securely destroy all information stored on the hardware

7.6. Office equipment

- Sensitive information processed by or stored on office equipment is subject to similar threats as to servers
- Could be also multifunction devices (MFD) - network-attached document production device that combine two or more functions
- Each contains some processing power and are attached to a network, and each is an asset to protect opportunities for threat and protection
  - Most such devices are both assets to protect and opportunities for threat. Such equipment often is not provided with the necessary security controls
- Could be exposed to several threats:
  - Network services
  - Information disclosure
  - DoS attacks
  - Physical security
  - OS security
- There is a useful checklist for MFDs provided by SANS institute

7.7. 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
- Based on the risk assessment for an office device, an organization can assign a security category to the data on the device and then use this flowchart to determine how to dispose of the memory associated with the device

7.8. Industrial Control System (ICS) security

- ICS = collective term used to describe different types of control systems and associated instrumentation
- 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 (e.g., touchscreen panels/cockpits, etc.)
  - Remote diagnostics and maintenance = Against abnormal operations or failures

  - Sensors = Measure some parameters
  - Actuators = Interact with environment to produce an effect
  - Controller = Interpret the signals and generates variables
- They are distributed in insecure locations, often with microcontrollers with limited processing power - often ICS involves widely distributed devices that may be in insecure locations
- There could be several threats:
  - Blocked/delayed flow of information
  - Unauthorized changes to instructions
  - Inaccurate information sent to system operators
  - ICS software or configuration settings modified
  - Interference with operation of equipment protection systems, safety systems and system settings

7.9. Mobile device security

- Mobile device = Portable computing and communications device
- Prior to the use of smartphones, user devices were clearly confined over defined perimeters and limited to Windows PCs
- 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
- An organization's networks must accommodate the following:
  - Growing use of new devices
  - Cloud-based applications
  - De-perimeterization
  - External business requirements
- Millions of apps are available and security of apps may vary weidely and an enterprise should perform evaluation of security of apps to determine compliance with security requirements
- 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
  - IT managers should be able to inspect each device before allowing network access
  - Rooted or jailbroken devices are not permitted on the network, and mobile devices cannot store corporate contacts on local storage

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

(On book: §10 - System Access)

8.1. System access and its functions

- Capability that *restricts access to business applications*, denying or limiting access to specific users
- Concerned with denying access to unauthorized users and limiting the activities of legitimate users
- *Functions*:
  - *Authentication*
    - *Verifying the identity* of user, establishing his identity
  - *Authorization*
    - *Granting of access* by a security administrator, based on a security policy
    - Has a database that defines the access privileges
  - Access control
    - Granting or denying specifying access requests for accessing and using information
    - Ensures access to assets is authorized and restricted
    - Has different access control policies that specify user's privileges
- 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

8.2. Authentication factors and means

- A designated security administrator is responsible for creating and maintaining the authorization database
- The administrator sets these authorizations on the basis of the security policy
- The process for authorizing should include the following:
  - Associating access privileges with *uniquely defined individuals*
  - Maintaining a *central record of access rights granted* to a user ID to access information systems and services
  - *Obtaining authorization from the owner* of the information system or service for the use of the information system or service
  - *Applying the principle of least privilege* to give each person the minimum access necessary to do his or her job

  - Assigning individual *access privileges for resources based on information security levels* and classification of information
  - *Specifying the networks and networked services to be accessed*, such as files and databases
  - Defining requirements for *expiration of privileged* access rights
  - Ensuring that *identifiers are not reused*. Deleting authorizations associated with a user ID when the individual changes roles or leaves the organization
- User authentication is the *basis for most types of access control* and the primary line of defense, including:
  - An *identification* step
  - A *verification* step
- *Authentication factors* are methods based on either something:
  - 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

8.3. Authenticators

- Means used to *confirm the identify of a user/process/device*
- Each method has problems: data may be stolen and there can be false positives/false negatives
- Can be:
  - *Multi-factor*: use of one or more authentication means and strength depends by the number of factors used
  - Password-based: use of an ID (discretionay access control, determines authorization and privileges) and a password

8.4. 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
- The server looks up the password for that ID in the password file to determine if there is a match
- Different kinds of attacks exist:
  - *Offline dictionary attacks* = compares the password hashes against hashes of commonly used passwords and if a match is found
    - Countermeasures include intrusion detection measures and rapid reissuance of passwords
  - *Specific account* = an attacker targets a specific account and submits password guesses
    - Countermeasures include account lockout mechanisms

- *Popular password attack* = use a popular password and try it against a wide range of user ID
  - Countermeasures include policies to inhibit the selection by users of common passwords
- *Password guessing against a single user* = gain knowledge about an account holder and system password policies
  - Countermeasures include training in and enforcement of password policies that make passwords difficult to guess
- *Workstation hijacking* = an attacker waits until a logged-in workstation is physically left unattended
  - Countermeasure is automatically logging out the workstation after a period of inactivity
- *Electronic monitoring* = if a password is communicated across a network to log on to a remote system
- *Exploiting multiple password use* = if different network devices share the same or a similar password
  - Countermeasures include a policy that forbids using the same or similar password
- *Exploiting user mistakes* = If the system assigns a password, then the user is more likely to write it down because it is difficult to remember
  - It can be tried using social engineering tactics that trick the user or an account manager into revealing a password. Many computer systems are shipped with preconfigured passwords
  - Countermeasures include user training

- Rely on hardware/SSO/password managers to avoid problems
- They remain the most commonly used user authentication techniques
- Reasons for the persistent popularity of passwords are:
  - Techniques that utilize client-side hardware require the implementation of the appropriate user authentication software
  - Physical tokens are expensive and/or inconvenient to carry around
  - Schemes that rely on a single sign-on (SSO) create a single point of security risk
  - Automated password managers

8.5. Hashed password and salt

- Widely used technique virtually found in all UNIX variants which combines 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 serves *three purposes*:
  - *Prevents duplicate password*
  - *Increases difficulty for offline dictionary attacks*

- Nearly impossible to *use same password for more systems*
- To mitigate the damage that a hash table or a dictionary attack could do, we salt the passwords, given the salt is *non-deterministic* (according to here)

8.6. Password cracking

- *Process of recovering secret password stored in a system*
- *Traditional approaches* include:
  - Develop a large dictionary of possible passwords
  - Each password must be hashed using each available salt
  - The cracking program tries variations on all the words in its dictionary
  - Backward spelling of words
- An alternative is to trade off space for time by *precomputing potential hash values*:
  - In this approach, the attacker generates a large dictionary of possible passwords
  - For each password, the attacker generates the hash values
  - This approach is contrasted by using a sufficiently large salt

8.7. Password file access control

- Deny the attacker access to the password file
- Allowing access only for a privileged user
- The hashed passwords are kept in a separate file from the user IDs (referred to as shadow password files)
- File can become readable or physical security might be a problem, to use a policy to force users selecting passwords difficult to guess
- There remain vulnerabilities, including the following:
  - An accident of protection might render the password file readable
  - Some of the users may have accounts on other machines in other protection domains, and they may use the same password of all of them
  - A lack of or weakness in physical security
  - Collecting user IDs and passwords is through sniffing network traffic
- Thus, a password protection policy must complement access control measures with techniques to force users to select passwords that are difficult to guess
- When not constrained, many users choose a password that is too short or too easy to guess: the goal is to eliminate guessable passwords

8.8. Possession-based authentication

- Object the *user possesses for user authentications = hardware tokens*
- *Memory cards*: have an electronic memory, store but do not process data, used alone for physical access
  - For authentication, a user provides both the memory card and some form of password or PIN
  - Potential drawbacks: special reader requirement, hardware token loss, user dissatisfaction
- *Smart tokens*: have specific physical characteristics, a user interface, an electronic interface and an authentication protocol
  - Have a smart card, a microprocessor, I/O ports accessible with a compatible reader, a co-processing circuit and some have an embedded antenna for wireless communication
- *Electronic identity cards*: national ID cards for citizens, also called *eID*, they provide stronger proofs of identity, given thy are verified by the national government
- *One-Time Password (OTP) device*: it generates one time passwords, using a seed embedded as secret, preventing the risk of guessing and reusing a password

8.9. Biometric authentication

- Based on the specific unique physical characteristics
- These include both *static* characteristics (fingerprints, hand geometry, facial characteristics, retinal and iris patterns) and *dynamic* characteristics (voiceprint, signature)
- Technically complex and expensive
- *Nature* and *requirements* of biometric features/system should be considered, being universal, distinct, permanent and collectable
- Should meet some *criteria*:
  - Performance and *required level of accuracy*
  - *Difficulty of circumventing*
  - *General acceptability* by users

8.10. Access control

Some *terms* here:

- *Access*: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge
- *Access control mechanism*: Security safeguards designed to detect and deny unauthorized access
- *Access control service*: A security service that protects against a system entity using a system resource in a way not authorized

And definitely:

- *Access control*: The process of granting or denying specific request, gaining the ability to communicate or interact with a system
  - System access deals with denying access to unauthorized users and limiting the activities of legitimate users, moderating access attempts
    - The *authentication* function establishes the identity of the user
    - The *authorization* function maintains an authorization database that defines access privileges and uses an access control policy that specifies how a user's privileges are
- Defined as two functions: $\text{Access Control} = \text{Authentication} + \text{Authorisation}$
- Has different *inputs*:
  - *Who* issued the request?
    - Better to ask the source or the process
    - The question then becomes: "For whom or for what does the process speak when it makes the request?".
  - *What* is required?
  - *What rules* apply when deciding on the application?
- *System access* deals with moderating access to system objects via authentication (establishing user identity) and authorization (defining user privileges)

8.11. Access control elements

- *Subject*
  - Entity capable of accessing objects
  - Typically considered accountable for their actions
  - There are *three classes* of subjects:
    - *Owner*: creator of a resource
    - *Group*: group of uses with granted access rights
    - *World*: the least amount of access is granted to users who are able to access the system
- *Object*
  - Resource which access is controlled and used to contain and/or receive information
  - The number and types of objects to be protected by an access control system depends on the environment
- *Access rights*
  - The ways in which a subject can access an object, including Read/Writ/Execute/Delete, etc.

8.12. Access control policies

- Dictate what types of access are permitted
- Different categories exist:
  - *Discretionary Access Control (DAC)*
    - *Based on requestor identity and on access rules*, granting specific permissions according to specific access permissions for a subject (so, discretionary)
  - *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 by enabling another
  - *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
    - Example:
      - An access by a subject to an object and the mechanism is governed by a set of rules, assesses the attributes of the subject, object and current environmental conditions to determine authorization
      - The access control mechanism grants the subject access

8.13. Access control structures

- *Access matrix* = usually sparse and is implemented by *decomposition* in one of two ways
  - Decomposition by columns, yielding *access control lists (ACLs)*
  - Decomposition by rows yields *capability tickets*
- Governed by a set of rules granting the subject access

8.14. Customer access

- It refers to *access to business applications by individuals*
- Each customer *needs to be uniquely approved and identified*, providing the customer with awareness training and education
- *Ensuring customer access to the organization's business applications meet security requirements*
- *Balance* between *customer satisfaction* and *meeting security requirements*
- Customer access remotely over the Internet or on a private network, should be *subject to the same types of technical controls*
- Authorize each customer with the process which includes defining access privileges
- Determine the authentication assurance level and *select an appropriate authentication procedure*
- It is absolutely clear to the customer that they cannot connect their own network to the organization's computer network

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

(On book - §11 - System Management)

9.1. 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 *smaller* organizations can be the security team, in *large* ones they are two separate entities
- The main goals of the CSIRT are to *minimize* risk, *contain* cyber damage, and *save money*
  - It is a good practice to review and *calculate the "value add" of the CSIRT*
  - This calculation *can be used to determine when to invest more, not only in a CSIRT, but also in operational best practices*

9.2. Security Incidents

- Any action that threatens one or more of the classic security services
- *Unauthorized access* or *modification* of information
- *Managing* security incidents involves *procedures* and *controls*:
  - Sorting, detecting, identifying, documenting

9.3. Managing, detecting and responding to incidents

- Should be detected and reported
  - *Manually* (reports by staff)
  - *Automatically* (with integrity/log tools)
- *Triage*
  - Ensure that all information designed for the *incident handling service is channeled through a single focal point (single point of contact for the whole incident handling service)*
  - Responds to incoming information by:
    - Requesting additional information in order to categorize the incident
    - Notifying the various parts of the enterprise or constituency about the vulnerability

  - Identifies the incident as either new or part of an ongoing incident

- Once a potential incident is detected, we must have *documented procedures to respond to incidents*
  - Detail/Describe/Identify typical categories, management personnel, circumstances
  - Should immediately follow a *response* to the incidents
    - What led to its occurrence
    - How this might be addressed to prevent the incident in the future
    - Details of the incident and the response taken
    - Impact on the organization's systems and their risk profile
  - Generally, a security incident reflects a change in the risk profile and this could involve reviewing the risk assessment
  - It could involve reviewing controls identified for some risks, strengthening existing controls, and implementing new controls

- *Once an incident is opened*, has to go through a number of states *until no further action is required and is considered closed*

- An example of the information flow to and from an incident handling service gives a breakdown, useful in organizing and optimizing the incident handling service and in training personnel

Security controls are in place throughout:

- Hardware
- Software
- Firmware

9.4. Malware and protection

- Malicious software (malware) is *perhaps the most significant security threat* to organizations
- NIST SP 800-83 defines it as "program covertly inserted into another program compromising confidentiality, integrity, availability"
- Malware can pose a threat to application programs, to *utility* programs, and to *kernel-level* programs
- Malware is also used on compromised or malicious *websites* and servers, or in especially *crafted spam emails*
- Many types and should be protected against them as much as possible
  - Zombie, bot
  - Ransomware
  - Spyware
  - Flooder

- Logic bomb
- Remote access trojan
- Worm
- Backdoor
- Spammer
- Keyloggers
- Scarper
- Malware as a service
- Virus
- Exploit

ENISA's annual threat report lists malware as the top cyber threat for 2016 and 2017 found:

- Businesses experienced far more malware threats
- Ransomware continues to dominate the Windows malware scene
- There is increasing threat from clickless/fileless malware
- There has been a growth of malicious functions being packaged within Potentially Unwanted Programs (PUPs)
- The adware industry is creating its own custom browsers, given they will replace your own browser

9.5. Practical malware protection

- The battle against malware is never-ending
- Malware enters through a variety of attack surfaces
- Malware is designed to avoid, attack, or disable defenses
- Organizations need to automate anti-malware actions as much as possible
  - Effective malware protection must be deployed at multiple potential points of attack
  - Enterprise endpoint security suites should provide administrative features to verify that all defenses
  - There should be systems in place to collect ongoing incident results
- IT management can take a number of practical steps to provide the best possible protection:
  - Procedures, do not grant administrative privileges, conducting regular rweviews, use filtering software, use whitelisting, monitor available logs, have backup strategies, report problems to IT security, regularly participate in security training and awareness

There are numerous open source and commercial malware protection software packages. NIST SP 800-83 lists the following as *desired capabilities in malware protection software*:

- Scanning
- Watching real-time
- Monitoring
- Scanning files
- Identifying
- Disinfecting files

Malware protection software does not provide the same level of protection against previously unknown viruses. Accordingly, you should also have in place other measures:

- Application sandboxing
- Intrusion detection software
- Awareness training
- Firewalls
- Application whitelisting
- Virtualization and container techniques

9.6. Intrusion Detection

- The sooner the intrusion is detected, the less damage can be done
- It assumes that the behavior of the intruder differs from that of a legitimate user in ways that are quantifiable
- You cannot expect that there will be an exact distinction between an attack by an intruder and the normal use of resources by an authorized user: there will be some overlap
- When an intrusion happens, confidentiality is lost on all levels and collecting information can help assessing risks and other means of security

Useful *terms*:

- *Intrusion* = Violations of security policy, usually characterized as attempts to affect the confidentiality
- *Intrusion detection*: The process of collecting information about events occurring in a computer system or network and analyzing them for signs of intrusions
- *Intrusion detection system (IDS)*: Hardware or software products that gather and analyze information from various areas within a computer or a network
- *Host-based IDS*: Monitors the characteristics of a single host and the events occurring within that host for suspicious activity

