# Curriculum – English

Learning Units for knowledge, skills and competences for information security and data protection in SME

Funded by the Erasmus+ Programme of the European Union

TeBeISi

Funded by the
Erasmus+ Programme
of the European Union

This document is licensed under CC BY-SA 4.0.

This document was produced within the scope of the ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi”, Project ID: 2018-1-EN02-KA202-005218

The European Commission support for the production of this publication does not constitute endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

# Content

1 TeBeISI – The project at a glance ........ 1
1.1 Project Partner: ........ 2
2 Preparatory steps which led to the TeBeISi Curriculum ........ 3
2.1 Step 1 (IO1) – Identification of Competence Profiles ........ 3
2.2 Fase 2 (IO3) - The Online Questionnaire ........ 3
3 The TeBeISi Curriculum ........ 5
4 The Job-Profile of the “IS-DP Practitioner for SMEs” ........ 6
5 The “making of” the Learning Units (LU) ........ 7
5.1 Chart with Learning Units (based on ECVET) ........ 7
5.2 Learning Units – overview and short description ........ 9
6 Detailed description of Learning Units (based on ECVET) ........ 10
6.1 LU1 – Process Management ........ 10
6.2 LU2 – ICT Risk Management ........ 12
6.3 LU3 – Compliance Management ........ 14
6.4 LU4 – ICT Procurement ........ 17
6.5 LU5 – Sensitisation and Influencing ........ 19
6.6 LU6 – Education and Training ........ 21
6.7 LU7 – Security Testing ........ 23
6.8 LU8 – Encoding ........ 25
6.9 LU9 – Data Management ........ 27
6.10 LU10 – Role Based Access Control ........ 29
6.11 LU11 – Password Management ........ 31
6.12 LU12 – Business Continuity Management ........ 33
6.13 LU13 – Mediation and Stakeholder Management ........ 35

Funded by the
Erasmus+ Programme
of the European Union

# 1 TeBeISI – The project at a glance

The IT sector is generally characterized by short innovation and product cycles among developers and manufacturers. Due to the constantly changing requirements in the IT sector, learning and recognition of informal aspects is becoming a decisive factor in the area of information security as well. The lack of certification opportunities results in a lack of experts in the field of information security (worldwide). This problem has been known for years and poses serious challenges for the economy. Therefore, the „Betriebswirtschaftliches For-schungszentrum für Fragen der mittelständischen Wirtschaft e. V.“ (BF/M-Bayreuth) started the European joint project TeBeISi - "Partial Certification in the Occupational Field of Information Security" to identify and evaluate competencies in the field of information security. The Europe-wide uniform assessment and recognition of informally acquired qualifications has enormous potential in terms of combating the shortage of skilled workers in the field of information security.

The project helps to promote the recognition and certification of qualifications and competences, including those acquired through non-formal and informal learning. Through European exchange between the institutions, the certifications of occupational profiles that are specifically prevalent in the countries are to be processed and incorporated into newly developed occupational profiles in the exchange of experience. The project aims to transfer these profiles including certification procedures to the European partner countries and to implement them successfully in practice. The focus is on the validation of learning outcomes from non-formal and informal learning.

A large number of instruments were needed to work on the project. In order to determine the required information security competencies, extensive literature research, expert interviews and focus groups with companies were conducted. These findings served as a basis for the creation of a catalogue of requirements. For a Europe-wide establishment, the development of recommendations for action was required. This was done, among other things, by involving associations and associated partners from the economy. The next step was the development of an online personnel questionnaire to determine information security competencies with the focus on social competences.

The next important project step, which we present in this paper, is the development of further education modules for training of specific sub-competencies, taking social and technical components into account: The TeBeISi Curriculum

The main product in the final project phase, is a strategy paper based on the new data protection regulation, a glossary for application and the research report "Status Quo Information Security Training for SMEs".

## 1.1 Project Partner:

- BFM - Betriebswirtschaftliches Forschungszentrum Mittelstand (Germany): www.bfm-bayreuth.de
- Hafelekar Unternehmensberatung – (Austria): http://www.hafelekar.at
- Consulenza Direzionale Paolo Zaramella (Italy): https://www.linkedin.com/in/paolozaramella
- MRU - MYKOLAROMERIS UNIVERSITY (Lithuania): www.mruni.eu
- WSBINOZ (Poland): www.medyk.edu.pl

# 2 Preparatory steps which led to the TeBelSi Curriculum

## 2.1 Step 1 (IO1) – Identification of Competence Profiles

All five participating organizations have set themselves the goal of finding out what concrete requirements SME's do have in the fields of Information Security and Data Protection. The findings on required information security and data protection competencies started in each partner country with a Desk Research, which was supplemented by a Field Research by each partner: Partner organizations invited experts for interviews and organized focus groups to find out more about the real (local) needs in SME's. The outcomes of these activities served as the basis for the “Report on Identification of Competence Profiles”, which aimed to further identify competences needed, both in the field of Information Security and Data Protection.

