**Information Security Overview**

**Confidentiality:** guarantees that only authorized users can view sensitive information

**Integrity**: guarantees that only authorized subjects can change sensitive information

**Availability**: guarantees uninterrupted access by authorized users to important computing resources and data

**Asset**: Anything with value to an organization. It can be a router, servers, hard drives, laptops or can be databases, spreadsheets, trade secrets

**Vulnerability:** is a weakness in the system design, implementation, software, or code, or the lack of a mechanism. We can find vulnerability in: applications, operating systems, hardware, misconfigurations.

**Threats**: is any potential danger to an asset.

**Exploit**: piece of software, a tool, a technique, or a process that takes advantage of a vulnerability that leads to access, privilege escalation, loss of integrity, or denial of service on a computer system

Sometimes no one may even know the vulnerability exists, and it is exploited. That is known as a zero-day exploit.

**Countermeasure or safeguard**: a protection that reduces or mitigates a potential risk

**Categories of vulnerabilities**: design errors, protocol weaknesses, software vulnerabilities, misconfiguration, human factors, hostile code

Industry that classifies and keep track of vulnerabilities: CVE (Common Vulnerabilities and Exposures) National Vulnerability Database

**Risk**: is the probability or likelihood of the occurrence or realization of a threat.

**Risk management options:**

* **Risk acceptance**: it is use when the cost of other risk management options such as avoidance may outweigh the cost of the risk itself
* **Risk avoidance**: action that avoids any exposure to the risk. It is the most expensive risk mitigation option
* **Risk limitation**: limits a company’s risk exposure by taking some action. It is the most commonly used risk mitigation strategy.
* **Risk transfer**: is the transference of risk to a willing third party

**Vulnerability assessment (test)**

The objective of a vulnerability assessment is to ensure that network and the information systems are tested for security vulnerabilities.

Activities that are performed during the vulnerability assessment process:

* Device discovery (identify, ping, TCP SYN scan)
* Service enumeration (TCP ports, UDP ports, web services)
* Scanning (configuration issues, missing patches, dangerous services)
* Validation

**CVSS**

* CVSS: free and open industry standard for assessing the severity of computer system security vulnerabilities
* It allows vendors to better analyze the impact of security vulnerabilities
* Current version CVSS 3.0