Information System Security

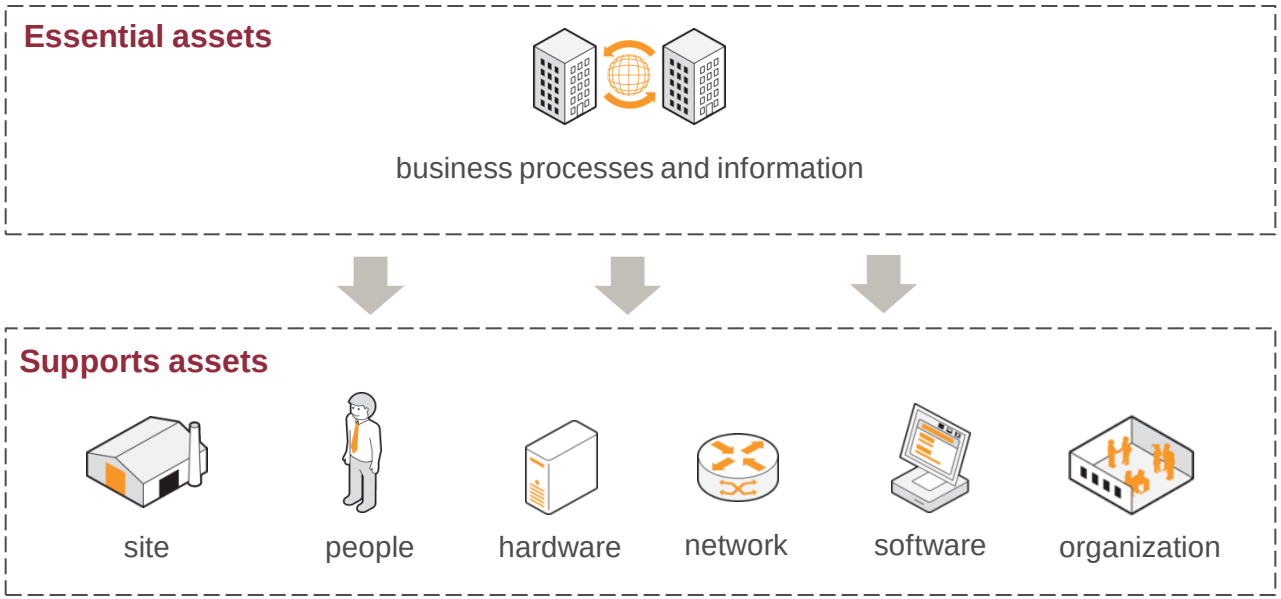
Risk Analysis

Summary

- Stakes of security
- Security needs
- Vulnerability, threat, attack and risk
- Integrate security into projects

Stakes of security

- An information system of an organization contains a set of assets:



ISO/IEC 27005:2013

The Information System Security consists in ensuring the security of all these assets

Stakes of security

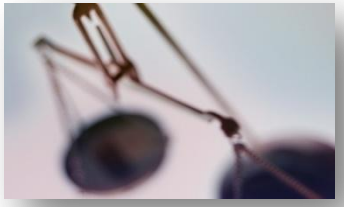
- **Risk is the combination of the likelihood of an event and its impact**
  - Security aims to reduce the risks to the information system, to limit their impact on the operations and business activities of organizations

Financial Impacts

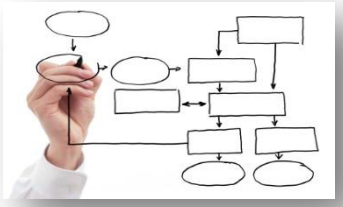
Impacts on image and reputation

IS Security

Legal and regulatory impacts



Organizational impacts



Stakes of security

Example of security impact on privacy

- Image impacts :
  - ✓ Defamation
  - ✓ Disclosure of personal information
  - ✓ Harassment
- Identity theft :
  - ✓ Theft and reuse of logins / passwords to perform actions on behalf of the victim
- Definitive loss of data :
  - ✓ Ransomware
  - ✓ Fraudulent connection to a cloud account and malicious deletion of all data
- Financial impacts :
  - ✓ Credit card spoofed and reused for online purchases
  - ✓ Blackmail (disclosure of compromising information if ransom not paid)