- *Network-based IDS*: Monitors network traffic for particular network segments or devices and analyzes network, transport
- *Approaches*:
  - *Misuse detection*: based on rules, take the strange behavior and consider it as normal attack, via usage of pattern-matching algorithms, operating on large databases of attack patterns, or signatures
    - It is accurate and generates few false alarms. A disadvantage it that it cannot detect novel or unknown attacks
  - *Anomaly detection*: involves searching for activity that is different from the normal behavior, is able to detect previously unknown attacks and there is a significant trade-off between false positives and false negatives
    - Again, there is some overlap in these behaviors: it catches more intruders, but leads to an increase in false negatives
- An IDS comprises *three logical components*:
  - *Sensors*: collecting data and inputs
  - *Analyzers*: receive data from sensors and support evidence providing guidance
  - *User interface*: enables a user to view output from the system or control the behavior of the system
- Techniques
  - Host-based IDS:
    - Add a specialized layer of security software
    - The primary purpose is to detect intrusions, log suspicious events, and send alerts
    - The primary benefit is that it detects both external and internal intrusions
    - For anomaly detection, two common strategies are:
      - Threshold detection
      - Profile based
  - Network-based
    - Monitor the traffic on the networks segments
    - Network-based intrusion detection involves looking at the packets on a network as they pass by some sensor (or probes)
    - Packets are considered to be of interest if they match a signature
    - Three primary types of signatures are:
    - String signatures
    - Port signatures

  - Header condition signatures
  - Inside of a NIDS:
    - A NIDS sensor sees only the packets that are carried on the network segment to which it is attached
    - A NIDS deployment is typically set up as a number of sensors distributed on key network points to passively gather traffic data and feed information
  - There are four types of locations for the sensors:
    - Outside the main enterprise firewall
    - In the network demilitarized zone (DMZ), inside the main firewall but outside internal firewalls
    - Behind internal firewalls to monitor the backbone
    - Behind internal firewalls to monitor LAN

9.7. Data Loss Prevention

- Intentional/unintentional leakage can happen in an untrusted environment (also called information leakage)
- Monitor, and protect data in use and data at rest through deep content inspection
- DLP controls are based on policy and include classifying sensitive data
- Sensitive information that is at risk of leakage or is actually leaked often includes shared and unencrypted content
- All sensitive data within an enterprise needs to be protected at all times and in all places. As a first step, an enterprise needs to define what is sensitive data and, if necessary, establish different levels of sensitive data.
- Then there is a need to recognize sensitive data wherever it is encountered in the enterprise. There are common *approaches*:
  - *Rule-based recognition*
  - *Database fingerprinting*
  - *Exact file matching*: involves computing the hash value of a file and see whether a file has been accidentally stored or transmitted in an unauthorized manner
  - *Partial document matching*: it involves the use of multiple hashes on portions of the document
- Data *states*: Key to effective DLP is to develop an understanding of the places and times at which data are vulnerable. There are three main states
  - Data *at rest* = big risk with info stored throughout the enterprise. This is a significant risk for an enterprise
    - Records may have a “home” location, but portions of that data may also migrate to other storage

  - One example of how data is replicated and proliferated is file sharing
  - The same risk exists with the many web-based collaboration
  - The fundamental task of DLP for data at rest is to identify and log where specific types of information are stored
- 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
  - Data-in-use solutions generally involve installing DLP agent software on endpoint systems
  - The agent monitors, reports, blocks, or quarantines the use of particular kinds of data files
  - The agent also maintains an inventory of files on the hard drives and removable media that is plugged in to the endpoint
  - The agent either allows or disallows certain types of removable media

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

(On book: §12 - Network and Communications)

10.1. Network models

There are 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
  - Encapsulation process of adding headers/trailers at each layer
- TCP/IP made up by 4 levels: application, transport, internet, network access
  - It's simpler than OSI and also widespread
  - Networking devices - hubs, bridges, switches, routers
  - Topologies - bus, star, ring, mesh

There are many protocols between the different levels of the two (e.g., HTTP, SMTP, DNS, etc.)

10.2. Network types, topologies and devices

- *LAN/WLAN*
  - Commonly used to describe a network of devices in a limited area (mostly using Ethernet, Token ring or fiber)
  - Most LAN networks use TCP/IP to communicate and these are owned by the companies
- *WAN*
  - Used to describe a network that spans multiple geographic locations
  - There are not owned by the companies
- *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 (some tool examples are present here and here)

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
  - Not used anymore in WLANs, substituted by switches
- 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)
  - *Routes* 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 (each one containing network *destination, remote router* and *outgoing interface* but also a *default gateway*)
  - It *does not forward broadcast by default, it breaks up both collision and broadcast domains*

10.3. Network protocols

- IP Addressing (IPv4)
  - Dedicated to everything, from unicast to broadcast and multicast, using different classes of IPs assigned by NIC (Network Information Center): special, reserved, private (not routable in the Internet)
- 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

10.4. 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.

- 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:

- *NME = Network Management Entity*
  - Software at each network node/device devoted to network management tasks
  - Collects statistics, responds to commands, provides status information
- *NMA = Network Management Application*
  - Software running on the designated network control host/manager
  - Provides the user interface to allow authorized users to manage the network
- Every other node containing an NME is referred to as *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 (EML) 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 (SML) is responsible for *adding intelligence* and automation to filtered events

10.5. Security management

Security management:

- Handles *encryption keys*, *monitors and controls access*, examines *records and security logs*, provides *facilities for protection of network resources* and applies *security policies*
- 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 (C): Only authorized individuals can access
- Integrity (I): Changes made to data are done only by authorized individuals/systems
- Availability (A): 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

Attacks methods in networks can be of all kinds: reconnaissance, social engineering, backdoors, privilege escalation, Man-in-the-Middle, covert channels, password attacks, botnets, DoS, DDoS, Internet protocols attacks.

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: travelling from one location to one another
- At rest: not travelling, it's stored into drives
- Encryption: best practice for data protection for both previous types, using cryptographic protocols like HTTPS for the transit one, or AES for the at rest one.

10.6. 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 untrusted outside the network (demilitarized)
    - DMZ has some advantages: enabling access controls to some services, blocking IP spoofing and preventing network reconnaissance
- The Admin must create *policies* for traffic
  - They should be taken on the traffic itself
- The *border router (firewall router)* 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) (some tools here and here)
  - 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) (some tools here and here)
  - 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

10.7. 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
- For Virtual Private Networks (VPNs), both authentication and encryption are generally desired:
  - Ensure that unauthorized users do not penetrate the virtual private network
  - Ensure that eavesdroppers on the Internet cannot read messages sent over the VPN

IPSec Tunnel mode is done using ESP and a key exchange function.

- For traffic offsite, through some sort of private or public WAN, IPsec protocols are use
- Tunnel mode provides protection to the entire IP packet
- Tunnel mode 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
- Host A on a network generates an IP packet with the destination address of host B on another network
- If this packet from host A to host B requires IPsec, the firewall performs IPsec processing and encapsulates the packet with an outer IP header

10.8. 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 tunneling/Traffic flow confidentiality
- Data integrity

- Data origin authentication
- Anti-replay

Some examples of VPN protocols to quote: OpenVPN (here), Wireguard (here), IPSec IKEv2.

Consider this *VPN Security Scenario*: 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 *switch 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 protected ports

Some clues about *router security*:

- *Today's router can be equipped with* firewall modules, IDS, malware scanners, using ACLs, IPSec, VPN, transparent firewall, content filtering

10.9. 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:

- *Transparent* (Layer 2)
- *Static packet filtering* (Layer 3 - Layer 4)
  - Check against rules
  - A simple packet filtering firewall must permit inbound network traffic on all these ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users
- *Application layer gateway* (Layer 3 - higher)
  - No direct communication occurs between the client and the destination server
  - Application-level gateways are more secure than packet filters. Rather than try to deal with the numerous possible combinations that are allowed and forbidden at the TCP and IP levels, the application-level gateway only needs to scrutinize a few allowable applications

  - A prime disadvantage of this type of gateway is the additional processing overhead on each connection

- *Stateful packet filtering*
  - IP address, destination IP address, the ports in use, and layer information and are stored in a stateful database on the firewall
  - Take into consideration any higher-layer context
  - A stateful inspection packet firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections. The filter allows those packets present in those directories
- *Application inspection* (Layer 7)
  - Analysis and verification of the protocols at Layer 7
- *Transparent* (Layer 2)
- *Circuit-level Gateway*
  - ‣A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host

The firewall *should*:

- Be resistant to attacks
- Be the only transit point
- Enforce the access control policy of the organization
- 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 (DMZ)

- *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*

10.10. 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, terminating all sessions, document the installation and use of remote maintenance and diagnostic links
- Reauthorize firmware codes when returned, require strong authenticators for maintenance sessions, notify remote maintenance planning, require maintenance approval, implement cryptographic mechanisms to protect the integrity and confidentiality, employ remote disconnect verification at the termination of remote maintenance

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 - Private Branch Exchange (private telephony network used inside of a company) - 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)*
  - Undesired/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 (MITM) attack*
  - The attacker secretly relays and alters the communications between two parties who believe they are directly communicating with each other

11. M3.5 - Cybersecurity Operations and Management - Logging, classification, analysis and mitigation

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

11.1. 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.*

It involves *five key steps*:

- *Plan*: inventory/assets/lifecycle
- *Discover*: monitor sources of information
- *Scan*: tools/modes/comparisons
- *Log and report*: rank vulnerabilities and log results
- *Remediate*: perform patches/metrics

11.2. Plan, discovery and scan for vulnerability

Effective management of technical vulnerabilities begins with planning. Key *aspects* of the *Plan* step include:

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 (reference here)
- Security focus: site using BugTraq (mailing list of vulnerabilities) and SecurityFocus Vulnerability Database
- Internet Storm Center (reference here)

Enterprises need to *regularly scan software, systems, and networks*. The Center for Internet Security (CIS) (reference here) 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 for the *Scan* step:

- *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*

11.3. Log, report, patch

When a vulnerability *scan is completed*, the organization should *log* the results (the *Log* step). 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

11.4. 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:

- *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*

11.5. 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*: For effective management, the log data needs to be in a common format to enable further processing
  - *Filtering*: This step includes assigning priorities to various types of events
  - *Aggregation*: The IT facility of a large enterprise generates millions of events per day; it is possible to aggregate them by categories

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

- Pattern matching: A collection of events with a given

pattern can signal a security incident

- Scan detection: Often, an attack begins with a scan of IT resources by the attacker. A substantial number of scans being found from a single source
- Threshold detection: If the number of occurrences

of a type of event exceeds a given threshold in a certain time period

- Event correlation: Correlation consists of using *multiple/particular events from a number of sources/ with known system vulnerabilities* to determine that an attack or suspicious activity occurred

11.6. Threat intelligence (CTI) 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 *threat sources* to consider:

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

- *Environmental*: Failures of critical infrastructures

The *primary purpose* of threat intelligence is to *help organizations understand the risks* (including most common or exploit, APTs - advanced persistent threats, zero-day threats):

- 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

One of the most important incident management tools is a *SIEM (Security Information and Event Management)*.

- 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
- Capabilities of a typical SIEM include data collection, aggregation, correlation, alerting, reporting, forensics, retention, dashboards

11.7. 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 systems 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 *preparation 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

Moing on with the *analysis*, *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: examples of criteria include potential damage to and theft of resources

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

11.8. 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 - Information technology:

- *Emergency*
- *Critical*
- *Warning*

- *Information*

Example of incident category and severity class includes in a table 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
  - Topics include: vulnerability/security event management, logging, threat intelligence, cyber attack protection
- *Security incident management*
  - The objective of this area is to develop a comprehensive and documented strategy for managing security incidents
  - Topics include: security incident management framework/process, emergency fixes, forensic investigations

11.9. 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*

11.10. Physical and technical security prevention and mitigation measures

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 further organized into:
  - *Environmental*
  - *Technical*
  - *Human-caused*
- *Technical* threats
  - *Electrical power is essential to run equipment* (*power* utility problems)
  - There can be power utility problems or *electromagnetic interferences (EMI)*, like *noise*

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*: limit dust entry, pest control

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*

11.11. Physical and logical security integration

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) System Model* works as follows: the *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
- Certificate-based access control systems can leverage user ID certificates for other security applications, such as document esigning and data encryption

11.12. Business continuity management

A couple of *definitions/concepts* 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 during a wide range of emergencies* 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, using vertical training and training peers
- *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: rapide recovery
  - Hardening: fortification of infrastructure
  - Redundancy: duplication of infrastructure
- Offensive measures that go beyond traditional approaches to resilience:
  - Accessibility: enable access to infrastrcuture when primary work is not accessible
  - Diversification: physical distribution of resources and implementation of diverse communication pathways
  - Automation: inclusion of self-managed hardware and software components in the infrastructure

12. M4.1 - Security Assessment and use cases - Rails, infrastructures and their standards

(This whole part is basically Soderi flexing his researches, so I only suggest to look at it with critical eye to understand what to use and what to not use)

12.1. 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, with full connectivity
- *Safety through electromechanical* devices with *COTS* (Commercial-of-the-shelf) *technology*

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*

12.2. 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*

12.3. Critical infrastructures

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

- In this category there are the electrical grid and *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 a *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

12.4. 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.

  - *ATP*: 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* 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*.

12.5. 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, defining *the need for more advanced measures to intergate security into the development process*
- The ICT systems and ICSs have a *different emphasis on confidentiality, integrity, and availability (CIA)*, being concerned with data integrity
  - ICT focuses on confidentiality to prevent stealing of private information
  - ICSs are more concerned with data integrity and avoiding unplanned outages

12.6. 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*

12.7. 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
- The cybersecurity assessment ends with a *report* with the primary objective of providing the proper network security awareness
- *The proposed methodology formulates hypotheses and assigns a risk for each threat*

12.8. Cyber ranges as tools

Cyber ranges (or *theatres*) 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

Scenarios represent particular settings of a theatre, specifying the elements, applicable rules, and selected interconnections.

- So that the participants can carry out the testing or learning activities in the desired way
- The first *benefit* we get when defining virtual scenarios is understanding *how the original system works in more detail*

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*

Once we find the vulnerabilities with the cyber range, we can fix them and give evidence of the countermeasures, creating new scenarios that don't contain them anymore.

13. M4.2 - Security Assessment and use cases - Railway sector and standards

13.1. 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
- For *OT systems*, the frameworks cited were ISA/IEC 62443, CLC/TS 50701, and the recommendations from European projects (Shift2Rail project and CYRail Project). *Those standards or approaches are often used in a complementary way to adequately address both IT and OT systems*
- *CLC/TS 50701 applies ISA/IEC 62443 to the railway sector*

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

13.2. 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

13.3. 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 traffic supervising systems*, thus leading to an urgent stop of train traffic
- *Scenario 3*: *Ransomware attack*, leading to a disruption of activity
  - An attacker infiltrates 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 travelers 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, affects the datacenter with permanent damage and IT-related activities 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

13.4. 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.

We now describe the *scope* of CENELEC TS 50701:

- 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 functions, *guaranteeing continuous security operation*

"Defense 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 SuCs*

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

Some "very very useful" reference to conclude this ~~absolutely useless~~ "absolutely wonderful" set of slides of this "amazing" course: Prof. paper, ENISA Good Practices, ENISA Zoning and Conduits

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

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

14.1. 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
- It's the part of the management system that follows a *risk-based 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* (appalti) 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/end users/auditors/shareholders/stakeholders/regulatory bodies)

- 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
- Acknowledging *what* is risky, for *who/why* and what is the *reach* of risk management is the *key*

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 goal (mapped with ISO 27001).

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"

14.2. 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 (ISO/IEC 27001 - A.5.12).

