Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security
SEGSI

TP08

Risk Management

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Risk Management

- Risk is an ubiquitous element of our life, as well as its management
- Consciously or not, we all manage risk through our choices
  - When crossing a street
  - When changing job
  - When travelling
- On an organization point of view, it is a key activity
- And if that organization provides essentials services to society, the risk
  - Leads to even more important layers
    - Because a failure due to the risks has a heavy impact on society
  - Leads to a bigger and unavoidable threat
    - Because turns it to a possible target

Risk Management

- Regulations have been launched to prevent the risk and the obligations of (by now, some) an organization
  - As seen on TP06 and in EU, Directive released on 2016 and its subsequent application in Portugal Law 46/2018 and Decree-Law 65/2021
- Article 9.º of 65/2021
  - Organizations (entities) must comply with technical and organizational measures to manage the risks posed to the security of the networks and information systems they use
  - These measures must guarantee a level of safety appropriate to the risk involved, taking into account the latest technical progress, through the use of the use of internationally accepted standards and technical specifications applicable to the security of networks and information systems

Risk Management

- Article 10.º of 65/2021 (i)
  - Organizations must carry out a risk analysis in relation to all the assets that guarantee the continuity of the operation of the networks and information systems they use, as follows terms
  - a) Analysis of global risks, at the following intervals:
    - i. At least once a year;
    - ii. Following notification by the CNCS of an emerging risk, threat or vulnerability that implies a high probability of an incident with a relevant impact occurring, within the deadline set by the CNCS;
  - b) Analyzing risks of partial scope, with the following periodicity:
    - i. During the planning and preparation of the introduction of a change to the asset or assets, in relation to the asset or assets involved;
    - ii. After the occurrence of an incident with a relevant impact or other extraordinary situation, in relation to the assets affected;
    - iii. After notification by CNCS of an emerging risk, threat or vulnerability that implies a high probability of an incident with a relevant impact occurring, in relation to the asset or assets involved high probability of an incident with a relevant impact occurring, within the time limit set by CNCS

Risk Management

- Article 10.º of 65/2021 (ii)
  - The risk analysis must cover each asset:
    - The identification of threats, internal or external, intentional or unintentional, including, in particular
    - Failure of a system or in the supply of goods or services by a third party;
    - Natural phenomena;
    - Human error;
    - Malicious attack;
    - Characterization of the impact and probability of occurrence of the threats identified.
  - This risk analysis must take into account
    - The history of extraordinary situations that have occurred, and of incidents with a relevant impact with their respective duration;
    - The number of users affected by the incidents;
    - The geographical distribution, in terms of the area affected by the incidents;
    - Inter-sectoral dependencies for the purposes of service provision

Risk Management

- Article 10.º of 65/2021 (iii)
  - Organizations must document the preparation, execution and presentation of risk analysis results.
  - Following each risk analysis, entities must adopt the appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems they use, and which result in particular from:
    - Complementary sectoral regulations approved by the CNCS, without prejudice to the application of other national and European Union regulations on the security of networks and information systems;
    - The National Cybersecurity Reference Framework, and its complementary provisions, drawn up by the CNCS, in the absence of or in addition to the sectoral regulations provided for in the previous paragraph.
  - The measures to be adopted must enable:
    - Risk prevention, management and reduction;
    - Strengthening the robustness and resilience of assets, including their protection against identified threats and their recovery or redundancy, in order to ensure the rapid restoration of the functioning of networks and information systems;
    - An effective response to incidents, threats or vulnerabilities

Risk Management

- It is expected that organizations perform, maintain and manage the risks associated to their activity
- When starting it for the first time it is always difficult to do it – as they don't have a backlog of problems – but as time goes by, the backlog is usually a helper that should not be underestimated
- Risk analysis should
  - Contain the threats identification, internal or external, with the corresponding impact and probability
  - Take into consideration
    - Historic extraordinary situations
    - The incidents with relevant impact
    - Number of users affected by the incident with their geographic distribution
    - Inter-sectorial dependencies