Stakes of security

Security impact on critical infrastructure

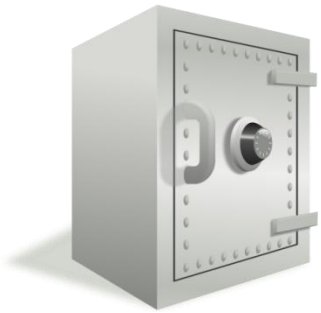
- Critical Infrastructure : set of organizations considered to be **critical** to the nation
- France requires that **special security measures** must apply to these organizations :
  - ✓ Sectors of citizen protection: health, water management
  - ✓ Sectors of economic and social life: energy, communication, electronics, audiovisual, transport, finance…

- These organizations are classified as **Operators of Vital Importance** (OIV). The exact list is classified (therefore not available to the public).

Security needs

- **How to define the security level that we need for assets?**
- **3 criteria are used to answer this problem, known as C.I.A.**

Asset to protect

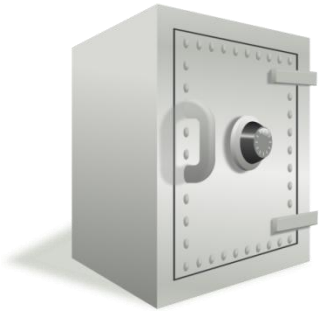


- **Confidentiality**
  Ability to protect information from unauthorized disclosure
- **Integrity**
  Ability to provide accurate and complete information (i.e. illegitimate modification should not be possible)
- **Availability**
  Ability to provide the information during the intended ranges of use

Security needs

- **1 additional criterion is often associated with C.I.A.**

Asset to protect



- **Proof**
  Ability to provide audit trails and evidence corresponding to actions performed on the information.

  ➢ This property includes:

  ✓ Traceability of the actions

  ✓ User authentication

  ✓ Accountability of the person responsible for the action

Security needs

Evaluation for C.I.A. need

- Metric for confidentiality evaluation :

Level	Impact	Description
0	None	Public information
1	Minor	Internal use
2	Serious	Restricted
3	Major	Confidential
4	Catastrophic	Secret

- Confidentiality level for institutional website : 0 (public information only)
- Confidentiality level for commercial website : 3 (confidential because of credit card numbers)

Security needs

- **Evaluation for C.I.A. need (scale from 0 to 4)**
  - Example for institutional (static) website of a company that wants to promote its services on the internet:

Availability = 3

A high level of availability of the website is necessary, otherwise the company can not achieve its goal of publicizing its services to the public

Integrity = 3

A high level of integrity of the information presented is necessary. The company does not want a competitor to fraudulently modify the content of the website to insert erroneous information

Web server

Confidentiality = 0

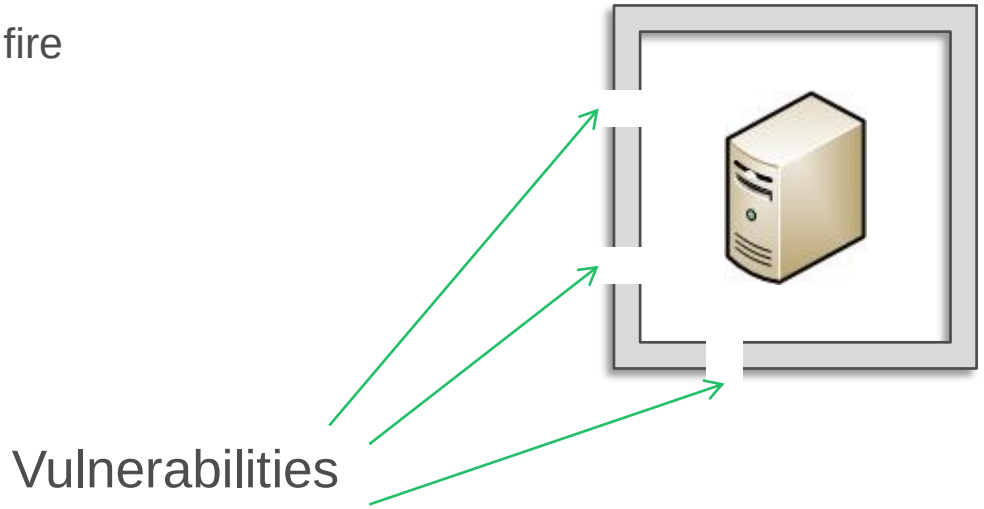
A low level of confidentiality is enough. The information contained in this website is public by nature

