Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security
SEGSI

TP02

Business Continuity Plan

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

Business Continuity Plan

- A BCP does not have a formal template, however there are some parts that must / should be included
- As a principle, it must / should be and / or provide:
  - Multidisciplinary
  - Proportional
  - Integrated
  - Timely action
  - Re-evaluation
  - Awareness raising
  - Continuous protection

Business Continuity Plan

- Multidisciplinary
  - Security must take into account a variety of perspectives (administrative, technical, organizational, commercial, legal, etc.)
- Proportional
  - Security must be implemented in accordance with the anticipated risks and only about them
- Integrated
  - Security must be coordinated and integrated in order to create a global security system

Business Continuity Plan

- Timely action
  - Stakeholders must take coordinated and timely action on security threats and vulnerabilities
- Re-evaluation
  - Security should be periodically reassessed to identify changes in security requirements
- Awareness raising
  - Users must be aware of and properly sensitized to existing security measures
- Continuous protection
  - Security must be continuous, without any interruption

Business Continuity Plan

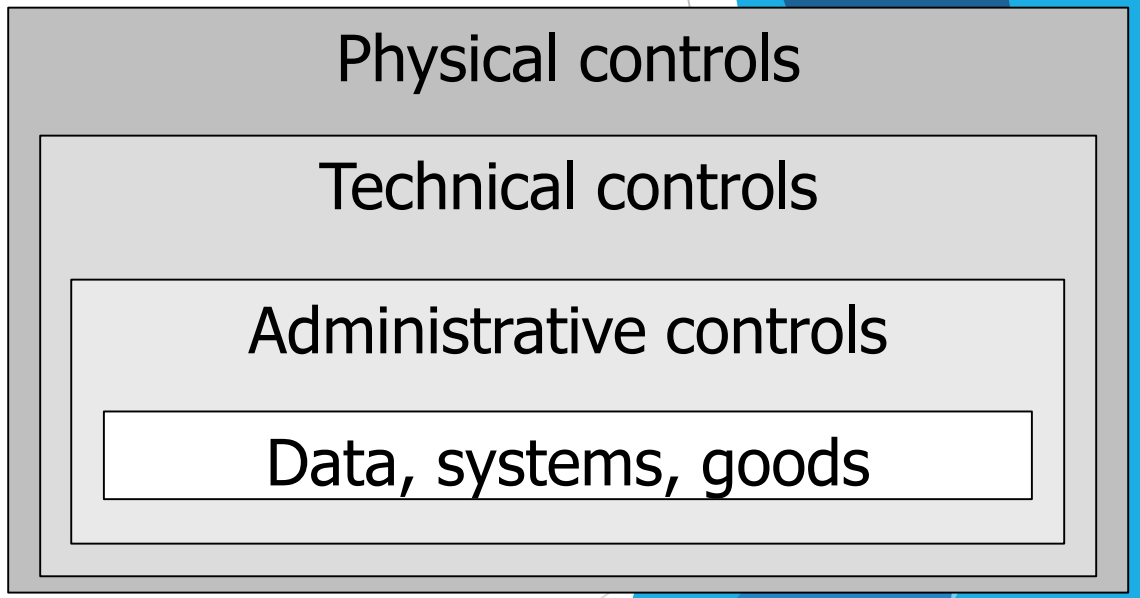
- Definitions
  1. Definition of the team responsible for implementing and maintaining security
  2. Analysis of needs and procedures
  3. Identification of critical processes
  4. Information classification
  5. Drawing up standards and procedures
  6. Definition of sanctions or penalties for non-compliance with the policy
  7. Implementation (followed by reviews)

Business Continuity Plan

- Adequacy of a security policy
  - Accessibility for all members of the organization
  - Definition of security objectives, including a succinct analysis of all the aspects addressed
  - Justification of the options taken
  - Definition of the rules to be applied, who is responsible for them and the contact details for clarifying questions
  - Specification of the consequences of non-compliance with the rules defined
  - Definition of the level of privacy guaranteed to users
  - Definition of the treatment of omitted situations

Business Continuity Plan

- The BCP intention is to define control metrics to assure the security of all parts of the infrastructure
- The controls might be
  - Administrative: policies, guidelines, etc.
  - Technical: access control, encryption, etc.
  - Physical: facilities, guarding, intrusion, etc.