Once again, some definitions, following here the specified ISO standards (for the thousand time, I know, I suffered more than you believe me):

- 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"

14.3. 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*. 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 of both ISO 27001/27002:

- *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* as documented 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 (4-7 of the following list)
    - *Insurance (Do)* trust that the requirements will always be met and then pursue them (8 of following list)
    - *Check (Check)* identify the performances which are different from those expected (9 of following list)
    - *Continuous Improvement (Act)* has the purpose to increase performance (10 of following list)
  - *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*
    - 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…
        - The *scope* must be available as documented information
  - 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. *SoA is mentioned in the certificate*
    - This provides the controls, the reason for the inclusion and a "map" of where to find such controls
- 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

14.4. 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 ISO 27001 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*):
  1. *Organizational controls*
  2. *People controls*
  3. *Physical controls*
  4. *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*, *access* management, *classification*, *incidents*, *privacy* indications, *suppliers* management and *guidelines* for including the right amount of interaction 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

15. M6.2 - Cloud security

15.1. Cloud computing

Cloud computing (as defined by IEC here):

- 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*"

15.2. 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)

15.3. Key terms of cloud computing

Here, some definitions given by ISO/IEC 20924:2018 (Internet of Things - IoT).

- *Cloud service*
  - A cloud service is one or more *capabilities* offered via cloud computing invoked using a *defined interface*
- 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 (ISO/IEC 27018 - Information technology)
- 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*

15.4. 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)* (e.g. AWS, Azure, DigitalOcean)
  - 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)* (e.g. Heroku, Oracle Cloud, Google Cloud)
  - 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)* (e.g., Google Workspace/G Suite, Office 365, Salesforce)
  - 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) - source here.

- 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

15.5. 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 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 (the *new* one is 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*
  - 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

15.6. 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 (for more info here)
  - 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 *IaaS* solutions

15.7. 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

(From slide 28 up to 38 some "very useful" examples on how to read such matrices)

15.8. 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, describing 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.

15.9. 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 (source here) to evaluate and document their security controls
  - The privacy assessment submissions are based on the GDPR Code of Conduct (source here)

- 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 (voluntary compliance standard for service organizations), GB/T 22080-2008 (Guobiao Standards - is a Chinese national standard), or GDPR
      - Looking for a *cost-effective way* to increase assurance for cloud security and privacy

Some "very very useful" reference to conclude this ~~absolutely useless~~ "absolutely wonderful" set of slides of this "amazing" course: NIST definitions, AgID tools for cloud enabling, CSA "SECURITY GUIDANCE"

16. M6.3 - Personal data processing

16.1. Personal data and definitions

- Privacy
  - *The state of being alone*, or the right to keep one's personal matters and relationships secret. A *fence* would give us more privacy in the backyard - Cambridge University
  - *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 - ISO/IEC 24775-2:2014 - Storage management*
  - The value of the information we have is something which we have to protect at all costs

16.2. Privacy law

- *Why is privacy so important*?
  - The protection of *natural persons* in relation to the processing of personal data is a *fundamental right*
  - According to Article 8 of Fundamental Rights of EU and Treaty on the Functioning of EU, *everyone* has the *right* to the *protection of personal data concerning him or her* (GDPR - Recital 1)

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* (ISO 29100:2011 - Privacy management)
- 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 boundaries, 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

16.3. Privacy laws and certification

- Europe
  - *Reg. (UE) 2016/679 European General Data Protection Regulation - GDPR* (which basically applies to european citizens personal data)
    - 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 other ones to quote:
  - *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*: 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

16.4. GDPR definitions

GDPR reports, in various articles, the following statements:

- "*Personal data*" means any information relating to an identified or identifiable natural person
  - "*Data subject*" → "PII principle" in the ISO/IEC 29100″
  - 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. (GDPR - Art. 4)
- 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 (GDPR - Art. 9)
  - Personal data which are, by their nature, *particularly sensitive* in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms (GDPR, Recital 51)

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 (according to article 4):

- "*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. making available, alignment or combination, restriction, erasure or destruction (GDPR - Art. 4)
  - 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. (GDPR - Art. 4)
- "*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* (GDPR, art. 14).

- *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)

Consider "*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 organizational measures
   - (a) the *pseudonymization* 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 organizational measures* for ensuring the security 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

16.5. 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 - source here

How do they work? *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*

16.6. 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 improving a *Privacy Information Management System (PIMS)* in the form of an *extension to ISO/IEC 27001 and ISO/IEC 27002* for privacy management within the context of the organization
  - 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
  - *Structure* of the standard:
    - 6.2 Information security policies, 6.3 Organization of information security, 6.4 Human resource security, 6.5 Asset management, 6.6 Access control, 6.7 Cryptography, 6.8 Physical and environmental security, 6.9 Operations security, 6.10 Communications security, 6.11 Systems acquisition, development and maintenance, 6.12 Supplier relationships, 6.13 Information security incident management, 6.14 Information security aspects of business continuity management, 6.15 Compliance…
    - *7 Additional ISO/IEC 27002 guidance for PII controllers*
    - *8 Additional ISO/IEC 27002 guidance for PII processors*

  - ...
  - Annex C - Mapping to *ISO/IEC 29100* and Annex E - Mapping to *ISO/IEC 27018*
- Basically, we are describing: 4 - Context of the organization (with additional requirements) and 6 - Planning (with additional requirements)
- 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*
- Some additional guidance refers to information security policies, organization of information security, access control, etc.

- *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

16.7. 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

Notes of circumstance for maniacal people like me:

- ISDP: This could stand for "Information Security and Data Protection" or "International Standard for Data Protection."
- SGCMF: This might stand for "Standard for General Compliance in Medical Files" or "Security and Governance Compliance for Medical Files."

Moving on:

- *UNI / PDR 43 - Management of personal data in the ICT field*
  - The accredited certification is issued in accordance with the UNI 43: 2018 Reference Practice "Guidelines for the management of personal data *in the ICT field* according to EU Regulation 679/2016 (GDPR)", and is 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 accredited certification is issued in accordance with UNI 11697 "Non-regulated professional activities - Professional profiles relating to the processing and protection of personal data - *Requirements for knowledge, skills and competence" to the professional Data Protection Officer (DPO)*, the person responsible for data protection introduced by the GDPR
  - The standard defines the professional profiles relating to the processing and protection of personal data in accordance with the definitions provided by the EQF (European Qualifications Framework) and provides for a series of specialized figures for the business management of all aspects relating to privacy

Some "very very useful" reference to conclude this ~~absolutely useless~~ "absolutely wonderful" set of slides of this "amazing" course: GPDR (full text), Register of certification mechanisms, seals and marks (from European Data Protection Board), Italian Supervisory authority website

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

17.1. 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 (many of the following parts have as reference this site:

- Developed by Uptime Institute (source for industry tier certification in data center design), it 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, costs, sustainability, and uptime*
- 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
- They have three key features:
  - *Flexible* (compliant with codes/regulations)

Lifecycle (covers all organization phases)

- *Certification* (administered by the author of the standard itself)

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 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 I - 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 II - Redundant capacity*
  - The 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 III - Concurrently maintainable*
  - 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 IV - Fault tolerant*
  - A Tier IV data center has *several independent* and *physically isolated* systems 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*

More specific resources are available here.

17.2. NIST Framework

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including *industry, government, academia, and nonprofit* — to manage and reduce their cybersecurity risks (source here).

- It is useful regardless of the *maturity* level and technical sophistication of an organization's cybersecurity programs

- Nevertheless, the CSF *does not embrace a one-size-fits-all approach*. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions
- By necessity, *the way organizations implement the CSF will vary*

It includes the following *components*:

- CSF *Core*, the nucleus of the CSF, which is a *taxonomy* of high-level cybersecurity *outcomes* that can help any organization *manage its cybersecurity risks*
  - The CSF Core components are a *hierarchy of Functions, Categories, and Subcategories* that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise
  - Because the outcomes are *sector-, country-, and technology-neutral*, they provide an organization with the flexibility needed to address its *unique risks, technologies, and mission considerations*
- CSF Organizational *Profiles*, which are a mechanism for describing an organization's *current* and/or *target cybersecurity posture* in terms of the CSF Core's outcomes
- CSF *Tiers*, which can be applied to CSF Organizational Profiles to *characterize the rigor of an organization's cybersecurity risk governance and management practices*
  - Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks

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*: Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps
- *Prioritize*: Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations
- *Communicate*: Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations

17.3. CINI – Consorzio interuniversitario nazionale per l'informatica

The following is more of an italian use case; CINI has improved the Framework Core by introducing (source here):

- New categories and subcategories dedicated to *data protection* topics (in its Section 4.1)
- *Contextualization Prototypes*, a new *tool* that supports and facilitates the definition of contextualizations (in its 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 take 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

17.4. EU strategies and NIS directives

Regarding cybersecurity, different EU strategies exist (source here):

- 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*
    - 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 Resilience 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.

17.5. New challenges 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 (source here).

- 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 - meaning that *all medium and large companies in selected sectors will be included in the scope*
- 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 *important* categories 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 harmonizing 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

Some “very very useful” reference to conclude this ~~absolutely useless~~ “absolutely wonderful” set of slides of this “amazing” course: ENISA website, Nist cyberframework, Nist Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, Cybersecurity national lab, Nis Directive full text Directive (EU) 2016/1148

18. M6.5 – NIST CSF Laboratory (Useful for the report not for exam)

This is a laboratory held at the end of April/beginning of May in order to help write the report for the exam. Basically (for this year - 2023/2024), you let the AI do the main work and comment the result. I would also simply say this: this was the only useful lesson for this "course" and was not even made by the professor, but more intended as collaboration in pairs and discussion. Amazing stuff, I know.

18.1. How to read the NIST CSF

This document is version 2.0 of the NIST Cybersecurity Framework (Framework or CSF). Recall from the previous lesson (6.4) the following components, depending on the risk level the organization needs to face:

- CSF Core, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks
  - The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome
  - These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise
  - Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations
- CSF Organizational Profiles, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes
- CSF Tiers, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices
  - Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks

By itself, the Framework provides a common taxonomy and mechanism for organizations to:

- 1) Describe their current cybersecurity posture
- 2) Describe their target state for cybersecurity
- 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- 4) Assess progress toward the target state
- 5) Communicate among internal and external stakeholders about cybersecurity risk

The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives.

- Ideally, organizations using the Framework will be able to measure and assign values to their risk along with the cost and benefits of steps taken to reduce risk to acceptable levels

- The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be

18.2. How to use the Framework in the laboratory assessment

The simulation that we will do for the purposes of both the laboratory and the exam will not be able to consider all the real factors encountered in a real organization.

- Some activities, such as risk analysis, for example, involve carrying out interviews with top management capable of quantifying the impacts and the whole process of risk analysis itself, especially the quantitative kind, can even require months of work
- Nonetheless, the exercise is useful to understand, learn and familiarize yourself with daily used tools for cybersecurity workers within the organizations, developing, where appropriate, an approach to recognizing risks at a glance
- To better understand the security controls, you can use examples described in this Reference Tool offered by NIST for each subcategory
- It might be important to include historical events over the application

In specific, consider the following steps:

- Step 0. Take a quick read at the categories and sub-categories of the NIST CSF 2.0
  - Take a brief look at the Framework (.pdf) and in particular, chapters 3 and 4.0
- Step 1. Choose a use case. Assume an organization. Some examples of organizations are as follows:
  - A hospital
  - A bank or financial institute
  - An energy supply company
  - A public administration (of various kinds)
  - A Telecommunication company

Start describing a drafted organization chart, stakeholders, assets, risks and opportunities (some examples follow). Use generative AI to help create a realistic and unique organization chart and/or draw inspiration from the following

- Step 1. Drafted organization chart for a hospital:
  - a) CEO/President
  - b) Medical Director
  - c) Department Heads (Surgery, Medicine, Pediatrics, Radiology, etc.)
  - d) Nursing Director
  - e) Human Resources

    - f) Finance and Administration
    - g) Patient Services
    - h) Information Technology
    - i) Quality Control
- Step 1. Drafted organization chart for an Energy Supply Company:
    - a) CEO/President
    - b) Operations Manager
    - c) Engineering and Design
    - d) Project Management
    - e) Finance and Accounting
    - f) Human Resources
    - g) Environmental and Regulatory Compliance
    - h) Information Technology
    - i) Customer Service
- Step 1. Drafted organization chart for a Public Administration:
    - a) Mayor/Chief Executive Officer
    - b) Department Heads (Public Works, Parks and Recreation, Finance, Health, etc.)
    - c) Attorney/Legal Affairs/Regulation office
    - d) Human Resources
    - e) Planning and Development
    - f) Public Relations (external communication. E.g. press interaction)
    - g) Information Technology
    - h) Economic Development
    - i) Community Services
- Step 1. Drafted organization chart for a Telecommunication Company:
    - a) CEO/President
    - b) Chief Technology Officer
    - c) Sales and Marketing Department
    - d) Human Resources
    - e) Information Technology

  - f) Network Operations
  - g) Customer Service
  - h) Finance and Accounting
  - i) Engineering and Design
- Step 2. AI driven Risk analysis. Use generative AI to perform an assessment for the chosen Organization.
  - Utilize prompts that reference the NIST CSF 2.0. The assessment should evaluate the current security posture and risk, including examples from at least five to no more than ten specific subcategories
  - The AI should consider the sub-categories among the most significant for the audited Organization (where usually related risk in higher), and the relative gaps that it is possible to find.
  - It can be helpful to refer to multiple controls within the same category, for ease of presentation and consistency, but try choosing multiple categories for greater completeness and cross-disciplinary exercise.

Some considerations:

- "The non-implementation of the control (sub-category) arises a risk. Which one?"
- "N.B. Risk is usually higher in the areas that are closer to the core business or to the main activities carried out by the specific organization, or represent the prerequisite for their achievement"

Moving on:

- Step 3. Human Risk analysis and assessment.
  - Using the concepts and examples seen in the course, following a risk assessment procedure for the chosen use cases, which are the most risky areas and activities from the point of view of information security and cybersecurity?
    - Did the AI address them correctly? What can be added or integrated? Are there any specific, additional, or different examples you would provide? Write them as a comment
    - Think about the type of data processed, the purposes, the type of services provided and the consequences of an interruption (due to any event or threat) of the service or the loss of confidentiality, integrity or availability of information for all the stakeholders
    - What could go wrong for the specific organization?
  - To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of technology is required
  - Because each organization's risks, priorities, and systems are unique, the tools and methods used to achieve the outcomes described by the Framework will vary
- Step 4. Having determined the current implementation status, decide the minimum level to reach (in terms of Tiers from 1 to 4, according to the scale offered by NIST CSF 2.0, on pages 8-11)
  - You now have a gap between your current state and your desired level

- Choose the desired levels of implementation for each area considered (5 to 10 areas, according to Step 2). Now you have drafted a profile for the controls for the specific organization
- Explore why the current state isn't secure, what risks the organization is exposed to, and why it's good to implement certain controls, prioritizing each based on the risk highlighted, utilizing both the AI written report and your comment
- Report assessment for an organization, for the purposes of the laboratory, could be around 500 words

19. 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

19.1. ISO / IEC 15408 - Common Criteria (Evaluation Criteria for IT Security)

- 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 - CC, currently considered the most reliable (transposed by the ISO / IEC 15408 standard) - actual is of April 2022, Release 1
  - Their goals is to develop confidence and trust in the security characteristics of a system and in the processes used to develop and support it
  - Specifically, use the following:
    - "Secure" to do *what* (security *goals*)
    - "Secure" in which *context* (security *environment*)
    - "Secure" against which *checks* (*assurance* requirements)
  - CC have the following structure (coming from here:
    - *Part 1 - Introduction and general model*: This 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*: This 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 organizes them in *families and classes*
    - *Part 3 - Security assurance components*: This 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 organize them into *families and classes*
      - It also defines evaluation criteria for PPs (Protection Profiles) and STs (Security Targets) and presents seven pre defined 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 documentation used during analysis/ 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* (source here)

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

19.2. Federal Information Processing Standard (FIPS) 140-2 - Security Requirements for Cryptographic Modules

Federal Information Processing Standard (FIPS) 140-2 is one of the main standards 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

19.3. Federal Information Processing Standard (FIPS) 140-3 - Security Requirements for Cryptographic Modules

On March 22, 2019, the Secretary of Commerce approved FIPS 140-3 - see here, which supersedes FIPS 140-2.

