Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Module

Information Security for Managers Unit (Module) 4, Week 7 and 8 Unit (Module) name: Cyber Risk and Resilience	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Simon Tjoa • Peter Kieseberg
Learning Activity Goals	1. The participants know foundations of risk and resilience management 2. The participants are able to perform business impact analysis and risk analysis 3. The participants can derive counter measures and security decisions from the results of analyses
Skills to be Gained	• IS 1, IS 3 • MS 1
Duration of Learning activity	2 weeks • Week 7 (2 hours) • Week 8 (2 hours)
Learning requirements	***What is needed?*** • Basic management skills • Basic IT skills • Basic security skills

Brief information about the module

Description
Perfect security is not possible. Knowing this, it is vital to make informed decisions how to spend money for right security measures. Cyber risk and resilience management provides a vital set of tools and techniques to assess the current state of security of an organization and to plan controls to keep the information security risk at an acceptable level.

Content of the Learning Material

Without taking risks, making business is impossible. Therefore, risk management and the corresponding tools & techniques provide a systematic way to address risk. Questions such as how much security is enough or which counter measure should be implemented first are answered by risk management. Thus, risk management is an important activity to enable informed decisions. Important standards and best practices addressing this essential topic include ISO 27005, ISO 31000 or BSI 200-3.

Before taking a closer look into the risk management process, it is essential to define essential terms:

- **Vulnerability:** "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."[1]
- **Control:** "A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements."[2]
- **Threat:** "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control

unauthorized access, destruction, disclosure, modification of information, and/or denial of service."[3]

- Risk: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."[4] "effect of uncertainty on objectives"[5]

From the definition of ISO 31000 ("effect of uncertainty"), we can derive that risks can have positive and negative impacts. Often if risks have positive impacts they are referred as opportunities.

The general risk management process starts with the scope, context and criteria. As not all risks for all activities can be analyzed it is important to prioritize and to decide which services, processes & organizational units should be included in the assessment. Having an adequate scope is crucial to ensure valid results on the one hand and reasonable effort on the other side. The context is the internal and external environment. The determination of risk criteria is important to ensure a and repeatable process, which leads to comparable results. The criteria should be defined in a way that different persons are able to assess risks in a common way.

Examples of criteria include impact criteria (e.g. low, medium, high) for various dimensions, such as financial, reputation or health.

In the following, an example of OCTAVE Allegro regarding reputation and customer impacts is presented:

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Figure 1: Measurement Criteria for Reputation[6]

[3] https://csrc.nist.gov/glossary/term/threat
[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf

After the definition of risk criteria and the scope, the first step is to identify risks. Risk identification is crucial as only those risk can be assessed, which are identified. It therefore makes sense to compare identified threats with threat lists of ISO 27005, MEHARI or other best practices or standards.

There exist various techniques[7] to identify risks, such as brainstorming, Delphi technique, Failure Mode and Effects Analysis (FMEA) or Hazard and Operability studies (HAZOP).

In the next step risk analysis, a better understanding of the identified risks is gained. Therefore, occurrence probability/frequency and impact/consequences are determined. In order to determine consequences, it is important to define a systematic way how impacts are assessed. Often a qualitative measure (e.g., low, medium, high) is easier to use than quantitative measures.

Risks are often visualized in a so called risk matrix, which highlights the risk using the probability and impact as axes.

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Figure 2: Risk Matrix [Source Wikipedia][8]

In the next step, the risks are evaluated. This means that the results of the previous step are considered to decide, whether actions should be taken. Furthermore, a prioritization of risks takes place.

Next one of the four main strategies to address risks are determined:

- Risk acceptance: document and monitor risk if the risk is within the risk appetite of the organization
- Risk transfer: share risks (e.g., insurance, joint venture)

[7] Cmp. https://www.iso.org/standard/72140.html
[8] https://en.wikipedia.org/wiki/Risk_matrix

- Risk avoidance: remove the risk source (e.g., air gap)
- Risk mitigation: reduce the impact or occurrence probability (e.g., access control)

After the determination of measures, it is evaluated whether the residual risk is acceptable or further measures have to be taken.

As supporting activities beside the main risk assessment process, risk communication (i.e. communication with relevant stakeholder), risk monitoring, and risk reporting takes place.

As not all risks can be considered, in contrast to risk management, business continuity & resilience focuses on critical activities instead of individual risks. This way it is possible to prepare for unknown and low-probability/high-impact risks.

For ensuring an effective business continuity program, the support of top management is vital. An important artefact highlighting the importance of business continuity management, is the business continuity policy. In this document the management buy-in is formally expressed. Further, the document highlights the scope and aims of the business continuity activities, important roles and responsibilities (e.g, business continuity manager) as well as the operational framework used for performing the program. It should be stressed that the scope should not be too broad to ensure that the complexity of the analysis as well as the effort are not getting too high.

In order to understand the effects of services disruptions on the business and to have a good basis for planning recovery measures, business impact analyses are carried out. It is the central tool within the business continuity process and captures the relevance/significance of products/services. Apart from the criticality of products / services their dependencies are determined and assessed.

Important key figures, which are used when performing a business impact analysis include:

- **MAO (maximum acceptable outage):** "time it would take for adverse impacts [...], which can arise as a result of not providing a product/service or performing an activity […], to become unacceptable"[9]
- **RTO (recovery time objective):** "period of time following an incident […] within which a product and service […] or an activity […] is resumed, or resources […] are recovered"[10]
- **RPO (recovery point objective):** "point to which information […] used by an activity […] is restored to enable the activity to operate on resumption"[11]

[9] MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[11] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

In the first step, the most critical or essential products and services are identified. After the identification, it is assessed which damage would arise over time if a certain product or services is disrupted or interrupted.

The succeeding figure shows how the impact over time could be captured in a spreadsheet.

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Furthermore, the business impact analysis surveys from which processes, activities and resources relevant services are dependent. This way important key figures, such as the recovery time objective, recovery point objective and the maximum acceptable outage can be determined.

After knowing the criticality of processes, services and resources, business continuity strategies are elaborated. Strategies include amongst others diversification (e.g., activities at geographically separated places), replication (e.g., copying data to recover at other site) or subcontracting (e.g., using third party services).

Based on the strategies business continuity plans are written, which support organizations to react in an efficient manner following an incident. In order to be usable in high pressure situations it is vital that plans are written accordingly. This means that plans should only contain that information which is relevant while handling an incident. Furthermore, the information should be quick to grasp. Thus, clear and action-oriented checklists should be used.

Typical business continuity plans contain information about the purpose, scope, incident management structure, roles and responsibilities, plan activation, recovery arrangements, and contact details.

In order to rehearse and check the adequacy of plans, different types of exercises are used. This can be either discussion-based exercises, such as desk checks or tabletop exercises or technical exercises, such as testing the restore of certain systems.

Questions:

See Word Documents

Attachments:

See Powerpoint and Video files

References:

- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22317:2021, Security and resilience — Business continuity management systems — Guidelines for business impact analysis
- ISO/TS 22331:2018, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy
- ISO/TS 22332:2021, Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures
- ISO 31000:2018, Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risk management — Risk assessment techniques