The graphic shown below is the result of what the invited experts had to say: Words and phrases appearing in the graphic are the most frequently given answers to the question about the skills and competences necessary for their work. The larger the font, the more often the answer was named:

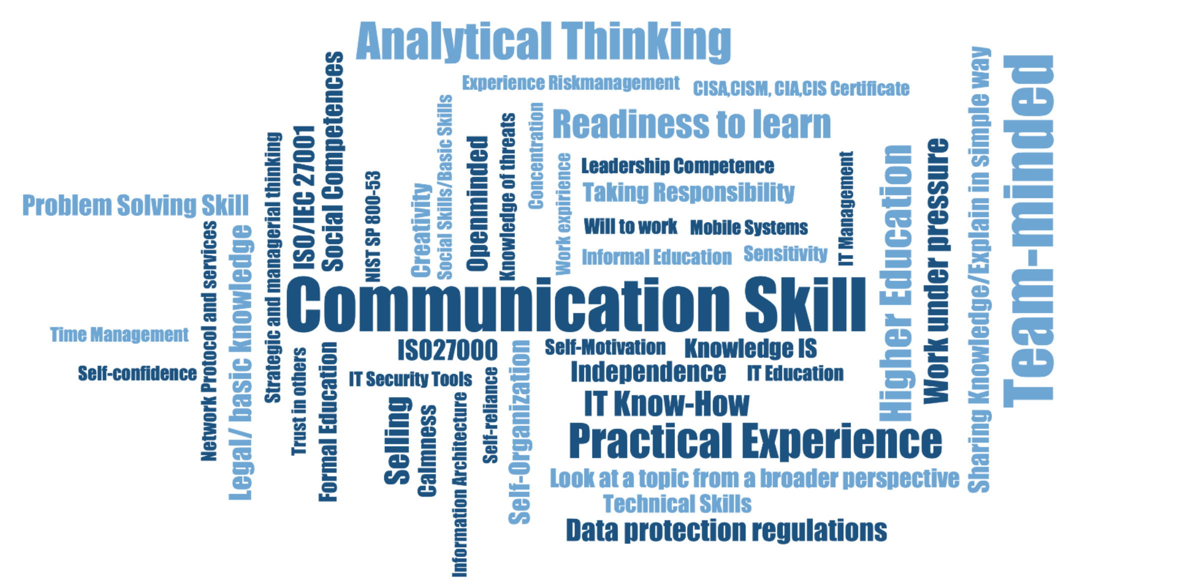


*Figure 1: Simon Rath, BFM: Coding Cloud - created from data of desk and field research*

## 2.2 Fase 2 (IO3) - The Online Questionnaire

The preliminary results gathered through desk- and field research were further specified and built the base for a first draft of Learning Units. In order to review and expand the partnership's needs analysis (as a result of IO1), an online questionnaire was designed, in order to 1) verify the project result 2) improve an understanding of what competences SMEs are looking for 3) establish references of competence levels for sub-competences in each unit (which can be used for self-assessment) and 4) establish an overview of what strategies (if at all) are being deployed by SMEs to overcome the shortage in labour supply.

The online questionnaire, therefore, is composed of two parts: the questionnaire itself, directed at firm owners, employees working in HR and IT as well as general employees in SMEs. Depending on their function within the firm, the questionnaire adapts so that each group receives a suitable set of questions, making sure that, e.g., questions corresponding to the information security curriculum for SME, are only being answered by experts. The second part represents the self-evaluation tool: The tool allows firms to check what kind of competences they need (depending on their used technology as well as the amount of and importance of certain tasks being conducted), and to specifically self-evaluate the corresponding units. This way, it can be assured that only important competences are being evaluated, which supports the intent of the project team to keep the self-evaluation as short and easy to handle as possible.