Proof = 0

A low level of proof is enough. This website does not allow any interaction with users, it simply provides fixed information

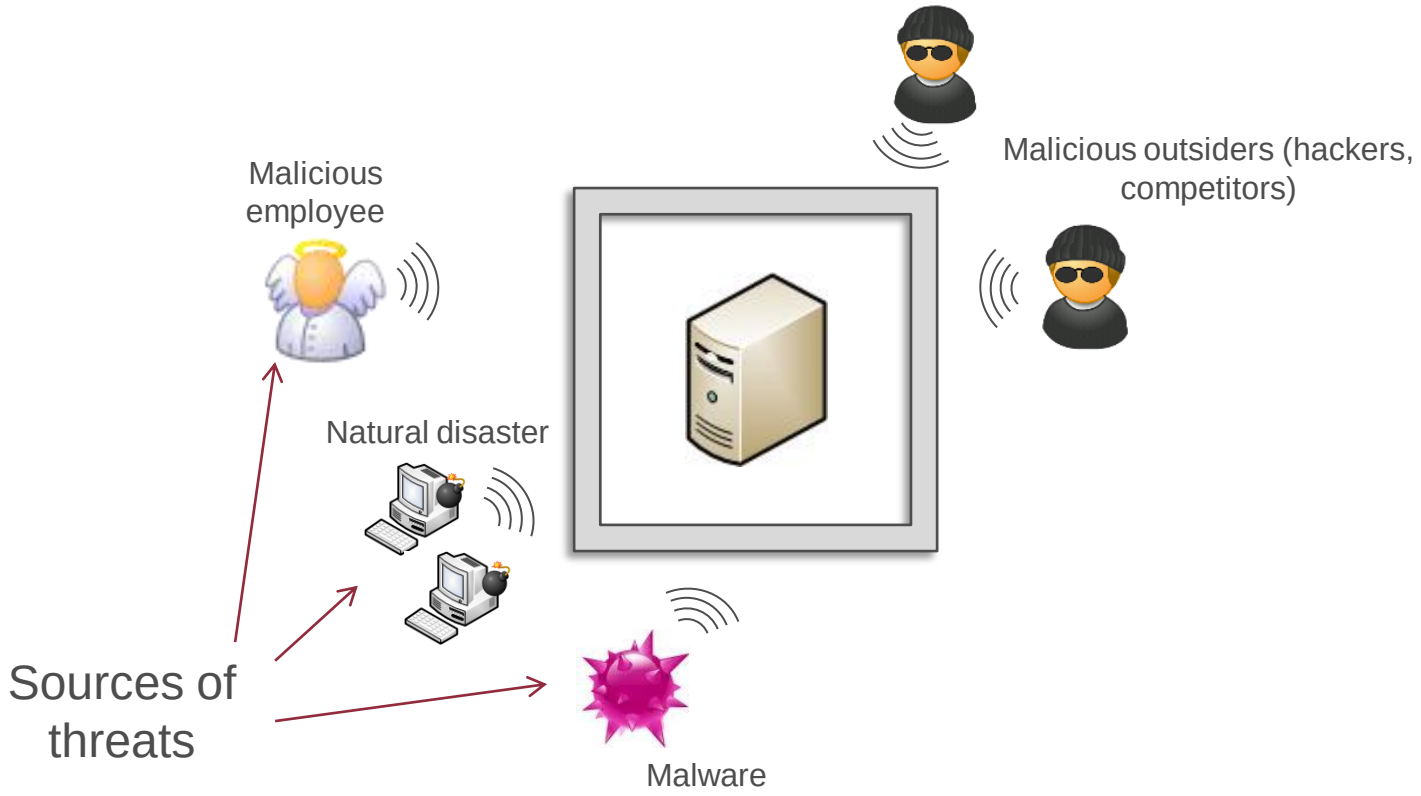
Vulnerability, threat, attack and risk

- **Vulnerability : Weakness in an asset (in the design, construction, installation, configuration or use of the property)**
  - Examples :
    - ✓ Absence of means to fight fire
    - ✓ Absence of encryption
    - ✓ Bad sizing of resources
    - ✓ Inappropriate skills
    - ✓ …