Business Continuity Plan

- When analyzing and defining the SLA (*Service Level Agreement*) the main components should be
  - Business Impact Analysis (BIA)
    - Identifies the critical activities of the organization and its dependencies; this way allows prioritizing recovery operations after a disruption
  - Risk Assessment (RA)
    - Constituted by scenarios that can affect business continuity, the probability of occurring and their impact

Business Continuity Plan

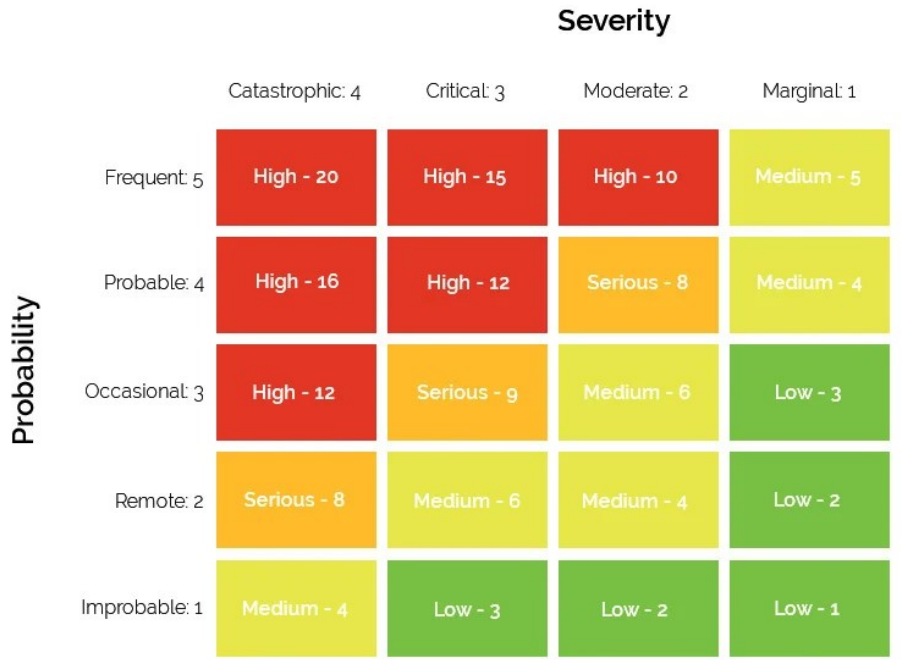
- Risk Assessment (RA) is usually represented by a risk matrix
- Each item has an associated probability and estimated impact (severity); the product of these factors gives a measure for the risk

  Risk = Impact x Probability

- Note: some defends

  Risk = (Impact x Probability)/(1+ Implemented Defenses)

- Considering probabilities on a scale of 1 (least possible) to 5 (most possible) and impact on a scale of 1 (marginal) to 4 (catastrophic), we have



Source: Industry Safe

Business Continuity Plan

- *Risk assessment* must be defined for all risks identified
- There may be no need to build the risk matrix, but having it helps to determine the most worrying risks and reduce (mitigate) them
- But it is important that in BCM the threats considered and their risk classification are defined
  - Also for the formula that is applied to calculate the risk

Business Continuity Plan

- The plan by itself must contain the following parts
  - Policy
  - Standard / Baseline
  - Guideline
  - Procedure

(based on SANS)

Business Continuity Plan

- Policy
  - A formal, brief, high-level statement or plan that encompasses an organization's general beliefs, goals, objectives and acceptable procedures for a specific subject area
  - Policy attributes include the following
    - Require compliance (mandatory)
    - Failure to comply results in disciplinary action
    - Focus on desired results, not on means of implementation
    - Further defined by standards and guidelines

Business Continuity Plan

- Standard / Baseline
  - A mandatory action or rule designed to support and conform to a policy
  - A standard should make a policy more meaningful and effective
  - A standard must include one or more accepted specifications for hardware software, or behavior
  - Standards may not exist for some parts of this section of the plan, so the *baseline* is included for all those parts
  - Standards / Baselines are usually written to describe the requirements for various technology configurations
  - As an example, most organizations have a policy about the use of wireless technology. That policy should have an accompanying wireless standard which discuss the accepted protocols, encryption key requirements, etc.

Business Continuity Plan

- Guideline
  - General statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures
  - A guideline can change frequently based on the environment and should be reviewed more frequently than standards / baselines and policies
  - A guideline is not mandatory, rather a suggestion of a best practice. Hence "guidelines" and "best practice" are interchangeable
  - Guidelines are not a required element of a policy framework, however they can play an important role in conveying best practice information to the user community. Guidelines are meant to guide users to adopt behaviors which increase security posture of a network

Business Continuity Plan

- Procedure
  - Detailed instructions on how to implement the policies, the standards / baselines and the guidelines
  - This part of the plan isn't usually disclosed to all organization staff, only to the ones that implement the instructions
  - Procedures define how the plan is implemented. They should contain contacts (if implemented by a third-part), and the actions to be performed not only to implement the plan but also to solve any unexpected result

Business Continuity Plan

- How they fit together