The exact content of the questionnaire is composed of items aiming at evaluating the market demand in conjunction with items stemming from the developed questionnaire. The latter decomposes the sub-competences of each of the 13 Units and asks participants for self-evaluation (both the need of the firm and the own proficiency). The complete data set which is collected will be used to produce the report “Status Quo – Information Security in SMEs”.

The procedure of working on these tools is as follows: first, the grand questionnaire has been disseminated among firms and authorities from the partner countries to collect the needed data. Second, the data has been fed into the self-evaluation tool, which is to be provided to all firms interested. The importance of providing an easy-to-use tool merits the fact that overcoming skills shortages, firms need to invest time and resources. The simpler the tool is to be used, the higher the expected acceptance will be.

# 3 The TeBelSi Curriculum

The training aims to provide SMEs with resources to match their specific labour demand. Deriving from the idea of partial certification, the offering of a curriculum which allows to train a very specific set of competences, learners are enabled to carry out a set of specific tasks. Reconsidering the economic advantages of partial certification, an individual does not need to take an entire course (e.g., run through 3 years of education), even though a majority of needed competences for the qualification is already there. The reality is quite the opposite, and individuals refrain from taking the burden of the course to validate their competences. Ceteris paribus, firms are more likely to invest in the training of competences they specifically need, as the qualification process from their point of view is more time effective and cost efficient.

## 3.1 For whom is this further training designed?

In consequence, the general target group is two-fold: 1) firms who are looking to fill very specific demand 2) individuals who are interested in acquiring competences in the field of information security and data protection with a strong focus on action-oriented capabilities. Meanwhile the first group is composed of SMEs across all sectors within the EU, the latter is composed of a variety of learners, be it university students who want to achieve extra qualifications, learners in VET programs who are in need of acquiring new competences which can be incorporated into the existing curriculum, or employees on the free labor market which aim to improve their employability.

All of these groups, however, face similar requirements to be able to participate in the course:

- Do the participants need a formal educational qualification?
    - No, the curriculum is open for everyone, students and workers. However, some sort of experience will be required (e.g. work experience, some fundamental experience with and understanding of ICT).
- Do the participants need previous knowledge in the field of IS & Data Protection?
    - No. They need to be able to read and understand documents which deal with IS or DP issues. A certain affiliation to ICT is helpful.

## 3.2 In what form should this further training be offered?

The specific design of the course depends upon the target group of the educational institutions. The curriculum is supposed to provide the contents for the course, the final development of course materials is left to the institutions. In general, two options appear most natural: Online learning and blended learning. However, the preparation of learning material is not the scope of the TeBelSi project, which would heavily affect how the training could be done. The duration of the training cannot be estimated in general. Training providers are free to decide how much time they want to allocate to the individual learning units.

# 4 The Job-Profile of the "IS-DP Practitioner for SMEs"

The "Information Security and Data Protection Practitioner for SMEs", in the following referred to as "IS-DP Practitioner", fulfills a complementary role to the Management and/or IT department and is charged with the aim to protect the firm – in close cooperation with the management - from any damage as a direct consequence of data protection infringements or loss of information due to breaches in the security system. The corresponding competences shall allow specifically SMEs the access to personnel which is sufficiently skilled with regards to their specific needs, depending on how they work, which technology they use and what sort of data they process. Specifically, an SME shall be facilitated to re-skill an employee from within the firm in order to fill positions within the Information Security and Data Protection realm and to build up own technical capabilities.

Information security and data protection, in comparison to large corporations, poses very different requirements to SMEs: Communication channels are less elaborate, the sort and amount of data can be processed under GDPR conforming standardized processes and the business model generally is much less reliant on technological processes. Thus, the skillset required by an employee charged with data protection and information security duties changes significantly when working in an SME, despite the principal objectives of the work remaining the same as in large corporations.

In this context, the suggested competence set of an IS-DP Practitioner enables the employee to carry out tasks which fulfill the requirements of Information Security in SMEs. Nonetheless, a wide range of competences needs to be acquired. These involve both functional as well as interpersonal aspects. Especially the ladder is important in order to create awareness for IS and DP matters among the firm and to thereby mitigate the majority of threats, highlighting the need to find personnel with relative strong social and self-competence in order to fill in this position.

