Bruno Sousa, bmsousa@dei.uc.pt
2024/2025

Worksheet #2 –Risk Management

Practical Lectures #3, #4

OBJECTIVE:

Understand the process of analyzing, evaluating, and planning risk management activities.

CONTEXT:

The risk management process aims to identify, assess, and take steps to reduce an enterprise's risk to an acceptable level. The management of risk comprises three main steps: i) risk identification - recognition, enumeration, and documentation of risks; ii) risk assessment – determining to which extent assets are exposed to risk; and iii) risk control – measures that allow to control and reduce risks to acceptable levels.

EXERCISE:

Following the risk management frameworks and methodologies discussed in class, define a risk management plan for an organization (e.g., school, hospital, a software development company).

In the Exercise you need to **provide information** regarding (*#List 1*):

- Infrastructure (building, physical goods, vehicles, etc)
- Technological infrastructure (e.g., Information System, Communication networks)
- Employee information: researchers and other staff
- Financial/insurance and business planning data
- Public Data and presence on social media (Internet)

The risk management plan shall include the following steps:

1. **Risk identification:** including asset valuation, threat identification, vulnerability assessment, and Threat-Vulnerabilities-Assets (TVA) specification.
2. **Risk assessment:** including determining loss frequency, evaluating loss magnitude, risk calculation, and documentation.
3. **Risk control:** including control strategies, examples of security controls to implement, and a monitoring and re-assessment plan.

Each of these steps should cover all the assets and controls.

REPORT (WHAT TO DELIVER):

The report must include the following information:

1. Organization you choose and respective assumptions (Does it has security policies?)
2. Information items included in *#List 1*
3. TVA with risk Identification
4. TVA with Risk Assessment
5. TVA with Risk Control

Note: you can deliver a pdf document with information of points 1 and 2 and an Excel file with points 3-5.

READINGS:

- NIST. SP 800-37
- NIST. SP 800-39
- NIST. SP 800-30
- Whitman, M., & Mattord, H. (2017). Principles of Information Security (6 ed). Cengage Learning. **(Chapter 5)**
- Schumacher, M., Fernandez-Buglioni, E., et al (2006). *Security Patterns: Integrating security and systems engineering*. John Wiley & Sons. **(Chapter 6)**
- **NIST SP 800-39**, Managing Information Security Risk Organization, Mission, and Information System View