- FIPS 140-3 aligns with ISO/IEC 19790:2012(E) and includes modifications of the Annexes that are allowed to the Cryptographic Module Validation Program (CMVP) - see here, as a validation authority
- The testing for these requirements will be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2
- Major changes in FIPS 140-3 are limited to the introduction of non-invasive physical requirements

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

19.4. 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 (Information Technology Security Evaluation Criteria) 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

19.5. 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

Consider the *National Assessment and Certification Center*:

- 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*

But also *tasks* and *functions* (source here):

- The CVCN have the task of carrying out *preliminary* checks on the assignment procedures and may impose conditions and tests aimed at security analysis of hardware/software on some components of the supply that may be particularly sensitive if compromised

19.6. 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* (source here):

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

Now we will discuss *who issues the certificate and how to obtain the PCI DSS.*

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

Now we will discuss *the requirements of a PCI DSS 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 other information 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

To add context for you, I take this from the Wikipedia page of the standard. The PCI DSS has twelve requirements for compliance, organized into six related groups known as control objectives:

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access-control measures
- Regularly monitor and test networks
- Maintain an information security policy

Each PCI DSS version has divided these six requirement groups differently, but the twelve requirements have not changed since the inception of the standard. Each requirement and sub-requirement is divided into three sections:

- PCI DSS requirements: Define the requirement. The PCI DSS endorsement is made when the requirement is implemented.
- Testing: The processes and methodologies carried out by the assessor for the confirmation of proper implementation.

- Guidance: Explains the purpose of the requirement and the corresponding content, which can assist in its proper definition.

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

To conclude:

- At a high-level overview, it checks all the functions, from maintaining a secure network up to protect data and go against vulnerabilities
- 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 *other* information pertinent to each requirement

Some "very very useful" reference to conclude this ~~absolutely useless~~ "absolutely wonderful" set of slides of this "amazing" course: Common Critera - Part 1, 2 and 3, NIST FIPS 140-3, OCSI - Definitions, Agenzia per la cybersicurezza nazionale, PCI DSS - at a glance,PCI DSS - document library

20. 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.

20.1. 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, which has now became *regular*.
- Remote working or real smart working accentuate even more the importance of digital skills in the performance of work
- 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

20.2. e-CF

European e-Competence Framework (e-CF) is a reference framework of ICT *competencies* that can be used and understood by ICT users 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 can be integrated as examples in the description of knowledge and skills

We give some definitions related to e-CF (taken by the User Guide of application here:

- *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 competencies* 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 relational capacity" (e.g. analysis capacity, synthesis capacity, flexibility, pragmatism…). If skills and knowledge are the components, attitudes are the *glue*, which keeps them together

e-Competence *proficiency levels* "Level" is another basic concept used within the European e-Competence Framework (which is identified in the e-CF *Dimension 3*).

- In the e-CF this concept refers to "proficiency" levels instead of "learning" levels in the EQF (European Qualifications Framework)
- This is another reason why e-CF levels are different from the EQF levels, even though strong relationships can be found
- A proficiency level *integrates three facets*: *context complexity, autonomy and behavior*. Hence, the proficiency levels described in Dimension 3 *embed these three* components

All these dimensions are also present and easily identifiable within the *EQF* definitions and descriptions. This maintains a uniform relationship between the two frameworks. In particular, in the e-CF, these three dimensions can be summarized as following:

- *Autonomy* ranges between "Responding to instructions" and "Making personal choices"
- *Context complexity* ranges between "Structured –Predictable" situations and "Unpredictable – Unstructured" situations
- *Behaviour* here represents an observable outcome of attitude and ranges between "the ability to apply" and "the ability to conceive"
- Consider the EQF in annex 2 of the e-CF compares European e-CF and EQF levels

The European e-Competence Framework is structured from *four dimensions*. These dimensions reflect different levels of business and human resource planning requirements in addition to job / work proficiency guidelines and are specified as follows:

- Dimension 1:
  - 5 e-Competence areas, derived from the ICT business processes
    - PLAN – BUILD – RUN – ENABLE – MANAGE
- Dimension 2:
  - A set of reference e-Competencies for each area, with a generic description for each competence
    - 40 Competencies identified in total provide the European generic reference definitions of the e-CF 3.0

- Dimension 3:
  - Proficiency levels of each e-Competence provide European reference level specifications on e-Competence Levels e-1 to e-5, which are related to the EQF levels 3 to 8
- Dimension 4:
  - Samples of knowledge and skills relate to e-competencies in dimension 2. They are provided to add value and context and are not intended to be exhaustive

Whilst competence definitions are explicitly assigned to dimension *2* and *3* and *knowledge* and *skills* samples appear in dimension 4 of the framework, *attitude* is embedded in *all three dimensions*.

- A general overview of it encompasses all competencies and proficiency levels fairly precisely
- In its full version, all dimensions and levels are fully encompassed. You can find a visual overview here in case

20.3. NICE Framework

NIST Special Publication 800-181 revision 1, the Workforce Framework for Cybersecurity (NICE Framework - see here), provides a set of *building blocks* for describing the tasks, knowledge, and skills that are needed to perform cybersecurity work performed by *individuals* and *teams*.

- Through these building blocks, the NICE Framework enables organizations to develop their workforces to perform cybersecurity work, and it helps learners to explore cybersecurity work and to engage in appropriate learning activities to develop their knowledge and skills
  - This publication from the National Initiative for Cybersecurity Education (NICE) constitutes a fundamental reference for describing and sharing information about cybersecurity work
  - It expresses that work as Task statements and describes Knowledge and Skill statements that provide a foundation for learners including *students, job seekers, and employees*. The use of these statements helps students to develop skills, job seekers to demonstrate competencies, and employees to accomplish tasks
  - As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to *identify, recruit, develop, and retain* cybersecurity talent

The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity education, training, and workforce development.

- *Keywords* for the framework are: Competency; cybersecurity; cyberspace; education; knowledge; role; security; skill; task; team; training; workforce; work role

The “building blocks” approach uses the following:

- The “work” is what an organization needs to achieve cybersecurity risk management objectives. Every organization executes common tasks as well as some context-unique tasks
  - For example, every organization has some form of management tasks, whereas only some organizations have tasks to “deploy bulk energy systems securely”

    - The NICE Framework provides organizations a way to describe their work through Task statements that group supporting Knowledge and Skill statements

- The "learner" is the person who has knowledge and skills. The term learner applies to all people within the scope of this document. A learner can be a student, job seeker, employee, or other people within the workforce

    - In an organizational context, learners execute tasks. In an educational context, learners acquire *new knowledge and skills*

    - All individuals are considered learners due to education or training they received prior to entering the workforce, ongoing training, self-learning, or a career progression plan

The NICE Framework provides organizations with a way to describe learners by *associating Knowledge and Skill statements to an individual or group*. By using their Knowledge and Skills, learners can complete Tasks to *achieve organizational objectives*.

- While not all organizations will use every concept pertaining to learners, the NICE Framework provides organizations with a flexible set of building blocks to use as needed by their unique context

- The recognition of the role the learner plays in developing capabilities to perform cybersecurity work also reinforces the applicability of the NICE Framework to education and training providers

- By describing both the *work* and the *learner*, the NICE Framework provides organizations a *common language* to describe their cybersecurity work and workforce

- Parts of the NICE Framework describe an organizational work context (Tasks), other parts describe a learner context (Knowledge and Skill), and finally, the building block approach of the NICE Framework allows organizations to link the two contexts together

- Furthermore, the NICE Framework provides *a mechanism to communicate across organizations* at all levels (e.g., *peer*, *sector*, *state*, *national*, *international*, etc.). This can drive innovative solutions to common challenges, lower barriers for new organizations and individuals, and facilitate workforce *mobility*

The NICE framework has different attributes used as resources describe the cybersecurity work their organization does, the people who will carry out the work, and the ongoing learning that will be needed to do that work effectively.

The nature of the work, and consequently, the workforce, can be described using the *TKS (Task, Knowledge and Skill) building blocks* presented in the following sections, incorporating the following attributes:

- *Agility - People, processes, and technology* mature and must adapt to change. Therefore, the NICE Framework enables organizations to keep pace with a constantly evolving ecosystem

- *Flexibility* — While every organization faces similar challenges, there is no one-size-fits-all solution to those common challenges. Therefore, the NICE Framework enables organizations to account for the organization's unique operating context

- *Interoperability* — While every solution to common challenges is unique, those solutions must agree upon consistent use of terms. Therefore, the NICE Framework enables organizations to exchange workforce information using a common language

- *Modularity* — While cybersecurity risk remains the basis of this document, there are other risks that organizations must manage within the enterprise. Therefore, the NICE Framework enables organizations to communicate about other types of workforces within an enterprise and across organizations or sectors (e.g., privacy, risk management, software engineering/development)

Task statements describe the *work*, while Knowledge and Skill (K&S) statements describe the *learner*. They should focus on the organizational language and communication patterns that provide value to the organization and are designed to describe work to be done aligned with the context of the organization.

- They describe *work to be completed*. A task can be defined as an activity that is directed toward the achievement of organizational objectives, including business objectives, technology objectives, or mission objectives
- They should be *straightforward*. While the work encompassed within a Task statement may have many steps, the statement itself is easy to read and understand

Knowledge statements relate to Task statements thanks only to the understanding described by the Knowledge statement will the learner be able to complete the Task.

- Knowledge is defined as a retrievable set of concepts within memory. Knowledge statements may describe either *foundational or specific* concepts
- Multiple Knowledge statements may be needed to complete a given Task. Likewise, one Knowledge statement may be used to complete many different Tasks

Skill statements relate to Task statements in that a learner is demonstrating skills in performing tasks. A learner who is not able to demonstrate the described skill would not be able to complete the Task that relies on that skill.

- A Skill is defined as the capacity to perform an observable action. Skill statements may describe *straightforward or complex* skills
- Multiple Skill statements may be needed to complete a given Task. Likewise, exercising a Skill may be used to complete more than one Task

Users may also create *entirely new* Task, Knowledge, or Skill statements to help tailor the use of the NICE Framework for *local use* within their unique context. Such statements will help support consistent internal discussions regarding learners and their work activities.

Competencies provide a mechanism for organizations to assess learners. Competencies are defined via an employer-driven approach that provides insight to an organization's unique context.

- They allow education and training providers to be responsive to employer or sector needs by developing learning experiences that help learners develop and demonstrate the Competencies
- They consist of a *name, description of the Competency, assessment* method, as well as a group of associated *TKS statements*
- Other organizations could use Competencies to determine *whether a learner has achieved a defined set of Skills and Knowledge*

- These organizations could choose to use Competencies as groups of K&S statements and then assess the learners for these K&S statements. Assessments could take the form of *tests, lab-based demonstration, or oral evaluations*

Work Roles are a *common use case* of the NICE Framework and are a way of describing a grouping of work for which someone is responsible or accountable.

- While previous workforce frameworks also associated Work Roles with Knowledge, Skill, and Ability specifications, the NICE Framework encourages a more agile approach through Tasks
- Work Roles *are composed of Tasks that constitute work to be done*; Tasks include associated Knowledge and Skill statements that represent learners' potential to perform those Tasks. This transitive approach, supports flexibility and simplifies communication
- A *Work Role-centered approach* to building teams allows organizations to define what types of Work Roles are needed to achieve defined objectives
- Since Work Roles are themselves made up of Competencies, this approach to building teams starts with the work to be completed. This approach may be considered "*top down*"

Teams can also be *built using Competencies*.

- This approach to building teams recognizes that individual Tasks may be unknown, but the types of Competencies needed to solve the challenge are known
- This approach may be considered "*bottom up*". Therefore, teams built this way can help identify learners who may participate in the Team's work in the future
- These learners may or may not be associated with a Work Role and simply possess the Competencies needed to help meet organizational objectives

Concluding:

- Through the application of the building block approach described by the NICE Framework, users can benefit from a consistent method for organizing and communicating the work to be done via Task statements and the Knowledge and Skills of individual learners who support that work.
- The NICE Framework *helps guide the efforts of employers to describe cybersecurity work, education and training providers* to *prepare cybersecurity workers*, and learners to demonstrate their capabilities to perform cybersecurity work
- The ability to describe Tasks, Knowledge, and Skills is important to ensure a comprehensive understanding of the work and the workforce.
- The NICE Framework provides an extensible reference resource that can be applied and used by various organizations or sectors to describe the work to be performed in many areas

20.4. AgID guidelines

AgID - Agency for Digital Italy, acknowledging the provisions of the "2014-2020 digital growth strategy promotes the use of the e-CF 3.0 model and related profiles".

- LINEE GUIDA per la qualità delle competenze digitali nelle professionalità ICT ("GUIDELINES for the quality of digital skills in ICT professionals") apply the e-CF framework and related concepts to the world of public procurement

They have the following *purpose*:

- Provide the administrations with indications on *how to integrate* the provision of professional services in the context of *ICT service contracts*
- Provide cross-cutting information whenever it is necessary to deal with issues relating to the use of professionals
- Make it possible to clearly identify the regulated ICT professional profiles with related skills and competencies. Give suggestions and create a common lexicon to facilitate and simplify the relationship between public administration and suppliers

They offer the following *advantages*:

- An overall reference framework for public procurement of ICT services by administrations
- *Quantitative* methods to be applied to *define quality measures* and *identify measurement processes*, in order to provide concrete, pragmatic, immediately applicable indications, both to contracting administrations and to bidders

Adequate *clauses*, to be used in the negotiation phase when defining contracts in ICT sector, relating to the description of the activities to be contractually envisaged, to the products that these activities produce (contractual deliverables), quality indicators and measures to refer to both activities and products.

- Clauses that are subsequently useful in the implementation phase of ICT contracts, for the necessary management of the contract and the monitoring to verify compliance with contractual requirements in terms of time, costs and work progress, expected quantity and quality of ICT services required
- *Evolution and technical standardization* of profiles according to the needs of the market to ensure the recognition of skills

Some "very very useful" reference to conclude this ~~absolutely useless~~ "absolutely wonderful" set of slides of this "amazing" course: e-CF Explorer, Workforce Framework for Cybersecurity (NICE Framework), AgID guidelines and resources

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

21.1. Cyber Career Pathways Tool

The NICE framework defines *52 roles* (see here), divided into categories and specialty areas. The Cyber Career Pathways Tool is an interactive *online tool* for professionals, employers, and students (recent grads) to explore and build career roadmaps based on the NICE Framework.

- Users can select up to *five* work roles to learn more about their shared *skillsets*, alignment to the Cyber Skill *Communities*, or related *specialization* and *functions*
- The Cyber Career Roadmap highlights the mobility between these connection points to help you and others determine the next steps in your career progression and skillset development
- The tool also offers recommended on/off-ramps (i.e. steppingstones) and secondary work roles to consider and pursue in your career roadmap
- You can see and browse different job positions and see their level of detail, seeing the corresponding entries for how much knowledge is actually required (entry, intermediate, advanced), categorized by a legend accordingly

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

DoD Directive 8140, signed August 2015, establishes a definition for the *cyber workforce* and outlines Component roles and responsibilities for the management of the *DoD cyber workforce* (source here).

DoDD 8140 provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an *approved certification* for their particular job classification.

- This was a replacement of 8570.01-M whose guidance and procedures is still in effect
- The individuals who hold these work roles are required to carry an *approved certification* for their job classification
- This directive *affects* any full- or part-time military service member in the U.S., contractor, or local nationals with privileged access to a DoD information system performing information assurance (security) functions
- DoDD (Department of Defense Directive) 8140 *requires* the following (see more here:
  - All personnel performing Information Assurance Technical and Information Assurance Management functions must be certified
  - All personnel performing CSSP (Cyber Security Service Provider) and IASAE (Information Assurance System Architects and Engineers) roles must be certified
  - All IA jobs will be categorized as “Technical” or “Management” Level I, II, or III, and to be qualified for those jobs, you must be certified

21.3. Cyber Career Pathways DoDD 8140/8570

As an extension of the DoD 8570.01-Manual, some certifications have been approved as IA baseline certifications for the IA Workforce.

- Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level
- Refer to Appendix 3 of 8570.01-M for further implementation guidance here

This information was developed in partnership with the Interagency Federal Cyber Career Pathways *Working Group* (WG) - more here. The WG is dedicated to developing cyber career resources, including career pathways for NICE Framework work roles for use throughout the *Federal Government*, as well as *private industry and academia*.

- The DoD Cyber Workforce Framework (DCWF) establishes the DoD's authoritative lexicon based on the *work* an individual is performing, not *their position titles*, occupational series, or designator
- The DCWF describes the *work* performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01
- The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS)

21.4. NIST-NICE Framework and DoDD 8140/8570

Part of the confusion some have between these two frameworks is the entangled origins the two have. Firstly, the NICE Framework provides a *baseline for federal cybersecurity* but it is a non-binding baseline.