Vulnerability, threat, attack and risk

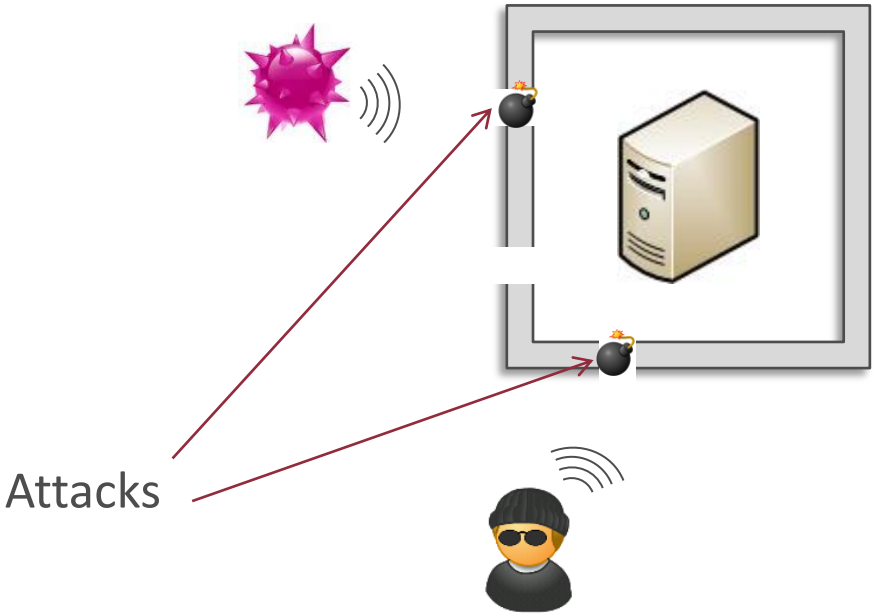
- **Threat : Potential cause of an incident that could result in damaging the asset if the threat materializes**



Vulnerability, threat, attack and risk

- **Attack : Malicious action intended to affect the security of an asset**

- **An attack represents the realization of a threat, and requires the exploitation of a vulnerability**



Vulnerability, threat, attack and risk

- An attack can only take place (and succeed) if the asset is affected by a vulnerability

The work of security experts is to ensure that the IS has no vulnerability

In reality, the goal is actually to be able to master these vulnerabilities rather than aiming to no vulnerability

Vulnerability, threat, attack and risk

- **Definition of the risk : it is a scenario which combines :**
  - A feared event (sources of threats, essential assets, criterion of security, security needs, impacts)
  - One or more scenarios of threats (sources of threats, support assets, criterion of security, threats, vulnerabilities)

- **Its level is estimated by its <u>severity</u> (significance of the impacts) and its <u>likelihood</u> (possibility that it is realized).**