The suggested profile of competences allows SMEs to cover their specific need of information security, depending on their processes, their technologies, and their working environment. The employee in charge with information security and data protection is not meant to implement a certification-ready information security management system, nor deeply analyzing and implementing new complex technological solutions to the firm. The main responsibility is to ensure that information security and data protection is lived and accepted by employees, that fundamental insurances to protect the firm against any sort of damage are being hold in place and security aspects being included in the strategic development of the firm. The IS-DP Practitioner is supposed to relieve the management by assuming a liaising function between the management and the employees.

# 5 The “making of” the Learning Units (LU)

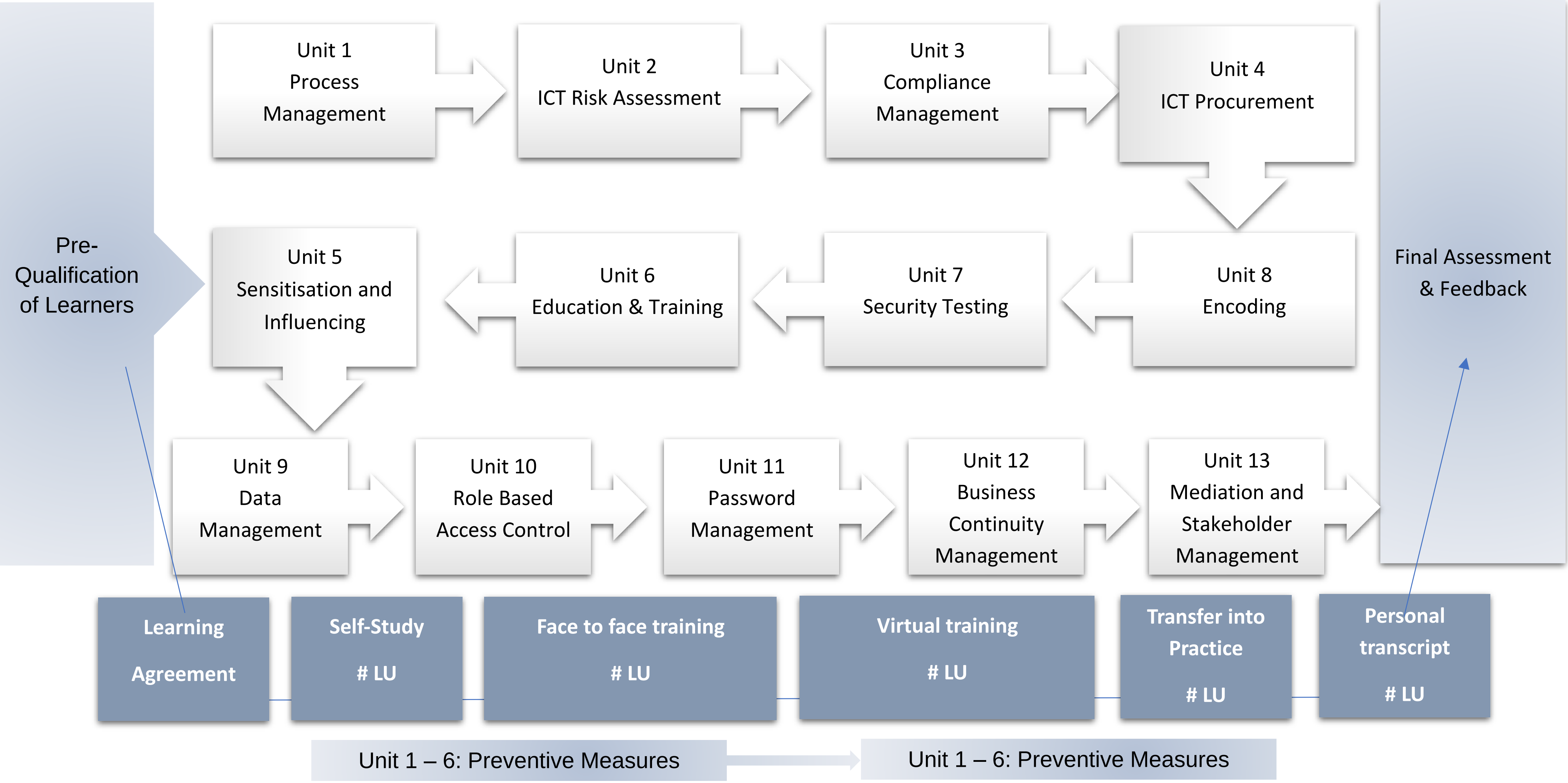
We have described the process that led to the definition of explicit learning content as well as learning outcomes. In doing so, we explored the following questions: What is required by information security professionals in SMEs? Which competences are absolutely necessary? Which are more important in large corporations? Throughout a series of expert interviews, the project group identified 13 fields which encapsule different competence domains of an information security officer. Based on these fields, learning units can be generated which allow learners to acquire all relevant competences to implement foundational security measures in SMEs.