- In practice, the NICE Framework is used as a starting point for *federal agencies*
- Next, what makes this confusing is the fact that the DoD Cyber Workforce Framework (DCWF) was defined in both DoDD 8140 and the NICE Framework (source here)
- To top off the confusion level, some jobs bleed into other jobs, which can ultimately cause security vulnerabilities
- The biggest difference between the NICE Framework and DoDD 8140 is their intended audience, or users and *stakeholders*
- The NICE Framework is intended for a broad *range of federal government employees*, from the GSA to the FBI. DoDD 8140 *is intended for United States military users and stakeholders*

This may seem like a slight difference, but it has a *huge impact* on how these frameworks operate. The NICE Framework and DoDD 8140's differences are best viewed through the lens of the seven categories of the NICE Framework because of the different intended audiences.

Let's take a look at how these framework's categories differ:

- *Analysis*: NICE focuses on the acts of cybercriminals and 8140 focuses more on foreign intelligence agencies and foreign actors
- *Collect & Operate*: 8140 focuses on counterintelligence and NICE has a counter-criminal focus
- *Investigate*: NICE focuses on locking cybercriminals up and 8140 focuses on building developed and detailed target packages for future use
- *Oversee & Govern*: 8140 places more emphasis on certification because it is more "baked in" for other federal agencies
- *Securely Provision*: The biggest difference here is that 8140 has built out the Secret Internet Protocol Router Network (SIPRNet)
  - While other federal agencies have secure networks, the *heightened* need for a secure network on the battlefield has given this category more *emphasis* for DoDD 8140

21.5. ENISA

The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to *achieving a high common level of cybersecurity across Europe*.

- ENISA contributes to EU cyber *policy*, enhances the trustworthiness of *ICT products*, services and processes with cybersecurity *certification* schemes, cooperates with Member States and EU *bodies*, and helps Europe prepare for the future cyber challenges
- It states that the cybersecurity workforce *shortage* and *skills gap* is a major concern for both economic development and national security, especially in the rapid digitization of the global economy
- It poses threats with a high impact on the data, information technology systems and networks that form the dorsal spine of *modern societies*
- This shortage can be further analyzed into two concurrent issues: a *quantitative* one and a *qualitative* one.
  - The *quantitative* issue is related to the insufficient supply of cybersecurity professionals to meet the requirements of the job market
  - The *qualitative* one is related to the inadequacy of professional skills to meet the market's needs

The European Cybersecurity Skills Framework aims to create a common understanding of the *roles, competencies, skills* and knowledge used by and for *individuals*, *employers* and training providers across the EU Member States, in order to address the cybersecurity skills shortage.

- Additionally, it will help to further facilitate cybersecurity-related skills recognition and support the *design* of cybersecurity-related training programs for skills and career development
- Consequently, the European Cybersecurity Skills Framework will boost employment and employability in cybersecurity-related positions

- Basically, for each role, there is:
  - Profile title (comprehensive of skills/tasks/mission/deliverables/competencies)
  - Job title (describing for each of the previous the precise information)

During the development of the Framework, there were few principles which were considered to be applied:

- The Framework should fit to European landscape of standardization and legislation.
- The European Norm (EN) 16234-1 European *e-Competence Framework (e-CF)* was selected as a *reference point*. Upcoming Cybersecurity Skills Framework will follow the construction approach of the above-mentioned norm.
- The Framework should be *simple* and made for use of SME's (small / medium enterprises) or other non-professionals in the field. This will be reflected in the limited number of profiles.
- The Framework should include only cybersecurity *specific competencies and skills*. General capabilities will not be included in the Framework.

The European Cybersecurity Month (ECSM) is the European Union's annual campaign dedicated to promoting cybersecurity among EU citizens and organisations, and to providing up-to-date online security information through *awareness* raising and sharing of *good practices*.

- Each year, for the entire month of October, hundreds of activities take place across Europe, including conferences, workshops, trainings, webinars, presentations and more, to promote digital *security* and cyber hygiene
- The ECSM campaign is coordinated by the European Union Agency for Cybersecurity (ENISA) and the European Commission, and supported by EU Member States and hundreds of partners from Europe, and beyond
- The EU Agency for Cybersecurity coordinates the organisation of the ECSM campaign by acting as a "hub" for all Member States and EU Institutions, and by providing expert suggestions, generating *synergies* among EU citizens, businesses and public administration
- The Agency also publishes new materials and provides expert advice on different cybersecurity topics for Member States' audiences

21.6. Conclusions

An analysis of cybersecurity skills needs requires a widely adopted *taxonomy* of cybersecurity competencies, also called "skills framework".

- A competency framework is based on a comprehensive classification of actual *roles, functions and tasks*, i.e. the scope of work. Role definitions provide the full scope of "what specialists in the organization, unit or role are doing"
- Frameworks are a form of expression, for companies, academia and institutions, of the demand regarding professional figures in the cyber field, *addressed to students and workers*. Therefore they should make an active contribution in guiding the *development* of skills

- Therefore they should make an active contribution in guiding the development of skills. It is appropriate that the skills described are able to reflect and impose themselves dynamically on the changing KSAs (Knowledge, Skills, and Abilities)
- Competence can be an *intermediate* unit between the job position (or title) with its tasks on the one hand and the KSAs on the other. Therefore it is appropriate that the *skills described are able to reflect* and *impose themselves* dynamically
- In the job market, those who want to be competitive in terms of information security must first of all work very well internally in defining the *objectives* pursued in the field of information security and cybersecurity (see for example ISO/IEC 27001, chap. 5)
  - Therefore carry out an *assessment* of internal *resources and competencies*, *understand* what is missing to achieve those objectives and therefore open job positions *consistent* with these purposes
- Sometimes the *meeting* between *employer* (companies and other organizations) and *employees* (young students, workers looking for a job) is the most delicate moment. Misunderstanding is around the corner, with great *loss* for both the parties
- Frameworks help in this sense and the requirements can be *composed, modulated*, based on the context (e.g. we see how the U.S. DoD requires very specific skills, also proven by precise certifications, for access to certain job positions). *University* and other institutions that provide for cyber education can play an important role

Some "very very useful" reference to conclude this ~~absolutely useless~~ "absolutely wonderful" set of slides of this "amazing" course: Career Pathway roadmap, DoD 8570.01-M, European Cybersecurity Skills Framework (April 2022 draft), Enisa webinar, Enisa cybersecurity Education

22. M9 - Certification of people

22.1. Accreditation body

According to ISO, an accreditation is a third-party *attestation* related to a Conformity Assessment Body (or "*CAB*") conveying *formal demonstration* of its competence to carry out specific conformity assessment tasks.

- *Accreditation bodies* (or *third parties*) are authoritative bodies that perform *accreditation*. The authority of an accreditation body is generally derived from government
- Examples: Accredia (Italy) and Ukas (UK) are *officially recognized* accreditation bodies in their respective countries

22.2. Conformity Assessment Body (CAB)

A Conformity Assessment Body (CAB) is an organization that performs *conformity assessment services*. It is important to note that an accreditation body *is not* a CAB.

CABs, also known as Certification Bodies (e.g., CSQA, Bureau Veritas, BSI), can certify:

- *Competence of people* according to *ISO/IEC 17024:2012*
- *Management systems*, such as Quality (ISO 9001) and *ISMS (ISO/IEC 27001)*, according to ISO 19011 and ISO/IEC 17021-1
- *Products and services* according to ISO/IEC 17065

22.3. IAF and Mandatory Documents

The International Accreditation Forum (IAF) is a worldwide association of accreditation bodies and other bodies interested in conformity assessments in various fields (see here).

- IAF *facilitates trade* and *supports* regulators by operating a worldwide mutual recognition arrangement among Accreditation Bodies (ABs), ensuring results issued by accredited CABs are accepted globally

Mandatory Document 13:2020 aims to enable ABs to *harmonize* their application of ISO/IEC 17011:2017 (Conformity Assessment) for the accreditation of bodies providing audit and certification to ISO/IEC 27001 (ISMS).

- It specifies *areas of knowledge* that the AB shall *define* for specific functions in the accreditation of bodies auditing and certifying ISMS
- The knowledge requirements are complementary to the general competency required for each function within an AB
- Generally, each assessor involved in ISMS assessment shall have knowledge described in A1 to A5 of Annex A, while knowledge in A6 and A7 can be held within the team as a whole

CAB's *client process and operation* associated with ISMS cover:

- *Typical* business activities related to the technical area (see ISO/IEC 17021-1:2015, clause 7.1.2)
- Information and communication technology *specific* to the technical area
- Information security *technologies* and *practices* specific to the technical area, especially identification of information security related threats and vulnerabilities and related mitigations and controls
- Related *legal* requirements

Legal requirements identified here are those regulations which the organization subject of the audit would be expected to comply for the information security field or country/state/province within which they operate. IAF MD26:2023 provides transition requirements for ISO/IEC 27001:2022.

22.4. ISO/IEC 17024:2012 - Conformity assessment

ISO/IEC 17024:2012 "has been developed with the objective of *achieving* and *promoting* a globally accepted benchmark for organizations operating *certification of persons*".

- Certification for persons is one means of providing assurance that the *certified person meets the requirements of the certification scheme*
- Confidence in the respective certification schemes for persons is achieved by means of a globally accepted process of assessment and *periodic re-assessments* of the competence of certified persons

However, it is necessary to distinguish between situations where certification schemes for persons are *justified* and situations where *other forms of qualification are more appropriate*.

- The development of certification schemes for persons can *compensate for variations in education and training and thus facilitate the global job market*
- Alternatives to certification can still be necessary in positions where public services, official or governmental operations are concerned

In contrast to other types of conformity assessment bodies, one of the characteristic functions of the certification body for persons is to *conduct an examination*, which uses objective criteria to *measure competence and scoring*.

- While it is recognized that such an examination, if well planned and structured by the certification body for persons, can substantially serve to ensure *impartiality* of operations and *reduce the risk of a conflict of interest*
- In either case, this International Standard can serve as the *basis* for the recognition of the certification bodies for persons and the certification schemes under which persons are certified, *facilitating their acceptance* at all levels
- Only the harmonization of the system for developing and maintaining certification schemes for persons can establish the environment for mutual recognition and the *global exchange of personnel*
- This International Standard specifies *requirements* which ensure that certification bodies for persons operating certification schemes for persons operate in a *consistent*, *comparable* and *reliable* manner

- The requirements in this International Standard are considered to be general requirements for bodies providing certification of persons

Certification of persons can only occur when there is a *certification scheme*. Such scheme is designed to *supplement* the requirements included in this International Standard.

- Standard and include those requirements that the market needs or desires, or that are required by *governments*
- This International Standard can be used as a *criteria document* for accreditation or peer evaluation or designation by governmental authorities, scheme owners and others
- Many certifications for people (even when they don't follow an ISO based certification scheme) are ISO/IEC 17024:2012 compliant

ISO/IEC 17024:2012 contains several *principles* and *requirements* for a *body* certifying persons against specific requirements:

- Certification *body*
  - The organization that conduits the certification process
- Certification *process*
  - A set of activities by which a certification body determines that a person fulfills certification requirements (ISO/IEC 17024 - 3.3), including *application, assessment, decision on certification, certification and use of certificates* (ISO/IEC 17024 - 3.5) and logos/marks
- Certification *scheme*
  - It is *competence* (ISO/IEC 17024 –3.6) and other requirements related to specific occupational or skilled categories of persons
  - *Certification requirements* are a set of specified requirements, including requirements of the scheme to be fulfilled in order to establish or maintain certification
- *Scheme owner*
  - It is the organization responsible for developing and maintaining a certification scheme (ISO/IEC 17024 - 3.2). The organization can be the certification body itself, a governmental authority, or other
- *Certificate*
  - A document issued by a certification body under the provisions of this International Standard, indicating that the named person has fulfilled the certification requirements (ISO/IEC 17024 - 3.3)
- *Competence*
  - The ability to apply *knowledge* and *skills* to achieve intended results (where "results" can be, for instance, tasks or other activities mentioned in the previous lessons)
- *Qualification*
  - A demonstrated education, training and work experience, where applicable

The certification of competence for *management systems* of the *auditors/lead auditors* is regulated by ISO/IEC 17024:2012 and the relevant standards (e.g., ISO/IEC 27001:2013 and ISO/IEC 17021-1:2015) for which the candidate seeks recognition of competence.

22.5. Certified ISO/IEC 27001 auditor

The ISMS Auditor / Audit Group Manager is a professional who conducts audits on Information Security Management Systems according to international standards: ISO 19011, ISO/IEC 27001, and ISO/IEC 17021.

- This figure must demonstrate that they have the *competencies* (in terms of Skills, Knowledge and Personal Behavior) to professionally carry out the activities related to the *conduct* of an ISMS audit

The following is an example of a certification scheme (coming from here):

- *Principles* of the audit activity
- *Management* of an audit program
- Audit *activities*
- Competence and evaluation of *auditors*

Audit *planning* which must include:

- Communication with the audited organization
- Documentation of the preliminary examination
- Examination of the documentation or selection of the audit team
- Preparation of the audit and team meeting
- Notes on the *preliminary* audit purposes
  - Preparation and use (with examples of forms) of *checklists* during the audit phases
  - Audit *meeting* preparations, with examples
  - Content, program and conduct of the *opening* and *closing* meetings

Auditor behavior in carrying out the audit, including relations with the company, the importance of objective evidence:

- Detection, drafting and communication of anomalies
- Criteria for the formulation and methodologies for identifying the findings and their classification
- Follow-up activities
- Notes on risk management as applicable in the ISMS sector
- Notes on compliance with the legal requirements on health and safety by the Audit Group
- *Role* differences between Auditors and Audit Group Managers, in the management of the audit and of team members

- Furthermore, the knowledge and *skills* reported, by way of example, in the UNI EN ISO 19011: 2018 standard
- Specific *legal requirements* for the country where the auditor will operate (see IAF requirements for ABs) are present

Moving on:

- *Skills*

The ISMS Auditor / Audit Group Manager must be able to:

- Apply, to different audits, *appropriate principles*, *procedures* and *methods* to ensure that audits are conducted in a coherent and systematic way
- Understand the *scope* of the audit and apply the audit criteria
- Understand the *structure, business and management practices* of the audited organization
- Operate within the *legal* and *contractual* requirements of the organization
- Use *appropriate language* at all levels within the customer's organization
- *Take notes* and prepare *written* reports
- Carry out *presentations* and *interviews*
- Identify *laws, regulations, directives*, etc., relating to the organizations to be audited

Moving on:

- *Personal behavior*

Auditors should possess the necessary qualities that enable them to act in accordance with the audit principles. In particular, the Auditor should be:

- Respectful of *ethical* principles (fair, truthful, sincere, honest and confidential)
- *Open-minded* (willing to consider alternative ideas or points of view)
- *Diplomat* (being tactful in dealing with people)
- Gifted with a *spirit of observation* (active observer of the activities and the surrounding environment)
- *Insightful* (aware of situations and able to understand them)
- *Versatile* (able to readily adapt to different situations)
- *Tenacious* (persevering and focused on achieving goals)
- *Resolute* (able to promptly reach conclusions based on analysis and logical reasoning)
- *Self-confident* (able to act and behave independently and at the same time to interact effectively)
- Capable of acting *firmly* (i.e. in a responsible and ethical manner)
- *Open* to improvement (eager to learn from situations and committed to getting better and better audit results)

- Sensitive to *cultural diversity* (attentive and respectful of the culture of the audited organization)
- *Collaborative* (able to interact effectively with others, including members of the audit team and the staff of the audited organization)

Other important requirements for an auditor:

- *Educational qualification*
  - The applicant for certification must be in possession of at least the Higher Secondary Education Diploma
- *Training and Specific Training*
  - It is necessary to have attended and passed the final exam of a [40-hour] ISMS Auditor course in accordance with current legislation
- *Working experience*
  - Documented and appropriate continuous work experience is required in technical activities at companies, organizations or in consultancy [for a period of not less than 5 years]
- *Documented and appropriate specific continuous work*
  - Experience [of at least 2 years] in the field of Information Security Management Systems is also required (this experience can be included in the overall work experience)
- *Audit experience*
  - ISMS Auditor
    - It is necessary to *document* an audit experience gained in the last 3 years on 5 complete audits on at least 4 separate information security management systems, of which at least 2 in the last year
    - It is also necessary to have passed a training course as an ISMS Auditor in accordance with UNI EN ISO 19011/UNI CEI EN ISO/IEC 17021 Standards by a System Certification Body
      - Or having carried out at least 4/5 audits for at least 20 days of audit experience, as an auditor under guidance of an Audit Group Manager certified by the certification of personnel/qualified by a System Certification Body
    - The audits in training can be included in those indicated above
  - ISMS Head of the Audit Group
    - It is necessary to document, in addition to the auditor's requirements, the following audit experience gained, in the last 2 years, as Head of at least 3 complete Audits, not all internal and on separate Information Security Management Systems
    - It is also necessary to have successfully passed a training course as an ISMS Audit Group Manager in accordance with UNI EN ISO 19011 / UNI CEI EN ISO / IEC 17021 Standards by a System Certification Body in the event part III audits
      - Or having carried out at least 3 complete Audits, not all internal, performed on separate systems for at least 15 days of audit experience as Head of the Audit Group under the direction/

guidance of an Audit Group Manager certified by a Personnel Certification Body/System Certification Body

- The audits in training can be included in those indicated above

An *exam* is therefore envisaged for the issue of personal *certification*, the criteria of which are defined in the scheme.