Vulnerability, threat, attack and risk

- **Scale for severity of feared event (related to security need) :**

Level	Severity
0	Insignificant
1	Minor
2	Moderate
3	Major
4	Catastrophic

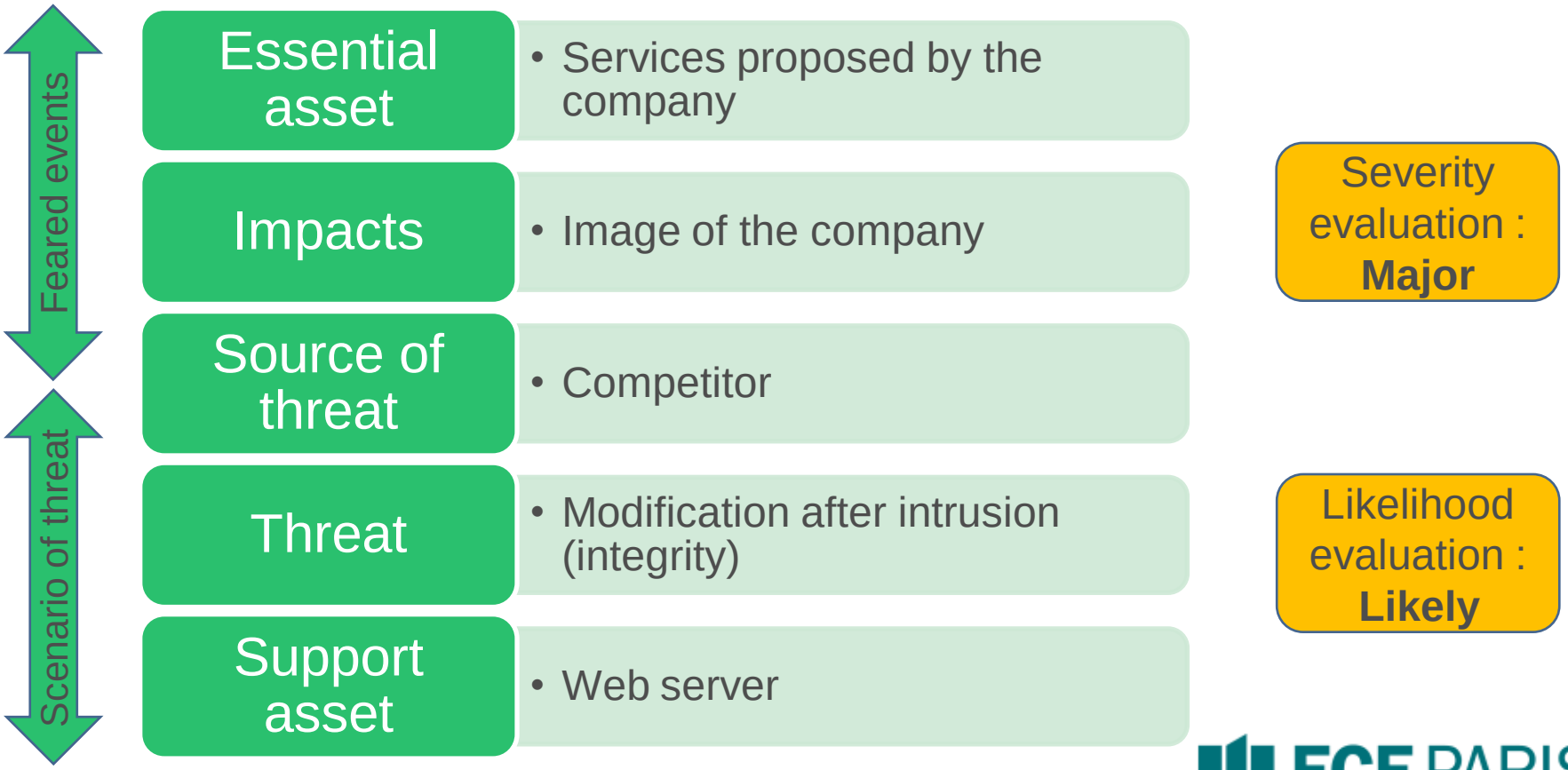
- **Scale for likelihood for scenario of threat :**

Level	Likelihood
0	Rare
1	Unlikely
2	Possible
3	Likely
4	Almost certain

Vulnerability, threat, attack and risk

Example of risk

- Institutional (static) website of a company that wants to promote its services on the internet



Vulnerability, threat, attack and risk

- **Example of risk**
  - Institutional (static) website of a company that wants to promote its services on the internet

- **Level of risk :**

Severity \ Liklihood	Rare	Unlikely	Possible	Likely	Almost certain
Catastrophic	Medium	Medium	High	Critical	Critical
Major	Low	Medium	Medium	High	Critical
Moderate	Low	Medium	Medium	Medium	High
Minor	Very low	Low	Medium	Medium	Medium
Insignificant	Very low	Very low	Low	Low	Medium

Integrate security into projects

- **Take into account as soon as possible the ISS risks in IS projects**
  - To prevent security incidents
  - To implement an intrinsically secure IS, rather than securing an already existing IS
- **Have an IS offering a level of security in line with the needs of the business and the company**
  - In line with the security sensitivity expressed by the business and the level of risk accepted by the business
  - In line with the security standards of the company
- **Helping project leaders to acquire reflexes to integrate security aspects**
  - Without security only appearing as a constraint (complexity, delay, cost ...)