Risk Management

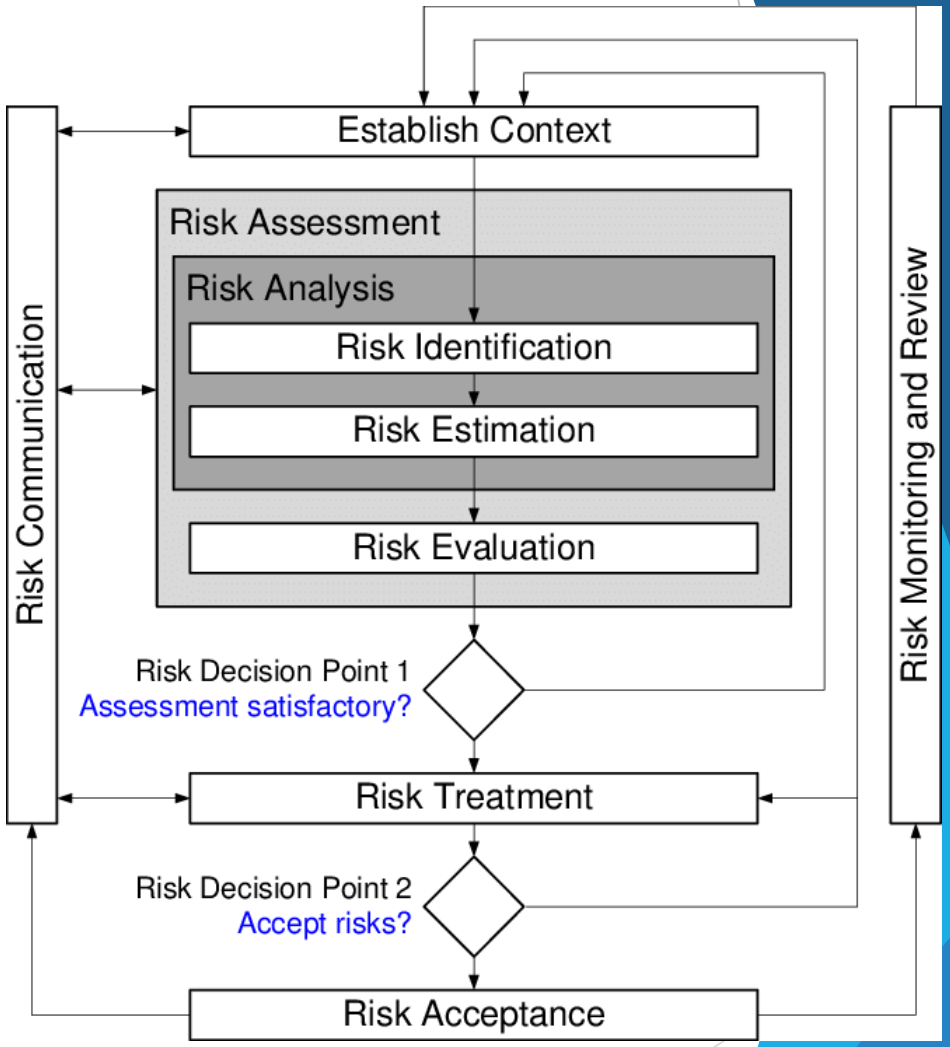
- The preparation, execution e results presentation of risk analysis must be documented
- For each risk, the planned technical and organizational actions to manage it must also be documented
- The planned actions should allow
  - Management, prevention and mitigation of the risk
  - Enforcement and resilience of the actives
  - A quick and effective response to incidents, threats and / or vulnerabilities