22.6. Conclusions

- Accredited certification bodies' assessments, based on shared standards and documents, provide added value compared to other forms of certification
- In a *competitive* job market, demonstrating competence through a degree and CV alone may not suffice; tools to demonstrate and maintain skills are crucial
- Third-party certification ensures *independence*, *impartiality*, and the professional's competence, encouraging continuous improvement of knowledge and skills, becoming *indispensable*
- Accredited certification offers advantages such as multiple *checks* by the *accredited* body, registration of professionals in AB databases, and international recognition of professional competence - using figures like *certification body*

23. M10 - Most common certifications available on the market

We have seen that standards and frameworks are a valid *tool* to guide organizations and companies in continuous improvement.

- Since companies are also made up of people, taking into account the human resources available and not, *governance* and *competence* can be very close issues
- There are specific *certifications* in this field to demonstrate the knowledge, the skills and ability of people who need to master how IT companies must be organized by adopting best practices

The organization of a company, starting from the definition of its *objectives*, is a fundamental skill for many professional figures (including those profiles who do not have to establish the strategic address or manage parts of the organization).

- The objectives of IT companies are *specific* to this type of activity and they must be integrated within the overall objectives
- *Information is a key resource for all enterprises* and technology plays a significant role. Information technology is increasingly advanced and has become *pervasive* in enterprises and all kinds of environments

23.1. COBIT 5

COBIT 5 provides a comprehensive framework that assists enterprises in *achieving their objectives for the governance and management of enterprise IT*. Side note: Remember COBIT stays for Control Objectives for Information and Related Technology and was created by ISACA.

Simply stated, it can help enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.

- This Framework enables IT to be governed and managed in a *holistic manner* for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders
- COBIT 5 is generic and useful for enterprises *of all sizes*, whether commercial, not-for-profit or in the public sector

There are different principles to consider (some useful reference for this here):

- Principle 1, *Meeting Stakeholder Needs*
  - It introduces the COBIT 5 goals cascade. The enterprise goals for IT are used to *formalize* and *structure* the stakeholder *needs*
  - Enterprise goals can be linked to IT-related goals, and these IT-related goals can be achieved through the optimal use and execution of all enablers, including *processes*
  - This set of connecting goals is called the *COBIT 5 goals cascade*. The chapter also provides examples of typical governance and management questions that stakeholders may have about enterprise IT

- Different steps to consider here:
  - Step 1. Stakeholder *Drivers* Influence Stakeholder *Needs*
    - Stakeholder needs are influenced by a number of drivers, e.g., strategy changes, a changing business and regulatory environment, and new technologies
  - Step 2. Stakeholder *Needs* Cascade to *Enterprise Goals*
  - Step 3. Enterprise *Goals* Cascade to *IT-related Goals*
  - Step 4. IT-related Goals Cascade to *Enabler* Goals
- Principle 2, *Covering the Enterprise End-to-end*
  - It explains how COBIT 5 integrates *governance of enterprise* IT into *enterprise governance* by covering all functions and processes within the enterprise
- Principle 3, *Applying a Single Integrated Framework*
  - It describes briefly the COBIT 5 architecture that achieves the integration
- Principle 4, *Enabling a Holistic Approach*
  - Governance of enterprise IT is *systemic* and supported by a set of enablers. In this chapter, enablers are introduced and a common way of looking at enablers is presented: the generic enabler model
  - Enablers are broadly defined as anything that can help to achieve the *objectives* of the enterprise. The COBIT 5 framework defines *seven* categories of enablers:
    - Principles, Policies and Frameworks
    - Processes
    - Organizational Structures
    - Culture, Ethics and Behavior
    - Information
    - Services, Infrastructure and Applications
    - People, Skills and Competencies
- Principle 5, *Separating Governance From Management*
  - It discusses the difference between management and governance, and how they *interrelate*. The high-level COBIT 5 process reference model is included as an example

  - *Governance*
  - It ensures that stakeholder needs, conditions and options are evaluated to determine *balanced, agreed-on* enterprise objectives to be *achieved*; setting direction through *prioritization* and *decision making*
  - In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson

  - Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises

  – *Management*

  - This *plans, builds, runs* and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives

  - In most enterprises, management is the responsibility of the executive management under the leadership of the CEO

Implementation Guidance describes how the appropriate environment can be created, the enablers required, typical pain points and trigger events for implementation, and the implementation and continual improvement life cycle.

- Consider the *COBIT 5 Process Capability Model* in the COBIT Assessment Programme approach here.

COBIT 5 was developed taking into account a number of other standards and frameworks.

- TOGAF (The Open Group Architecture Framework) for modeling the overall structure of the system and its components
- ITIL for IT Service Management
- *ISO27000 family for information security*
- *ISO31000 for risk management*
- PMBOK for project management and control

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

- COBIT 5 *Assessor*
  - Demonstrates mastery in understanding and performing a formal *Process Capability Assessment*
  - Holders ensure stronger, more reliable control over internal processes and provide stakeholders a clear line of sight into process capabilities, allowing IT leaders to redirect or liberate resources to increase innovation and value for the enterprise
- COBIT 5 *Foundation*
  - Affirms holders' understanding of COBIT principles and concepts. Holders understand the IT management issues organizations face today and know how to use COBIT to respond to these challenges
  - These professionals have used the elements of COBIT, in practice, and are prepared to recommended applications of COBIT for enterprise-wide project

The COBIT Foundation Certificate Exam ensures that you understand:

- How to align IT goals with strategic business objectives using tools designed to give governance a wider perspective, and practitioners more flexibility
- The value derived from IT, necessary resources, and potential risks in the process of building a mature relationship between the business and IT
- The *different* types of IT governance frameworks such as ITIL, NIST etc., including the benefits of each and how they work
- COBIT 5 *Implementation*
  - Confirms holders' ability to understand and apply the elements of COBIT 5 across an enterprise. These professionals have mastered the approach to implementing the "Governance of Enterprise Information Technology or (GEIT)" based on a continual improvement life cycle
  - These professionals have demonstrated the understanding of how COBIT 5 should be tailored to suit an enterprise's specific needs

It can be possible to implement the NIST CSF Framework using COBIT 5:

- Showcases the holder's understanding of the goals and content of the *Cybersecurity Framework (CSF)* and how to apply the seven Cybersecurity Framework implementation steps using COBIT
- In order to obtain this credential, professionals must be able to show that they have successfully completed the COBIT 5 Foundation Exam.

The following starts *M10.2 - Competence about Cybersecurity* - it's inside the slides, so I write it here as it is.

23.3. IT Security Certification for people

Why *certification is important*:

- *Job Security*
  - 82% of organizations prefer hiring candidates with certifications. The right certification could signal to HR teams and hiring managers that you have the specific job-role skills they need
  - A possible *obstacle* that is encountered in the search for professional figures in the field of cybersecurity is that of not having the *people* who are able to *evaluate* and *measure* the skills that are needed
    - Especially for those organizations that are starting to have to *build* their own staff because they do not still have one
- In these cases certification constitutes a credential that helps people to be recognized as competent by different employers and contexts
  - But there are many *certifications* and different *bodies* and *companies* that issue them. It is not always easy to find your way around in this world
- The *urgency* to find experts who know how to defend data and IT technologies from possible cyberattacks does not help and can lead to a poor consideration of real needs of the company

  - On the one hand organizations must clarify, based on the type of data processed, the type of *technologies*, the size, the people, specifically *which (and how many)* are the people to be included
  - On the other hand, people themselves must build a path that possibly reflects their *inclinations* and *passions*, but also a coherent and *realistic* set of skills as close to demand as possible
- *Enterprise Security*
  - Certifications provide confirmation of the skills needed to combat breaches and mitigate threats to the enterprise
  - 94% of cybersecurity practitioners believe their certs have better prepared them for their current role, allowing them to successfully protect their organization
- *Proven Ability*
  - If you have a certification proving you've mastered a specific skill-set, both *employers* and your *industry* peers know that you've got what it takes
- *Personal Validation*
  - Setting goals to learn new skills and pass a certification exam can be a *challenging* and *rewarding* internal experience
  - Proving to yourself that you can master skills and conquer the exam creates a sense of purpose and personal satisfaction

23.4. CompTIA certifications

CompTIA (The Computing Technology Industry Association) is a vendor-neutral, independent source of information on a wide range of technology topics, including cybersecurity; education/training, new and emerging technologies; legislation and policies affecting the industry and workforce data, development and trends.

- It has four IT certification series that test different knowledge standards – from entry-level to expert
- Certifications are divided in different levels:
  - Core
  - *Cybersecurity*
  - Infrastructure
  - Data and Analysis
  - Additional Professional

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

- Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

- Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011

CompTIA Cybersecurity Analyst (CySA+) is an IT workforce certification that applies behavioral analytics to networks and devices to prevent, detect and combat cybersecurity *threats* through continuous security *monitoring*.

This one meets the *ISO 17024 standard* and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements.

- It is compliant with government regulations under the Federal Information Security Management Act (FISMA)
- Regulators and governments rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program
- CySA+ will verify the successful candidate has the knowledge and skills required to:
  - Leverage intelligence and threat detection techniques
  - Analyze and interpret data
  - Identify and address vulnerabilities
  - Suggest preventative measures
  - Effectively respond to and recover from incidents

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for *security architects* and *senior security engineers* charged with leading and improving an enterprise's cybersecurity readiness.

Successful candidates will have the knowledge required to:

- Architect, engineer, integrate, and implement secure solutions across *complex environments* to support a resilient enterprise
- Use *monitoring, detection, incident response, and automation* to proactively support ongoing security operations in an enterprise environment
- Apply security practices to *cloud, on-premises, endpoint, and mobile infrastructure*, while considering cryptographic technologies and techniques
- Consider the impact of *governance, risk, and compliance* requirements throughout the enterprise

CASP+ is *compliant with ISO 17024 standard* and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program.

23.5. GIAC certifications

The GCLD - (GIAC Cloud Security Essentials) certification validates a practitioner's ability to implement preventive, detective, and reactionary techniques to defend valuable cloud-based workloads. Covered areas:

- Evaluation of cloud service provider similarities, differences, challenges, and opportunities
- Planning, deploying, hardening, and securing single and multi-cloud environments
- Basic cloud resource auditing, security assessment, and incident response

The GPCS (GIAC Public Cloud Security) certification validates a practitioner's ability to secure the cloud in both public cloud and multi cloud environments.

- GPCS-certified professionals are familiar with the nuances of AWS, Azure, and GCP and have the skills needed to defend each of these platforms
- Covered areas:
  - Evaluation and comparison of public cloud service providers
  - Auditing, hardening, and securing public cloud environments
  - Introduction to multi-cloud compliance and integration

23.6. ISC certifications

The International Information Systems Security Certification Consortium (ISC) is a non-profit organization that provides security training and certificates - source here.

- It is worldwide known for issuing, in particular, CISSP - Certified Information Systems Security Professional, CCSP - Certified Cloud Security Professional and CSSLP - Certified Secure Software Lifecycle Professional certifications.

Who earns the CISSP?

- Ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions:
  - Chief Information Security Officer
  - Chief Information Officer
  - Director of Security
  - IT Director/Manager
  - Security Systems Engineer
  - Security Analyst
  - Security Manager
  - Security Auditor
  - Security Architect
  - Security Consultant
  - Network Architect

Who earns the CCSP?

- Ideal for IT and information security leaders responsible for applying best practices to cloud security architecture, design, operations and service orchestration, including those in the following positions:
  - Cloud Architect
  - Cloud Engineer
  - Cloud Consultant
  - Cloud Administrator
  - Cloud Security Analyst
  - Cloud Specialist
  - Auditor of Cloud Computing Services
  - Professional Cloud Developer

As a side note, the CCSP meets the U.S. Department of Defense (DoD) Directive 8570.1.

Who earns the CSSLP?

- Ideal for software development and security professionals responsible for applying best practices to each phase of the SDLC – from software design and implementation to testing and deployment – including those in the following positions:
  - Software Architect
  - Software Engineer
  - Software Developer
  - Application Security Specialist
  - Software Program Manager
  - Quality Assurance Tester
  - Penetration Tester
  - Software Procurement Analyst
  - Project Manager
  - Security Manager
  - IT Director/Manager

As a side note, also the CSSLP meets the U.S. Department of Defense (DoD) Directive 8570.1.

The CCAK (Certificate of Cloud Auditing Knowledge) certification helps professionals learn how to audit *cloud systems*.

- CCAK is the first-ever, technical, vendor-neutral credential for cloud auditing

- This certificate qualifies competent technical professionals who can help organizations *mitigate risks* and optimize Return of Investment (ROI) in the cloud

As organizations migrate to the cloud, they need information security professionals who are cloud-savvy.

- The CCSK certificate is widely recognized as a standard of expertise for cloud security and gives a cohesive and vendor-neutral understanding of how to secure data in the cloud
- It covers key areas, including best practices for IAM, cloud incident response, application security, data encryption, SecaaS, securing emerging technologies, and more

23.7. EC-Council certifications

EC-Council's Certified Chief Information Security Officer Program (CCISO) is a program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security.

EC-Council's Certified Hacking Forensic Investigator (CHFI) is ANSI accredited, *lab-focused* that gives organizations *vendor-neutral training* in digital forensics.

- CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around *Dark Web, IoT, and Cloud Forensics*
- The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies
- The program is designed for IT professionals involved with information system security, computer *forensics*, and incident response
  - It will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers
  - The program equips candidates with the necessary skills to proactively *investigate* complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks

EC-Council Network Defender certifications are vendor-neutral and provide an approach to learning secure networking practices, as well as how to analyze and harden computing systems prevalent in the current IT infrastructure. It is completely focused on network *security* and *defense*.

Isaca's CISA, CRISC, CGEIT, CISM, CSX-P, CDPSE, ITCA certifications are shown in the specific slides (in case, see something here).

23.8. Pentesting certifications

CompTIA PenTest+ is for cybersecurity professionals tasked with *penetration testing* and *vulnerability management*. The CompTIA PenTest+ certification exam will verify successful candidates have the knowledge and skills required to:

- Plan and scope a penetration testing engagement
- Understand legal and compliance requirements

- Perform vulnerability scanning and penetration testing using appropriate *tools* and *techniques*, and then analyze the results
- Produce a written report containing proposed remediation techniques, effectively
- *Communicate results* to the management team, and provide practical recommendations

The GIAC (Global Information Assurance Certification) program is run by the SANS Institute, one of the oldest organizations that provide cybersecurity education.

- The GIAC Penetration Tester (GPEN) certification validates a practitioner's ability to properly conduct a penetration test, using best practice techniques and methodologies
- GPEN certification holders have the knowledge and skills to conduct exploits and engage in detailed *reconnaissance*, as well as utilize a process-oriented approach to penetration testing projects
- Covered areas:
  - Comprehensive pen test planning, scoping, and recon
  - In-depth scanning and exploitation, post-exploitation, and pivoting
  - In-Depth password attacks and web app pen testing

Certified Ethical Hacker (CEH) is about commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization.