Building upon the competences mentioned by the experts it becomes quite clear that social competences represent a very central aspects of successful information security professionals. Meanwhile a wide range of technical competences is necessary to master, both in the field of legal aspects and in the domain of ICT, social and self-competencies are seen as a prerequisite for employers. Meanwhile the former can be taught, specific attitudes and motivational aspects which come along the work in a firm with other employees are valuable assets which prove to be mandatory in case of critical situations.

## 5.1 Chart with Learning Units (based on ECVET)

Built upon this finding, following a procedural approach, tasks could be clustered into learning units, covering the whole range of information security responsibilities, and underlying them with core specific competences. These units can be used for educational purposes, be it existing employees in the firm which are seeking to assume new responsibilities, students in university who seek to improve their employability or other groups of learners looking for requalification. Further, professionals without formal qualification, e. g. from vocational or higher education providers, can use these units as benchmarks for their own proficiency.

# TeBelSi Curriculum (based on ECVET criteria)



Pre-Qualification of Learners

Unit 1
Process Management

Unit 2
ICT Risk Assessment

Unit 3
Compliance Management

Unit 4
ICT Procurement

Unit 8
Encoding

Unit 7
Security Testing

Unit 6
Education & Training

Unit 5
Sensitisation and Influencing

Unit 9
Data Management

Unit 10
Role Based Access Control

Unit 11
Password Management

Unit 12
Business Continuity Management

Unit 13
Mediation and Stakeholder Management

Final Assessment & Feedback

**Learning Agreement**

**Self-Study**
**# LU**

**Face to face training**
**# LU**

**Virtual training**
**# LU**

**Transfer into Practice**
**# LU**

**Personal transcript**
**# LU**

Unit 1 – 6: Preventive Measures

Unit 1 – 6: Preventive Measures

## 5.2 Learning Units – overview and short description

| # | Learning Unit | Short Description |
|---|---|---|
| LU1 | **Process Management** | Analyse business processes and produce a strategic report concerning data protection and information security. |
| LU2 | **ICT Risk Assessment** | Track changes in and outside the firm which have an impact on the firm's security strategy and produce reports for employees. |
| LU3 | **Compliance Management** | Write company guidelines on how to deal with specific information and data. |
| LU4 | **ICT Procurement** | Produce recommendations regarding items to be procured considering information security and data protection requirements of the firm. |
| LU5 | **Sensitisation and Influencing** | Conduct (informational) activities to sensitise employees for security risks in their working routine and to spread awareness among the workforces. |
| LU6 | **Education and Training** | Create training plans for the company in order to be able to regularly train the employees with regard to information security and data protection. |
| LU7 | **Security Testing** | Install a firewall and anti-virus software. Perform updates and apply basic methods to test the security of software used in the firm and produce a corresponding documentation. |
| LU8 | **Encoding** | Work on securitisation of mobile devices, communication channels and data storage units via passwords or other means of authentication. |
| LU9 | **Data Management** | Conduct routinised back-ups of data and apply methods of proper conduct under GDPR to the data processing in the firm. |
| LU10 | **Role Based Access Control** | Establish administrator accounts and restrict access-rights among employees according to defined security levels. |
| LU11 | **Password Management** | Establish passwords for individual access among employees and allow for a safe storage and recovery process. |
| LU12 | **Business Continuity Management** | Establish guidelines and procedures for the emergence of possible contingencies. |
| LU13 | **Mediation & Stakeholder Management** | Coordinate the needs of the firm’s executives and employees, providing both parties with information and insights from within the firm. |