Risk Management

- The actual situation of the organization must be characterized, objectives to mitigate the risk with the planned actions must also be documented
- The national authority might define technical instructions to assess a common line of risk matrix for all organizations
  - In Portuguese terms, the Centro Nacional de Cibersegurança, CNCS, has released in April 2023 a guide for risk management
- According to the instructions of the National Authority for Cybersecurity (CNCS for Portugal), organizations must update periodically their risk management – at least, once a year –, or whenever necessary and adopt appropriate technical and organizational measures

Risk Management

- Risk management is (or can be, depending on the instructions of the national cybersecurity authority) based on ISO 27005, which is composed by 8 phases



Risk Management – phase 1

- Establish context
  - It involves a series of base criteria to risk management
    - Organization on risk management
      - Identify applicable human resources and materials to prosecute a correct execution of all the process
    - Risk management approach
      - Adopt a risk management framework and the correspondent policy and procedures
    - Definition of scope and boundaries
      - Of risk management and information organization
    - Define criteria of risk evaluation
      - identify the criteria for assessing the relevance of the risk, considering the strategic value and/or criticality of the assets and/or operational and commercial importance. importance

Risk Management – phase 2

- Risk assessment
  - It's the first *real* phase of risk assessment stage
    - Active identification
      - The ones that support the scope defined in information security risk management
    - Vulnerabilities identification
      - Identification and selection the vulnerabilities related with each device
    - Threats identification
      - For each vulnerability, identify and select some potential threats
    - Controls identification
      - Identify existent controls, describing its implementation maturity and /or usage
    - Assess overall impact
      - Might include potential consequences like needed time to investigate and repair, wasted work time, etc.

Risk Management – phase 3

- Risk analysis
  - It is recommended to include
    - Impact on cybersecurity objectives
    - Legal or regulatory impact
    - Impact on clients
    - Economical impact
    - Reputation impact

Risk Management – phase 4

- Risk assessment
  - Must be connected with last part of phase 1, that should be reviewed accordingly
  - It is recommended that when documenting this phase
    - It is supported by the risk evaluation criteria defined in the context
    - The risk management are consistent with the internal and external context
    - The decisions taken for risk evaluation are based, mainly, on the acceptable risk level of the organization
    - The risks are prioritized with the defined evaluation criteria and related with the identified incident sceneries

Risk Management – phase 5

- Risk treatment
  - These are the ones previously presented
    - Avoid
    - Transfer
    - Mitigate
    - Accept
  - Residual risks might exist; they should be undermined here
    - Residual risk is the remaining risk that remains after executing the risk treatment activities
  - An update or revisiting the evaluation phase might be considered necessary, taking as a base the expected effects by the implementation of proposed risk treatment

Risk Management – phase 6

- Risk communication
  - It is recommended that the information and decisions regarding risks are shared with all the relevant interested parties
  - That would allow to
    - Ensure the outcome of the organization’s risk management
    - Sharing the results of the risk assessment, presenting the risk treatment plan and raising awareness about the importance of the risk management process
    - Support decision-making and provide decision-makers and the organization's stakeholders with a demonstration of responsibility for the risks
    - Co-ordinate with other stakeholders and plan responses to reduce the impact of incidents

Risk Management – phase 7

- Risk monitoring and review
  - It is recommended that risks and their factors are monitored and reviewed on a regular basis, in order to identify any changes that could result in a change in the organization's perception of risk
  - It is suggested to continuously monitor
    - New assets or changes in the criticality of assets for the entity
    - New active threats, both inside and outside the organization, which have not yet been assessed
    - New vulnerabilities being exploited by new threats
    - Possible increase in the impact, consequences of threats, vulnerabilities or grouped risks resulting in an unacceptable level of risk
    - Information security incidents that may occur
    - Unexpected patterns of traffic

Risk Management – phase 8

- Document all the processes, decisions and their analysis and any other assumptions and their framing taken during the previous phases is mandatory
- This is critical, as it can be used to show stakeholders - such as supervisory authorities and stakeholders - the organization's commitment and its systemic risk management
- It also allows the organization itself to validate its efficiency on risk management
- Previous versions of all documents make it possible to assess its continuous improvement