- In 2003, CEH introduced the five phases of ethical hacking, the blueprint for approaching target and succeeding at breaking in
- CEH has continued to hone these 5 *phases*, updating and refining them to match the skillset ethical hackers need today:
  - Reconnaissance
  - Gaining access
  - Enumeration
  - Maintaining access
  - Covering your tracks
- CEH covers many threats and vulnerability scenarios, like APT, Fileless Malware, Web API Threats, Webhooks, Web Shell, OT Attacks, Cloud Attacks, AI, ML, but also emerging technologies such as OT Technology and Container Technology.
- CEH includes Malware Analysis tactics for ransomware, banking and financial malware, IoT botnets, OT Malware Analysis, Android Malware, and more

Penetration Testing with Kali Linux (PWK/PEN-200) online ethical hacking course is self-paced.

- It introduces penetration testing tools and techniques via hands-on experience. PEN-200 trains not only the skills, but also the mindset required to be a successful penetration tester

- Students who complete the course and pass the exam earn the Offensive Security Certified Professional (OSCP) *certification* - some tips for that exam here
- All students are required to have:
  - Solid understanding of TCP/IP networking
  - Reasonable Windows and Linux administration experience
  - Familiarity with basic Bash and/or Python scripting

Gamification, gradual paths and playground/community are some *different* (or somehow *additional*) powerful tools to guide the improvement of competence, even without certifying them.

- But are we sure these tools do not assess the competence of people and don't they have a value almost comparable to certifications?
- Those who train challenge themselves and other apprentices, improving their own and others' knowledge and skills, obtaining *measurable* results within a *community*, so the usefulness of these workshops is evident
- Here are some known resources to improve by *doing*:
  - hackthebox.com
  - infoseclearning.com
  - tryhackme.com

To conclude:

- *Certification*: has the undisputed advantage of reliably certifying someone's competence, thanks to a system of trust that is built through the *consensus* that forms around them.
  - Certifications may provide for a necessary level of *abstraction* (which removes some dimensions in the real world) which varies according to the examination methods, which may be greater if the examination does not include practical tests, and vice versa
  - The more organizations accept certifications, the more they take on value
- *Laboratory*: participating in laboratories recognized for the level of difficulty, even in the absence of certification, can actually improve people's skills, especially in those sectors where lateral thinking and the development of concrete working methods are strongly required
  - (Such as for those who will carry out an ethical hacking activity)
  - In this case, competence tends to assert itself *in practice*, with mechanisms that reward results similar to those expected in real scenarios
  - The quality and realism of the laboratories are the key to their success (preparing people)

(With this set of slides, there is also a set called ISACA Chapter presentation, which is completely optional and just there for a more in-depth notion - in case I'll summarize it anyway, but do not focus deeply on that)

The document is a presentation by the ISACA Venice Chapter from May 23, 2022, introducing ISACA, a global non-profit association for IT audit, assurance, security, risk, compliance, cybersecurity, and governance professionals. The presentation covers the following key points:

1. ISACA has a worldwide presence with 224 chapters across various regions
2. ISACA offers certifications such as CISA, CISM, and CRISC, which are among the top-paying IT certifications
3. ISACA provides cybersecurity education and credentialing through its Cybersecurity Nexus (CSX) training program
4. ISACA organizes worldwide conferences, educational seminars, webinars, and virtual summits
5. Members have access to online resources, forums, special interest groups, volunteer opportunities, and networking events through the ISACA online community
6. ISACA offers career resources, including career pathways tools, discounted career coaching, and a job board
7. ISACA has a student membership program and supports the formation of ISACA Student Groups at higher education institutions
8. The ISACA Venice Chapter, established in 2011, covers Northern-East Italy and has over 250 members
9. The Venice Chapter organizes certification prep courses, the AppSec Conference, monthly events, and other conferences on specific topics
10. Students in the "Security and risk: management and certifications" course at the University of Padua can enroll in ISACA Venice courses for free - wow, amazingly useful I know!

24. M11.1 - Management Systems audit techniques and approach examples

24.1. Process and definitions

We give several definitions here, according to ISO 9000:2015 (Quality management systems). The following could be considered useful for an audit report (a bunch of general ones to aim the concepts):

- *Audit*
  - Systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
- *Management system*
  - Set of interrelated or interacting elements of an organization to establish policies and objectives, and processes to achieve those objectives
- *Combined audit*
  - Audit carried out together at a single auditee on two or more management systems
- *Joint audit*
  - Audit carried out at a single auditee by two or more auditing organizations
- *Audit programme*
  - Arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose
- *Audit client*
  - Organization or person requesting an audit
- *Audit team*
  - One or more persons conducting an audit, supported if needed by technical experts
- *Auditor*
  - Person who conducts an audit
- *Performance*
  - *Measurable* result
- *Process*
  - Set of interrelated or interacting activities that use inputs to deliver an intended result
- *Effectiveness*
  - Extent to which planned activities are *realized* and planned results achieved

Consider the prerequisites for assets:

- *Audit criteria*
  - Set of requirements used as a reference against which objective evidence is compared
- *Objective evidence*
  - Data supporting the existence or verity of something
- *Audit evidence*
  - Records, statements of fact or other information, which are relevant to the audit criteria and verifiable

Up next, we consider:

- *Audit scope*
  - Extent and boundaries of an audit
- *Audit plan*
  - Description of the activities and arrangements for an audit
- *Audit findings*
  - Results of the evaluation of the collected audit evidence against audit criteria

We then jump to the:

- *Audit conclusion*
  - Outcome of an audit, after consideration of the audit objectives and all audit findings

From the audit conclusion for the audit report, said report might go into two directions:

- *Nonconformity*
  - Non-fulfilment of a *requirement*. If major, no certification is possible. If minor, certification is still possible, but nonconformity will have to be dealt with by the following year
- Conformity
  - Fulfilment of a *requirement*. This here brings to the certification itself

24.2. Purpose of a certification

The *auditor* ("evaluator") is the *professional who collects this information*. Please remember that certification can also be a mandatory requirement in certain circumstances (e.g. calls for tender).

Audit can be:

- *First party*: internal, auditors and audited are in the *same* organization
- *Second party*: carried out by an interested external party (e.g. a Customer)
- *Third party*: carried out by an independent body (e.g. a Certification Body)

Some ISO standards on the matter:

- *ISO 17021* - Accreditation standard
  - It is addressed to the *Certification Body*
  - Contains information on *third party audits*
  - The first part deals with the general requirements for all system certifications
  - A series of subsequent parts supplement the text with specific requirements for the individual Management Systems
- *ISO 19011* - Guideline for management system audits
  - It is aimed at *anyone who carries out audits*
  - Focused on *first and second party audits*
  - Provides *guidance* on managing an audit program, planning and conducting audits of management systems, as well as the competence and evaluation of an auditor and audit team

An audit can be conducted against a range of audit criteria, separately or in combination, including but not limited to:

- *Requirements* defined in one or more management system standards
- *Policies* and *requirements* specified by relevant interested parties
- *Statutory* and *regulatory* requirements
- One or more *management system processes* defined by the organization or other parties
- Management system plan(s) relating to the provision of specific *outputs* of a management system (e.g. quality plan, project plan)

The certification audit consists of two phases:

- *Audit stage 1*
- *Audit stage 2*

The pre-audit is *optional*, but adds value:

1. Preparation of documentation and implementation audit
2. Helps the organization familiarize itself with the audit approach of certification
3. Address all regulatory requirements
4. Optional, at the request of the organization

- Stage 1 – “Preparation Audit”
  - It is recommended to do it in the *field*
  - *Documentation* review
  - Evaluation of the *structure* and specific conditions of the site

  - Review of key *performance* parameters
  - Validation of the *scope*
  - Collection of information on *mandatory* (legal and regulatory) requirements and their compliance
  - Reviewing the availability of *resources* for phase 2 audit, agreeing with the client and planning phase 2
  - Assessment of *overall* preparation for the phase 2 audit
  - Report the *findings*, including critical aspects, to the customer/audited entity
- Stage 2 – "Implementation audit"
  - The purpose is to evaluate the *implementation* and *effectiveness* of the system
  - It must be conducted on place
  - *Compliance* with all audit criteria requirements
  - Performance versus *goals*
  - Performance against *legal* requirements
  - *Operational* control of the audited processes
  - Results, actions and effectiveness in the field of *internal audits* and the *management review*
  - Management's responsibility towards its own *policies*
  - Interrelationship between *mandatory* requirements, quality policy, objectives and performance targets
- Evaluate the *effectiveness* of the system with regard to:
  - Achieve *goals* and *objectives*
  - Implement policy *commitments* (e.g. compliance, achievement of requirements, continuous improvement, etc.)
  - Operational controls in all areas of the system
  - Corrective actions
- Evaluate the organization's *implementation* and overall *effectiveness* of the Management System
- Stage 2 - "Complete system audit"
  - The complete Management System audit covers:
  - EVERY requirement: intent, implementation and effectiveness
  - Interrelationships between the elements of the MS (Management System)
  - 3 Key questions:
    1. Is the system *adequate*?

2. Is the system *suitable*?
3. Is the system *effective*?

Audit conclusion is:

- Based on the *results* of Stage 1 and Stage 2
- Decision to issue the *certificate* based on the findings of the Audit Team

Consider the example of a *surveillance* audit:

- Conducted in the field at least every year (sometimes every semester)
- They cover all processes / functions over a three year period following certification / renewal
- The audit program is based on the results of previous audits and on the importance and status of the processes
- They can take into account internal audits
- Evaluate the organization's continued compliance with the requirements of the certification standard

Following an ideal ISO 27011 Audit Cycle:

- Certification Audit (2018)
- Surveillance Audit (2019)
- Surveillance Audit (2020)
- Recertification Audit (2021)
- Surveillance Audit (2022)
- Surveillance Audit (2023)
- Recertification Audit (2024)
- Surveillance Audit (2025)
- and so on…

24.3. Audit plan, initiation and preparation

6 *phases* of the audit (ISO 19011):

- *Initiating* audit
- *Preparing* audit activities
- *Conducting* audit activities
- Preparing and distributing audit *report*
- *Completing* audit

- Conducting audit *follow-up*

Remember that management systems (such as ISMS or Quality MS) are based on the High level structure, which is founded on the Deming Cycle «Plan Do Check Act» (*PDCA*).

Conducting a single audit includes:

- Targets
- Criteria
- Extension (including processes and / or functions)
- Dates and sites
- Start and end times of activities
- Roles and responsibilities of auditors and accompanying persons

Some steps must be followed:

- Establish communication channels and prepare the audit client to cooperate in all the aspects of its competence
- Review of relevant documented information relating to the management system of the audited organization
- Documented information should include, but are not limited to: management system *documents* and *records*, as well as *previous audit reports*
  - The review should consider the context of the audited organization, including size, type and complexity, as well as related risks and opportunities
  - The review should also consider the scope, criteria and objectives of the audit
- The review is generally conducted personally by the Lead Auditor

24.4. Preparing audit activities

In preparing the audit, follow *Phase 1 - Documentary evidence*:

- Normally it is performed in the field
- Validation of the scope of the management system
- Gathering information on the legal framework
- Examination of documents
- Evaluation of the structure and specific conditions
- Review of indicators and parameters
- Establish general preparation for Phase 2
- Define the plan for Phase 2

- Report the findings, including areas for improvement

We compose the activities as follows:

- *Audit plan*
  - Field of application
  - Criteria dates & duration
  - Group of auditors
  - Detailed timetable
  - Planning matrix
  - Auditor requests
  - (Remember to cover shifts)
- *Working documents*
  - Checklist
  - Standard
  - Guidelines

A full system audit covers:

- *Every* point of the reference standard
- Links between elements of the system

Some key questions here:

1. Is the system *adequate*?
2. Does the system *work*?
3. Is the system *effective*?

Some other points:

- The *opening* meeting is important for introducing the audit team, discussing the objectives, scope and criteria of the audit, confirming the plan and methods, sampling for evidence acquisition and other important details for the execution of the audit
- *Intermediate* meetings will also be planned. with the management system contact person and other managers to review the findings, discuss non-conformities, manage the proposals for corrective actions and corrections

The auditor finds evidence by checking *documents*, looking at *records*, *interviewing* people at all levels, and observing practices and the physical environment.

- Production / service lines, activities, controls, inspections, audits, monitoring management of non-compliant products / services maintenance systems

  - Talk to the people on the field, if you can hear and understand them
- Product segregation
  - Ask what the dials and hands indicate about monitoring and measuring processes
- Conditions of the warehouses
  - Look at the processes in place at the moment, check what is happening and check the documented description of events and processes
- Handling, identification, packaging
- Data entry activity

24.5. Auditing a process and sampling

The following is the checklist (useful and necessary as a tool) on how to proceed on process auditing (all the following are always taken from ISO 19011):

1. Process
2. Input
3. Output
4. Resources
5. Who is involved (competence, ability, training)
6. How (methods, procedures and techniques)
7. Effectiveness (measurable goals)

Other recommendations on how to proceed:

- Leave space for your *notes*
- The Checklist must become an audit *diary*
- Reference to the audit *criteria*
- Reference to system *documents* (procedures)
- Reference to documents checked (records)

About the sampling, the following is how to proceed:

- An auditor always or almost always works on a sample basis
- *Judgment-based* sampling
- *Statistical* sampling
- Consider the *time since the last audit*
- Consider the *extension of the scope*

24.6. Nonconformities

According to ISO 19011 - Guidelines for auditing management systems, non-conformities are not to be intended in a negative way and a discovered nonconformity is a previously hidden opportunity for improvement.

- The auditors *do not provide suggestions* on how to resolve the nonconformities and nonconformity reports must be very *clear and objective*
- Nonconformity reports have 3 elements:
  1. The *declaration* of non-conformity (description of the element of the system that is incorrect)
  2. The *evidence* (what has currently been found)
  3. The *requirement* (what should have been)
- ISO 27021 requires that only non-conformities that involve failures in complying with one or more requirements and / or the system's inability to achieve the desired results, must be closed with an effective correction and corrective action before certification (*major non-conformities*)
  - Please note that the opportunities for improvement *are not* non-conformities
  - It is good practice to consider opportunities for improvement, even though recommendations are not binding

There are different kinds of nonconformities:

- *Product* nonconformities
  - Emerge during the daily work
  - They are usually identified by the operators
  - They are physiological in processes
  - Must be correct
  - Must be registered
  - Records must be analyzed
  - Possibly they must be improved with corrective actions
- *System* nonconformities
  - Emerge during audits or other external controls
  - They are identified by external bodies and not during normal control operations
  - They are pathological in the processes
  - The immediate effect must be corrected
  - The causes must be analyzed

In order to intervene, corrective and preventive actions must be implemented:

- *Corrective* action is needed to eliminate the cause of a detected non-compliance
- *Preventive* action is to eliminate the cause of a potential non-compliance

24.7. Closing meeting

It has the following characteristics:

- It must be preceded by an internal meeting of the audit team
- Presence of the *management* and the heads of the audited processes
- There must be *no surprises* (non-conformities must be communicated or anticipated when they are discovered)
- Discussion of corrective actions must occur first

Contents of the *final report*:

- *Objectives* of the scope of the audit itself
- *Dates* and *places* of the audit
- Identification of the *customer, auditor and people audited*
- Audit *criteria*
- Auditor's judgment on compliance with the *specified* criteria
- *Non-conformities* and *observations*
- *Confidentiality*
- Attachments: *complete* checklists and notes, non compliance reports, planning of *corrective* and *preventive* actions

24.8. Use cases

- *Case 1*
  - Beta company intends to certify its information security management system by declaring the insurance services it provides as the scope of the management system (and therefore of the certificate)
  - Beta also provides financial services, which are not included in the scope
  - The needs and expectations of stakeholders, who need an ISO27001 certified organization to deliver all services (not just insurance) are not considered in the scope
  - In the role of the auditor, what are the chapters of the ISO 27001 standard that have been disregarded, which may lead to non-compliance?