Integrate security into projects

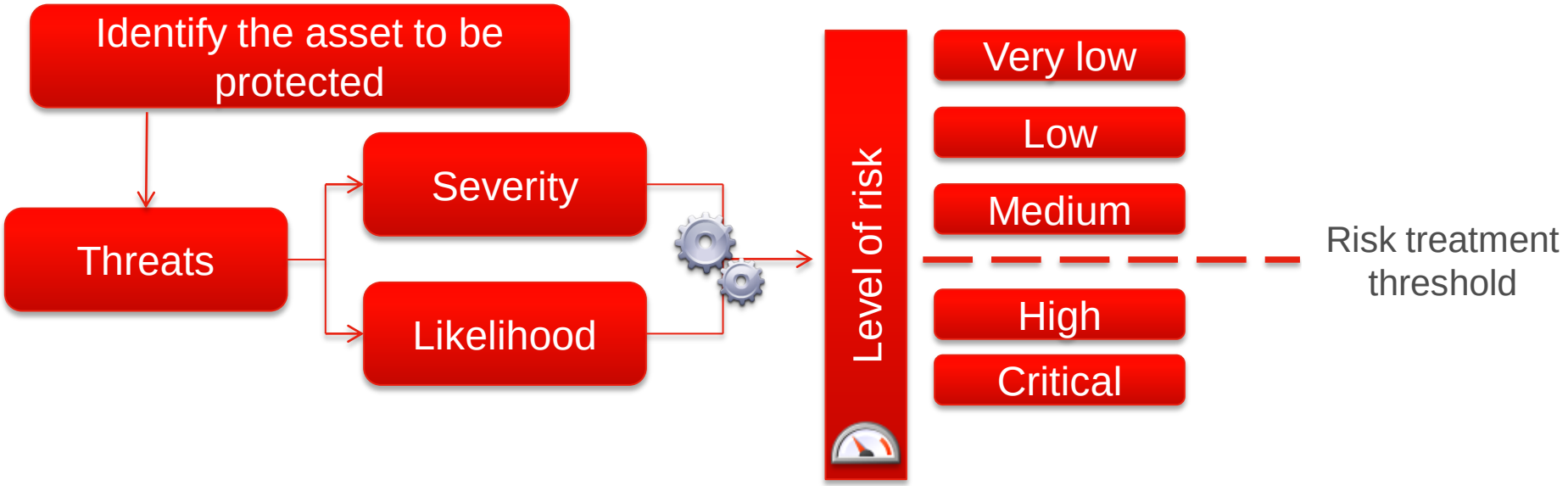
- **Risk Analysis Approach**
  - The risk analysis must be carried out before the project but must also evolve as the system operates (**continuous improvement**)

- **The risk analysis consists in:**
  - identifying the assets to be protected
  - analyzing the frequency and severity of danger to assess the criticality of the risk
  - establishing a threshold of acceptability for every risk
    - ✓ threshold beyond which the risk must be taken into account by security measures
  - identifying security measures

- **The identified measures can constitute a <u>security specification</u> for the project whether it is carried out internally or outsourced**

