AST

Audit de Sécurité Technique

Chapter 1.1
Principles of Information Security

Abraham Rubinstein / Jean-Marc Bost

abraham.rubinstein@heig-vd.ch / jean-marc.bost@heig-vd.ch

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Information Security

Information Security - protection of information for a wide range of threats in order to ensure business continuity, minimise risk, and maximise return on investments and business opportunities.

- Preservation of confidentiality, integrity, and availability of information.
- In addition, authenticity, accountability, non-repudiation, and reliability are also involved

Information?

- Meaningful data
  - Printed or hand written
  - Recorded using any technical support
  - Transmitted
  - On a website
  - Mentioned during conversations
  - Etc…
- Asset: anything having value to the organisation
  - information
  - software
  - equipment (e.g. computers)
  - services
  - people
  - reputation and image

Information classification - to ensure that information receives an appropriate level of protection in terms of its value, legal requirements, sensitivity and criticality.

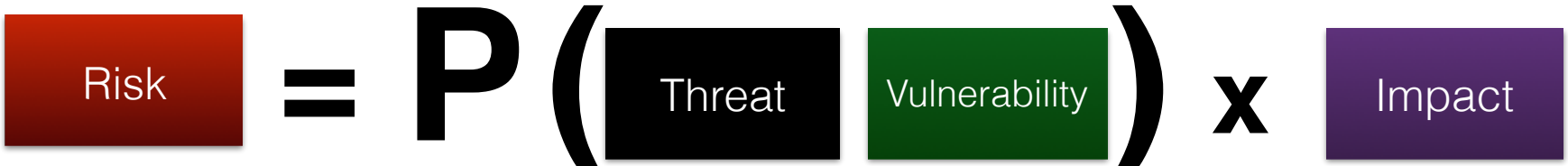
InfoSec triad - CIA

- **Confidentiality** - property that the information is not disclosed to unauthorised entities.
- **Integrity** - property of protecting the accuracy and completeness of information.
- **Availability** - property of information being accessible and usable upon demand by an authorised entity.

Vulnerability, Threat and Impact

- **Vulnerability** - weakness of the system/infrastructure.
  - Insufficient maintenance, lack of code review, lack of logs, lack of encryption, lack of segregation of duties.
- **Threat** - entity or event causing a harm and disruption to organisation and business.
  - fire, flooding, theft, unauthorised access, wiretaps, security bug
- **Impact** - effect or influence of an event with consequences to the organisation and business
  - Confidentiality impact - sensitive information leakage, invasion of privacy
  - Integrity impact - accidental or deliberate change of information, incorrect or incomplete results, loss of data
  - Availability impact - service interruption, unavailability of service, disruption of operations.

Risk



Probability that a given Threat will exploit a Vulnerability and cause a given Impact to the organisation.

Threat-Vulnerability Relationship

- By itself, the presence of a vulnerability does not lead to a risk
  - Threat must exist to exploit it
- A Threat which cannot exploit any vulnerability cannot represent a risk neither.

Vulnerability	Threat
lack of code review	security bug
lack of encryption	information theft
lack of logs	fraud
no segregation of duties	unauthorized use of the system

Risk Definitions

- Risk Management - coordinated activities to control an organisation with regard to risk
- Risk Treatment - process of selection and implementation of measures to modify risk
- Risk Evaluation - process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
- Risk Assessment - process of risk analysis and evaluation
- Risk Acceptance - decision to accept a risk
- Residual Risk - the risk remaining after risk treatment

Risk Scenario

- Relationship between concepts

A subcontractor of an infamous intelligence agency decides to whistleblow.

Asset	State secrets
Security aspect	Confidentiality
Vulnerability	Segregation of duties
Threat	Information theft
Impact	Intel sensitive data leakage

Controls

- Control - method to manage risk
  - Policies, procedures, guidelines, practices and organisational structures
  - Technical controls - controls related to the use of technical measures or technologies such as firewalls, alarm, CCTV, IDS
  - Administrative controls - controls related to organisational structure such as segregation of duties, job rotation, job description, approval processes.
  - Managerial controls - controls related to the management of personnel (training, coaching), management reviews and audits.
  - Legal controls - controls related to the applications of a legislation, regulatory requirements or contractual obligations.

Controls

- ISO 27001 classifies controls in three categories:
  - Preventive
    - Detect problems before their occur
    - Example: publish information security policy, have a confidential agreement signed by employees, segregation of duties.
  - Detective
    - search for, detect and identify problems
    - Example: monitor ressources and services, alarm triggering, regular review of user access rights, analysis of audit logs.
  - Corrective
    - solve problems found and prevent the recurrence
    - Example: Forensics following a security incident, patching following publication of technical vulnerabilities.

Operating mode of controls

- Manual control - control requiring human intervention
  - Example: conducting interviews, providing an authorisation, completing forms, auditing
- Automated control - control operated by a logical or a physical system
  - Example: validating data input, fire detector, alarm
- Mixed control - control requiring both human activity and t least one automated control to be in-use
  - Backup of files and verification of data integrity by the admin