(The following to give you more context)

In the role of the auditor, the chapters of the ISO 27001 standard that have been disregarded by Beta company, which may lead to non-compliance, are:

- Chapter 4 - Context of the Organization:
  - 4.1. Understanding the organization and its context: The organization must determine external and internal issues relevant to its purpose and that affect its ability to achieve the intended outcomes of its ISMS
  - 4.2. Understanding the needs and expectations of interested parties: The organization must determine the interested parties (stakeholders) relevant to the ISMS and their requirements. By not considering the stakeholders' needs for all services to be certified, Beta company fails to comply with this clause
  - 4.3. Determining the scope of the ISMS: The organization must consider the context and the requirements of interested parties when determining the scope of the ISMS. By excluding financial services without considering stakeholders' needs, Beta company does not properly determine the scope of its ISMS
- Chapter 5 - Leadership:
  - 5.2. Information security policy: Top management must establish an information security policy that is appropriate to the purpose of the organization, including the requirements of relevant interested parties. The exclusion of financial services may indicate that the policy does not align with the stakeholders' needs.
- Chapter 6 - Planning:
  - Section 6.1.3 - Determining the scope of the information security management system: By excluding the financial services from the scope of the management system, Beta company has not determined the appropriate scope, which should cover all relevant activities and services.

By disregarding these sections, Beta company may face non-compliance issues during the certification audit.

- *Case 2*
  - The Gamma company submits an application for certification of its ISMS to the certification body. When analyzing documented information from the management system, the company does not have a written information security policy
  - In the role of the auditor, what are the chapters of the ISO 27001 standard that have been disregarded, which may lead to non-compliance?

(The following to give you more context)

In the role of the auditor, the chapters of the ISO 27001 standard that have been disregarded by Beta company, which may lead to non-compliance, are:

- Chapter 5: Leadership
  - 5.2. Information security policy: This clause specifically requires that an information security policy must be established, implemented, and maintained. The lack of a written policy directly disregards this clause, leading to non-compliance

- Chapter 7: Support
  - 7.5. Documented information: This clause covers the requirements for creating and maintaining documented information. It includes ensuring that the information security policy is documented. The absence of a written policy indicates non-compliance with the requirements for documented information.

25. M11.2 - Practical cases, ISMS audit

In this chapter we will see, through examples, what are some important aspects to consider in the ISO / IEC 27001 audit. We will also deepen the concept of *document*, given that their examination is fundamental in audits.

25.1. Documentation for audit and certification process

The documentation of the management system is important to understand the attention that the organization pays in describing processes, policies and collecting documentary evidence.

Documents can belong to two types: *process* or *implementation*.

- The latter are records that can support evidence that *processes, instructions, procedures* and *policies* are in *place*
- Documents are *sampled* by the auditors

The documents *can be* written texts, flow charts, tables or matrices, drawings or sketches, series of sketches, drawings or photographs, audio, video and digital media of various types.

Purpose of the *main information security policy* is:

- Communicate the requirements
- Describe and implement the management system
- Basis for verification
- Ensure continuity
- Reduce the learning curve
- Demonstrate compliance with the standard
- Pre-qualification and contractual objectives
- Pursue continuous improvement especially in such a dynamic sector

Purpose of the *management system manual* is:

- Be a direct collection of policies, procedures and documents
- Be made up of more than one document or layer
- Be a grouping or selection of management system documents
- Be a series of procedures for a specific use or application
- Have a common part with differentiated appendages
- Being (or not) a self-supporting document
- It can be an integrated manual (certified company with more schemes can follow this best practice)

A management system manual usually contains *high-level information* (policy).

- The essential elements are:
  - *Introduction* (containing the objectives, the purpose of the system, the presentation of the company)
  - The *approval* and *modification* procedure, the explanation of the *terminology*, the writing of the system documentation
  - The general description of the management system and all relevant *annexes*

What are the *procedures* for?

- They have to answer the questions "what, why, who, where, when and how"
- They essentially *define the process*

What documentation is needed for the ISMS?

- a) Documents necessary for the organization in terms of *size and criticality*
- b) Documents required by *standards, codes, laws*, etc.
- c) The documentary complex must be like a "dress", it must not be *thin* or *redundant*

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

Let's add *detail* to what we saw in the first lesson (of this second part, keep in mind) by proposing some practical cases related to the auditable chapters of the standard, helping in understanding the principle and logic pursued by the auditors of ISO 27001 based ISMS.

Reconsider the whole standard structure:

- 0 - Introduction
- 1 - Scope
- 2 - Normative references
- 3 - Terms and definitions

These chapters are mostly reading indications and specifications about (e.g.) variations with respect to the previous version of the standard.

- 4 - Context of the organization
- 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

The *scope* must be available as documented information.

- E.g. the country where the organization is located, the laws it must take into account…

In this part, consider for instance:

- 4. *Properly defining the scope of the ISMS*
  - The Beta company, audited in its ISMS, defines its scope as "*protecting information*", and nothing else
  - Such a purpose does not help the organization to be aware of the exact boundaries of the management system, which must *adhere* to a known surface in order to function properly
  - The scope can include one or more *processes, functions, services, sections or places*, an entire *legal* or *administrative entity* and some *suppliers*

Moving on with the standard:

- 5 - *Leadership*
- 5.1 - Leadership and commitment
- 5.2 - Policy
- 5.3 - Organizational roles, responsibilities and authorities

Obtain the commitment of the Management (budget, definition of roles and responsibilities, promote improvement…). The *information security policy* must be available as documented information.

In this part, consider for instance:

- 5. *Participation of top management*
  - In the opening meeting of the Epsilon Inc.'s ISMS audit there are no directors and information security managers, but only the information security operative personnel
  - This *does not* support the requirement to ensure the involvement of top management, for which the *commitment* of those who can ensure the means and resources necessary to achieve the objectives is necessary
- 5. *Budget*
  - Delta Inc. shows in the managerial review, during the audit, the budget allocated to achieve the objectives of the ISMS. Sufficient explanation is not given that the funds allocated have effectively covered the security objectives
  - This translates into a poor consideration of the resources necessary to achieve the goals of the ISMS and, in particular, it is not clear whether these are available, fueling uncertainty about the capabilities and success of the ISMS itself
- 5. *Compatibility of the objectives of the ISMS with the strategic ones of the organization*
  - During the audit, it emerges that Gamma LLP has established, as the objective of the ISMS, that of "*protecting information relating to a printing service*" provided in the past to some customers

- For two years, however, this service has no longer been delivered, but some resources are still being dedicated to the protection of this service, through the adoption of specific security controls that are no longer useful (and unnecessarily expensive)
- This situation might denote a *distance* between the *aims* of the ISMS and the *strategic objectives* of the organization, nullifying resources that could be used more profitably (ISMS serves the purposes of the Organization).

Moving on with the standard:

- 6 - *Planning*
- 6.1 - Actions to address *risks* and *opportunities*
- The main "premise" of risk analysis
  - Based on the context, the Organization must establish how to identify risks and opportunities
  - Guarantee the Result. Establish evaluation criteria. Ensuring «rigor» (comparable results when identifying, analyzing and evaluating risk). Risk treatment (Annex A)
  - The objectives must be consistent with the policy and, if possible, measurable.

Information on the risk assessment process, *"SoA", Risk Treatment Plan* and information security *objectives* must be available as documented information.

- 6.2 - Information security *objectives* and planning to achieve them
- 6.3 - Planning of change

In this part, consider for instance:

- 6. *How many types of risk?*
  - In the risk assessment, Omicron LLP considers the risks of loss of confidentiality, integrity and availability and does not take into consideration the risks that affect the achievement of the goals of the ISMS
  - This is an important mistake, since in order to protect the functioning of the ISMS it is necessary to *first* consider the risk of failure to achieve its objectives and all the factors that can increase it, in order to keep the level under control
- 6. *Actions to address risks and opportunities*
  - Risk: In the risk identification phase, the Alpha company did not formally consider the actions to address risks and opportunities and these actions are not integrated into the organization's processes
  - This is a probable nonconformity, and the standard also requires that *the way* in which implementation takes place is established from the risk identification stage, as well as assessing the effectiveness of these actions
- 6. *Risk acceptance and assessment criteria*
  - The auditor asks the ISMS manager to show, in the risk analysis, where the risk acceptance criteria and the criteria for conducting the risk assessment lie

  - The manager verbally explains what the criteria are, saying that, since the risk is variable, writing them would not allow it to be monitored
  - Such an explanation is unacceptable. The ISMS asks that the criteria be *defined* precisely to allow measurement of effectiveness, as well as to obtain *comparable* results over time
- 6. *Risk Assessment consistency*
  - Pay attention to *scales* for assigning values to *likelihood* and *consequences* of risks
  - Identify all the relevant risks
- 6. *Information security objectives*
  - The Beta company sets the goal for its ISMS to protect classified information that is very sensitive. The information security policy does not include any reference to confidential documents and how to protect them
  - Such a scenario highlights an unfulfilled requirement of the standard. The objectives of the ISMS must be consistent with the general security policy

Moving on with the standard:

- 7 - *Support*
- 7.1 - Resources
- 7.2 - Competence
- 7.3 - Awareness
- 7.4 - Communication
- 7.5 - Documented Information

The Organization *determines* and *provides* competent, knowledgeable resources, establishing the rules for communicating and documenting information.

In this part, consider for instance:

- 7. *Awareness*
  - The auditor notes that the people in the Rho LLP company are in a hurry, they exchange information in the corridors, they switch roles to help each other
  - She then decides to follow the lead trail and interview staff about their role awareness and information security policies. 7 out of 8 people did not know about the information security policy, or did not know where to find it
  - This situation is very serious because people must have a defined *role* and *responsibility* to be *aware of*. Also *people are not aware of the security policy*. Non conformities are very likely in this case

Moving on with the standard:

- 8 - *Operation*
- 8.1 - Operational planning and control
- 8.2 - Information security risk assessment
- 8.3 - Information security risk treatment

The information *certifying* the *operation* of the processes, the *results* of the risk analysis and the risk treatment plan must be *documented* and *stored*.

In this part, consider for instance:

- 8. *Implementation problem*
  - The Lambda company, in a process establishes that invoices of a certain type must be saved in a protected area which is accessed only by authorized persons
  - The auditor, asking a person who is not part of the working group in question, and therefore does not have the authorization, notes that the latter *is able to access the protected area*
  - Furthermore, he realizes that *some invoices have not been saved in a protected area*, but in a shared area
  - The problem of non-implementation here is *twofold*: firstly, the rescue in a protected area does not always happen. Also, some people are allowed to log in even though they don't have to be

Moving on with the standard:

- 9 - *Performance Evaluation*
- 9.1 - Monitoring, measurement, analysis and evaluation
- 9.2 - Internal audit
- 9.3 - Management Review

This part is focused on:

- 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

In this part, consider for instance:

- 9. *Internal Audit*
  - The audit team is preparing to verify how the Beta company meets the performance evaluation requirement of the ISMS
  - The lead auditor asks the head of the internal audit function to produce the audit *program* and *reports*. Internal audit exhibits the documents.

  - The auditor notes that the program includes audits of various processes and services, but although Beta is a provider of a communication service, a key hosting provider who contributes to the provision of the service is *never* audited
  - The audit program must take into account the processes involved, such as the procurement and outsourcing process in this case, which must meet the requirements of the ISMS
- 9. *Management review*
  - The Kappa company has not produced a managerial review for 14 months and, despite having an ISMS for some years, does not contemplate the state of the art from previous managerial reviews
  - Kappa's ISMS is *unlikely* to be certified
  - The managerial review (to be released at least yearly) is *essential* to understand the findings of *nonconformities* and *corrective actions*, the monitoring of *results* and *audits* and, finally, the achievement of the *objectives of the ISMS*

Moving on with the standard:

- 10 - *Improvement*
- 10.1 - Continual improvement
- 10.2 - Nonconformity and corrective action

This part is focused on:

- 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

In this part, consider for instance:

- 10. *Reacting to nonconformities*
  - Sigma, an IT company, has an ISMS that has received nonconformities relating to certain security controls (annex A ISO / IEC 27001) and relating to personnel awareness
  - Sigma reacts only to the first, because it believes that people cannot be intervened and therefore does not take any action.
  - Sigma receives several reports from customers and occasionally opens security incidents
  - *All nonconformities should be reacted to*. Incidents, reports, or complaints are often indicative of a bigger problem that must be faced in terms of accountability towards the actors of the ISMS, of the organization and external, keeping track of what is being done to resolve the situation

25.3. Security controls (countermeasures)

There are a lot of countermeasures, listed as controls in the section "5. Organizational controls".

Between all of them, what we care the most here is *"5.24. Information security incident management planning and preparation"*.

In this part, consider for instance:

- 5. *Incident management*
  - Theta company is asked to audit the incident management procedure
  - Theta shows a document where relevant security incidents are indicated and described, without however indicating who should do what in the event of an accident
  - The problem is that since the roles and responsibilities are not defined, *it is not clear who should carry out the procedures*

There's also the list of people controls (6. People controls), which we care the most about *"6.7 Remote working"*.

In this part, consider for instance:

- 6. *Remote working*
  - Ypsilon, in a period of pandemic, is forced to have its staff work remotely, but many people do not have a company computer manned by the company. Ypsilon does nothing to reduce the risk.
  - If the control is applied in the Ypsilon ISMS, an auditor can only assign a nonconformity. The company should have a *policy* that imposes, for example, the use of the virtual machine, the VPN, physical protection measures of the device, firewall and antivirus, …

There's also the list of people controls (7. Physical controls), which we care the most about *"7.2 Physical entry"*.

In this part, consider for instance:

- 7. *Physical Entry*
  - Phi Inc., a logistics company, leaves a gate open that leads to a freight unloading area
  - An auditor sees a vehicle enter and collect a package undisturbed, without gate control or other measures
  - Poor supervision of an unloading area can lead to the entry of unauthorized persons or vehicles, the theft of assets and other dangers for the organization

There's also the list of people controls (8. Technological controls), which we care the most about *"8.28 Secure coding"*.

In this part, consider for instance:

- 8. *Secure coding*
  - Zeta company LLP develops software for resale, based on market needs. This service (and related processes) is part of the scope of the ISMS
  - Developers are skilled, but used to writing code along the way, without being trained in the specific knowledge of secure software development, without properly configuring an IDE, not regularly updating compilers, planning application security aspects
  - The software used includes libraries obtained from the internet that include many functions, largely unused and unknown, and so on. The auditor finds that A8.28 control is not applied, resulting in nonconformity.

25.4. Most common findings

Some classification of findings and relative results about the audit and certification process:

- A total of 78% of companies audited to ISO/IEC 27001 experienced at least one finding (any category) whilst 40% concluded the audit with at least one severe finding, i.e. with a major non-conformity (Cat1) or a minor non-conformity (Cat2)
- Almost the 40% of the companies had findings related to section A.12, where we find IT system management and, partially, IT network requirements

Here, reported, the list of the top 10 most frequent severe (non-conformity) failures per sub-process:

- Actions to address risks and opportunities - 5%
- Internal audit - 5%
- Management review - 3%
- Review of user access rights - 3%
- Inventory of assets - 3%
- Information security risk assessment - 3%
- Management of technical vulnerabilities - 3%
- Monitoring and review of supplier services - 3%
- Information security objectives and planning to achieve them - 3%
- Identification of applicable legislation and contractual requirements - 2%

A great way to conclude this file, given both you and me survived the atrocious sets of slides and the awfully long, verbose and terribly presented course content - it was exhausting. Made purposefully disgraceful. To represent the atrocious material and course.

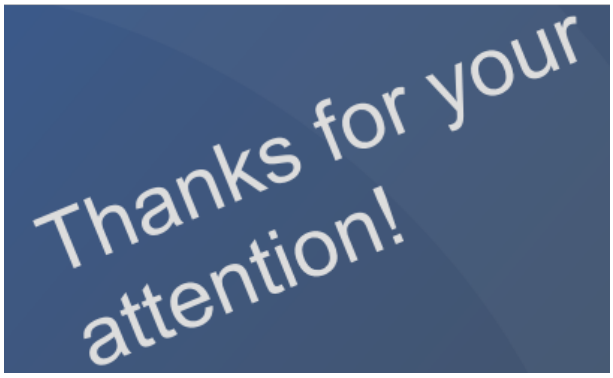

Figure 2: Thank God it's over