Integrate security into projects

- **Risk Analysis Approach**

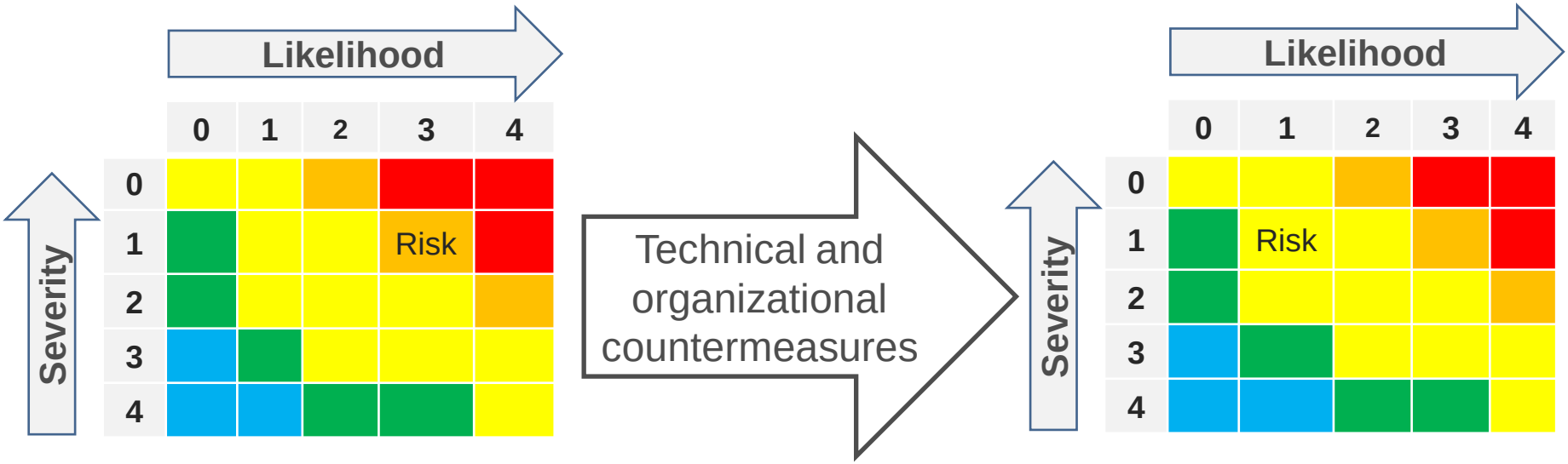


- **Risk prioritization identifies risks that:**
  - must be treated (reduced by measures)
  - those that are acceptable and with which the system can exist

Integrate security into projects

Risk treatment

- For risks with **higher** level than the threshold :
  - ✓ Define the **technical and organizational measures** that will reduce the risk
- For risks with **below** level than the threshold :
  - ✓ a **residual risk** is the risk remaining after the risk treatment (because the cost to compensate for this risk is too high compared to the risk incurred)



Integrate security into projects

- **Risk treatment options :**
  - Risk Reduction : selecting appropriate security objectives and measures
  - Risk Acceptance : accepting the current risks without complementary actions
  - Risk Transfer : transferring to a third-party, for example through insurance
  - Risk Refusal : abandoning the activity or the field of origin of the risk

- **The risks remaining after the risk treatment are the <u>residual risks</u>**

Integrate security into projects

Example of technical countermeasures	
Antivirus	Technical mechanism to detect any virus attack that has already been identified by the security community
Cryptography	Mechanism for implementing encryption and electronic signatures
Firewall	Equipment to isolate network zones and to allow only some flows to pass through
Logical access control	Mechanisms to restrict read / write / delete access to resources only to those who are duly authorized
Physical security of equipment and premises	Mechanisms to protect the physical integrity of equipment and buildings / offices (guardians, locks)
Example of organizational countermeasures	
Auditing capacity	Organizational mechanisms to ensure the effectiveness and appropriateness of the measures implemented
Contractual terms with partners	Mechanisms to ensure that partners and providers implement the necessary security measures
Training and awareness	Mechanisms of which purpose is to explain to all the people in an organization how their actions affect the security of the IS

Integrate security into projects

Risk analysis methodologies

- A risk analysis can be quite complex and requires rigor and method, we must find the right level of abstraction
- Here are 3 examples of risk analysis methodologies that are compatible with the guidelines of ISO 27005:
  - ✓ **EBIOS**: Expression of Needs and Identification of Security Objectives
    - developed by the EBIOS Club in which ANSSI participates, the French Agency for the Security of Information Systems
  - ✓ **MEHARI**: Harmonized Risk Analysis Method
    - developed by CLUSIF, French Information Security Club
  - ✓ **OCTAVE**: Operationally Critical Threat, Asset, and Vulnerability Evaluation
    - developed by Carnegie Mellon University

