
Hervé Cholez / Sébastien Pineau
Centre de Recherche Public Henri Tudor
herve.cholez@tudor.lu  sebastien.pineau@tudor.lu
Objectives

- ISO/IEC 27005 is a standard that propose a way to manage information security risks, particularly in the context of the implementation of an ISMS* (ISO/IEC 27001)

- ISO/IEC 27005 is not a method, just a guide
  - For the moment... discussions in progress!

* ISMS: Information Security Management System
Risk = $f(\text{Threat} \times \text{Vulnerability} \times \text{Impact})$

- **Vulnerability**: intrinsic to the object or situation
- **Threat**: probability of occurrence of an (external) event exploiting the vulnerability
- **Impact**: consequence

Example: burglary in your house
- **Vulnerability**: your home keys under your carpet
- **Threat**: a burglar comes along...
- **Impact**: loss of your money, your TV, etc.
“potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization”
Information Security Risk? (2/3)

Asset

- “anything that has value to the organization”
- Primary: business processes and activities, information
- Support: hardware, software, network, personal, facilities

Threat

- “Potential cause of an unwanted incident, which may result in harm to a system or organization”
- Source of the risk, possible attack
- 3 kinds
  - Accidental (unintentional human action)
  - Deliberate (voluntary human action)
  - Environmental (non-human action)
Information Security Risk? (3/3)

- **Vulnerability**
  - “weakness of an asset (or control) that can be exploited by a threat”

- **Impact**
  - “adverse change to the level of business objectives achieved”
  - Consequence of the risk on the system or organization
  - Generally expressed in terms of:
    - Confidentiality
    - Integrity
    - Availability
Impacts?

Confidentiality

“property that information is not made available or disclosed to unauthorized individuals, entities or processes”
- internal disclosure, external disclosure...

Integrity

“property of protecting the accuracy and completeness of assets”
- accidental modification, deliberate modification, incorrect results, incomplete results

Availability

“property of being accessible and usable upon demand by an authorized entity”
- performance degradation, short-term/long-term interruption, total loss (destruction)
Information security risk management (ISRM)?

“*The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources*” [ISO/IEC 13335-1]

3 objectives

- Improve information system security
- Justify information system security budget
- Prove the credibility of the information system using the analysis performed
ISO/IEC 27005

Information technology – Security techniques – Information security risk management
Process

TAO – Workshop on CBA Security
Process
Context establishment

- Basic Criteria
- The scope and boundaries
- Organization for IRSM
Context establishment > Basic Criteria

- Risk evaluation criteria
- Impact criteria
- Risk acceptance criteria

- These criteria are specific to a given organization/system, to a given study, etc.
Context establishment > Basic Criteria > Risk evaluation criteria (1)

- Depends on
  - The strategic value of the business information process
  - The criticality of the information assets involved
  - Legal and regulatory requirements, and contractual obligations
  - Operational and business importance of CIA
  - Stakeholders expectations and perceptions, and negative consequences for goodwill and reputation

- Enables to prioritize risks
Examples

<table>
<thead>
<tr>
<th>Financial</th>
<th>Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Loss &lt; 1000€</td>
<td>Unimportant risk</td>
</tr>
<tr>
<td>1 1000€ &lt; Loss &lt; 5000€</td>
<td>Risk affecting the internal operation</td>
</tr>
<tr>
<td>2 5000€ &lt; Loss &lt; 10000€</td>
<td>Risk affecting customers</td>
</tr>
<tr>
<td>3 Loss &gt; 10000€</td>
<td>Risk</td>
</tr>
</tbody>
</table>

Goal:
- Clear differentiation between levels
- Unambiguous interpretation
Context establishment > Basic Criteria > Impact criteria (1)

- Cost per security incident, considering
  - Level of classification of the impacted information asset
  - Breaches of information security (e.g. Loss of CIA)
  - Loss of business and financial value
  - Disruption of plans and deadlines
  - Damage of reputation
  - Breaches of legal, regulatory or contractual requirements
Example

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Public</td>
<td>No constraint</td>
</tr>
<tr>
<td>1</td>
<td>Restricted</td>
<td>Change visible</td>
</tr>
<tr>
<td>2</td>
<td>Very restricted</td>
<td>Change reduced</td>
</tr>
<tr>
<td>3</td>
<td>Secret</td>
<td>Can not be altered</td>
</tr>
</tbody>
</table>

Goal:
- Clear differentiation between levels
- Unambiguous interpretation
## Context establishment > Basic Criteria > Likelihood of risk

### Threat

<table>
<thead>
<tr>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

### Vulnerability

<table>
<thead>
<tr>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
</tbody>
</table>
Context establishment > Basic Criteria > Risk acceptance criteria

Formula:

\[ \text{Risk level} = \max(\text{concerned impact}) \times (\text{threat} + \text{vulnerability} - 1) \]

<table>
<thead>
<tr>
<th>Max(I) * (T+V-1)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
</tbody>
</table>
Example

An unacceptable risk is:

- A very likely risk
  - Threat = 3
- With inadequate or inappropriate measures
  - Vulnerability = 1
- And whose asset value is 3
  - Impact = 3

\[ RL = 3 \times (3 + 1 - 1) = 9 \]
Context establishment > Basic Criteria > The scope and boundaries

Generally the first step (chronologically)

Definition of:
- Activity, processes to take into account
- Objectives
- Study borders (geographically, logically, ...)
- Legal constraints
- Etc.
Roles and responsibilities definition for the risk management process

Must be documented
Risk assessment

- Risk analysis
  - Risk identification
  - Risk estimation

- Risk evaluation
Risk assessment > Risk identification > Asset identification (1)

- Primary asset identification
  - business processes and activities, information

- Support assets identification (and mapping)
  - Hardware, software, networking, people, facilities
  - Knowledge bases available (e.g. EBIOS method)

- For each asset
  - Owner identification
  - Value determination
    - Qualitative, quantitative, semi quantitative
Risk assessment > Risk identification > Asset identification (2)

- For each asset, impact determination

- Based on impact criteria

“if criteria X of asset A is not fulfil, the impact would be...”

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Public</td>
<td>No constraint</td>
</tr>
<tr>
<td>1</td>
<td>Restricted</td>
<td>Change visible</td>
</tr>
<tr>
<td>2</td>
<td>Very restricted</td>
<td>Change reduced</td>
</tr>
<tr>
<td>3</td>
<td>Secret</td>
<td>Can not be altered</td>
</tr>
</tbody>
</table>
Risk assessment > Risk identification > Threat and vulnerabilities identification

- Knowledge bases
- Interviews, brainstorming
- Expert analysis

- Take into account controls already in place (vulnerabilities)
- For threats, take into account:
  - Deliberate
  - Accidental
Risk assessment > Risk estimation

- Risk = \( f(\text{Threat} \times \text{Vulnerability} \times \text{Impact}) \)

- Use of the formula
  
  \[
  \text{Risk level} = \max(\text{concerned impact}) \times (\text{threat} + \text{vulnerability} - 1)
  \]

- Value for each identified risk
Risk evaluation

» Comparison

» Obtained risk levels from risk assessment
» Defined risk acceptance levels

<table>
<thead>
<tr>
<th>Max(I) * (T+V-1)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
</tbody>
</table>
Risk treatment

4 choices
- Risk Reduction
- Risk Retention
- Risk Avoidance
- Risk Transfer

Can be combined

Results on a risk treatment plan
Risk treatment > Risk reduction

- Controls (measures) are implemented to reduce the risk

- It generally affects the vulnerability

- ISO/IEC 27002 proposes a set of controls

- Constraints for risk reduction exist
  - Time, financial, technical, etc...
Risk treatment > Risk retention

- Risk is accepted
  - Nothing is done to reduce it

- Generally when risk level is less than risk acceptance value

- But can be decided when risk is greater than risk acceptance value
  - Negative ROSI
  - Risk-taking
Risk treatment > Risk avoidance

- Risk is refused
  - “business” function cancelled

- Generally if the risk is too high and that no “cost-effective” solution is found
Risk treatment > Risk transfer

- Risk is transferred or shared with third party
  - Outsourcing
  - Insurance

- Generally for high impact risks with low occurrence

- Can create other risks or modify existing risks

- Transfer the responsibility to manage the risk but not the liability of an impact
Risk acceptance

- Risks effectively treated
  - Review of the risk treatment
  - Validation of selected solutions
  - Selection of residual risks

- Residual risks
  - Accepting a number of risks that can consider itself unable to deal, or are acceptable to the organization
Process

- Context Establishment
- Risk Assessment
  - Risk Analysis
    - Risk Identification
    - Risk Estimation
    - Risk Evaluation
  - Risk Decision Point 1
    - Assessment satisfactory
    - Risk Decision Point 2
      - Treatment satisfactory
- Risk Communication
- Risk Treatment
- Risk Acceptance
- End of first or subsequent iterations

TAO – Workshop on CBA Security
Continuous step

Obtain and communicate with all the stakeholders
- Collect information on risks and security
- Share risk assessment results
- Present risk treatment plan
- Awareness
- Etc.
Process

CONTEXT ESTABLISHMENT

RISK ASSESSMENT
- RISK ANALYSIS
- RISK IDENTIFICATION
- RISK ESTIMATION
- RISK EVALUATION

RISK DECISION POINT 1
- Assessment satisfactory

RISK TREATMENT
- Risk Decision Point 2
- Treatment satisfactory

RISK ACCEPTANCE

END OF FIRST OR SUBSEQUENT ITERATIONS
Risk monitoring and review

- Continuous step

- Risks are constantly changing, all risk equation elements must be tracked!
  - New assets
  - New threats
  - New vulnerabilities
  - Incidents
  - Etc.

- Minor changes vs. major changes
Thanks for your attention!

Any questions?

jocelyn.aubert@tudor.lu