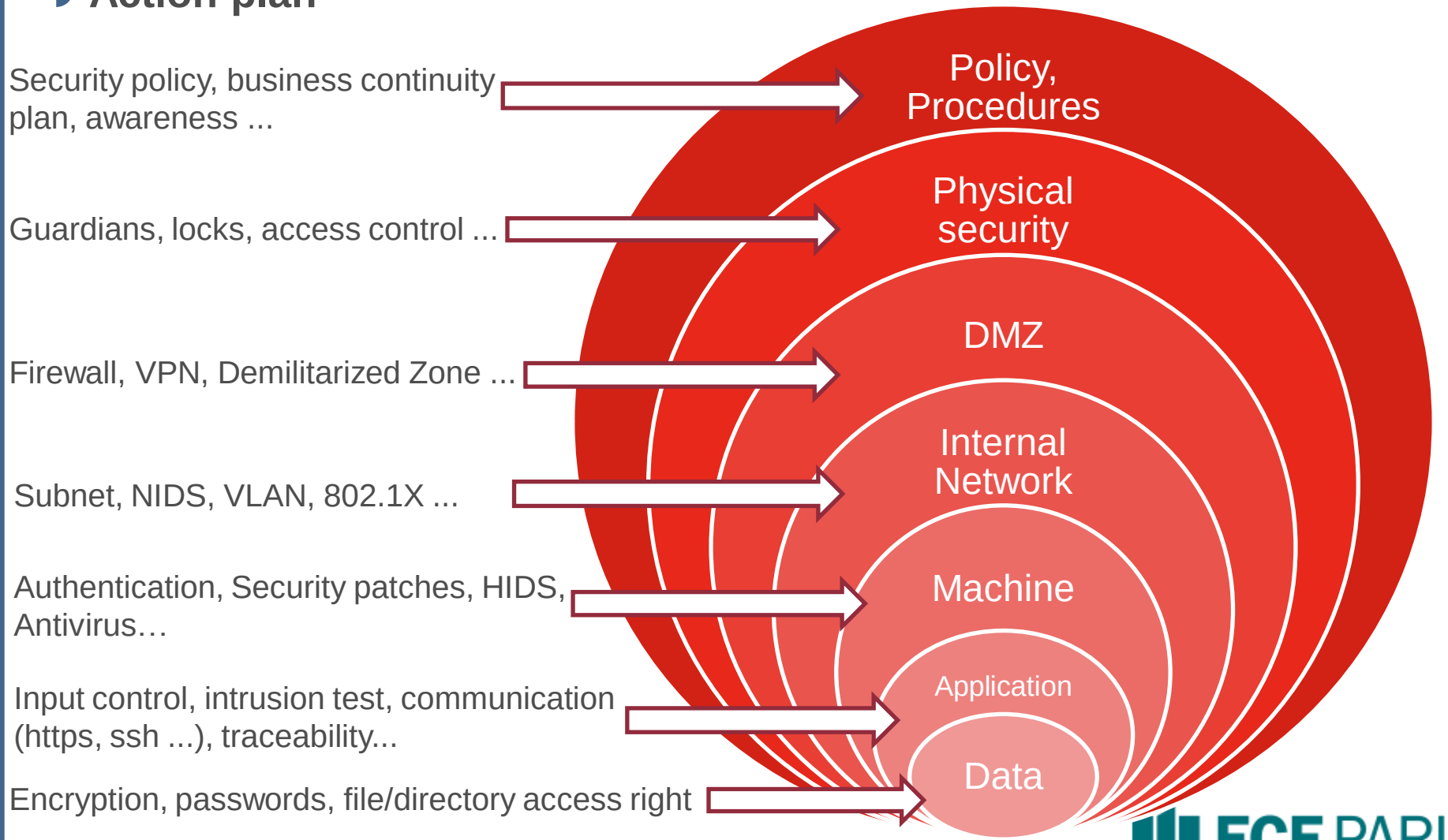
Integrate security into projects

Action plan

- The challenge of implementing security measures is **asymmetric** between "attacking" and "defending":
  - ✓ The attack can succeed by exploiting **a single** vulnerability
  - ✓ Whereas the defense has to take into account **the whole** system
- An action plan for the security measures that must be put in place following the risk analysis should respect the principle of "**defense in depth**" which recommends:
  - ✓ to have several lines of independent defenses
  - ✓ that each line constitutes an autonomous barrier against attacks
  - ✓ the loss of a line of defense implies moving to a higher level of defense
- The objectives of defense in depth are:
  - ✓ prevent, block, limit, detect, alert, react, repair

Integrate security into projects

Action plan



Conclusion

- **The security of information systems:**
  - An indispensable element of a project
  - Must be comprehensive and consistent, not an accumulation of security measures and products
  - Can be implemented with a realistic and pragmatic security policy
  - Goes through the knowledge of the information system (cartography) and its level of security (control, audit)
  - Is a difficulty and a necessity
  - Needs for skills and professionals (increase in security needs)