# 6 Detailed description of Learning Units (based on ECVET)

## 6.1 LU1 – Process Management

| Learning Unit 1 | Process Management |
|---|---|
| **General Description / Output** | **Analyse business processes and produce a strategic report concerning data protection and information security.** |
| Code number | LU 1 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of a structured process analysis in a firm. They are capable to recognise processes which evoke the necessity of further analysis considering their data and information security exposure. Participants are being familiar with process documentation and are capable to monitor changes in the working routine. They are capable to prepare documentation which allows for the formulation of recommendations for action. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- how to apply GDPR guidelines and good information security practices.<br>- how to identify, document, design, implement, governance and optimise business processes.<br>- how to strategically plan the process documentation.<br>- about communication techniques and channels.<br>**Can**<br>- implement documentation by using EDP systems.<br>- summarise the original information without losing the original message.<br>- effectively communicate with colleagues to adjust workflows.<br>- react appropriately to the statements of others, e.g., accept constructive criticism, and listen actively to find the best solutions.<br>- find relevant legal and technical information and corresponding recommendations for action from trustful sources.<br>**Personal Competence**<br>**The participants are able to**<br>- independently organise the documentation process, working in a structured way with a focus on details. |

| | |
|---|---|
| | - self-reliantly communicate with colleagues and be confident in the interactions.<br>- recognise the responsibility belonging to the task and be confident in the interaction with others. |
| **Recommendations for Learning & Teaching** | Process documentation with the help of real-world examples.<br>Exercises on documentation in the EDP system in free form and with the help of text modules. |
| **Literature & Further Resources** | Nguyen, B. T., Lee, G. M., Sun, K., & Guo, Y. (2019). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security,* 15, 1-13.<br>EU-GDPR. (2019). *EU GDPR portal*. [Online]. Available: https://eugdpr.org.<br>General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:32016R0679.<br>Gellert, R. (2015). Understanding data protection as risk regulation. *Journal of Internet Law*, 18 (11), 3-15. |
| | |

## 6.2 LU2 – ICT Risk Management

| Learning Unit 2 | ICT Risk Management |
|---|---|
| **General Description / Output** | **Track changes in and outside the firm which have an impact on the firm's security strategy and produce reports for employees.** |
| Code number | LU 2 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand dynamics of technological change and their influence on the firm’s strategy to mitigate risks. They are capable to decide upon the urgency of reacting to these risks. Participants will be able to track technological developments within and outside the firm and to provide assessments on the firm’s risk exposure. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- about assessment of risk exposure of the firm and adequacy of current measures to meet the associated risks.<br>- how to monitor technological developments within and outside the firm as well as changes to staff.<br>- how to determine the volume and purpose of personal data processed.<br>**Can**<br>- find information about technological developments by consulting relevant news sources and information from public or private authorities from the field.<br>- detect risks despite theoretical reluctance of employees to reveal mistakes or weaknesses.<br>- provide recommendations for actions based on the information gained.<br>- assess and mitigate risks related to data protection.<br>- identify personal data storages/process operations within organizations and evaluate their context.<br>- take actions on objectives set at a strategy level in order to mobilise resources and employees to strengthen cooperation.<br>**Personal Competence**<br>**The participants are able to**<br>- show resilience when facing non-willingness of colleagues to cooperate.<br>- stay flexible in order to find solutions and to create a supportive environment. |

| | |
|---|---|
| | - execute tasks strategically and in an organised manner.<br>- |
| **Recommendations for Learning & Teaching** | Process documentation with the help of real-world examples.<br>Exercises on documentation in the EDP system in free form and with the help of text modules. |
| **Literature & Further Resources** | European Banking Authority (2019). Final Report: EBA Guidelines on ICT and security risk management [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020.<br>NZ Digital Government (2021). ICT Risk Management Guidance [Online]. Available: www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html.<br>Commission de Surveillance du Secteur Financier (CSSF) (2020). ICT Risk [Online]. Available: www.cssf.lu/en/ict-risk/.<br>Rothman, T. (2020). Valuations of Early-Stage Companies and Disruptive Technologies: How to Value Life Science, Cybersecurity and ICT Start-ups, and their Technologies. Berlin: Springer. |
| | |

## 6.3 LU3 – Compliance Management

| Learning Unit 3 | Compliance Management |
|---|---|
| **General Description / Output** | **Write company guidelines on how to deal with specific information and data.** |
| Code number | LU 3 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of codifying company behavioural guidelines in order to establish proper conduct with data and information. They learn how to set guidelines which establish compliance among employees. They understand the importance of preparing for foreseen and unforeseen contingencies and setting out companywide rules how to behave and measured to be taken in critical situations. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- about the GDPR field of regulations and national legal documents, regulating information security and data protection.<br>- about information architecture and internal communication channels of the organization<br>- how to analyse, map and document processes that might cause a potential conflict with compliance policies.<br>- how to prepare compliance policy guidelines.<br>- how to collect, manage and assess data processing techniques.<br>- how to think analytically in processing of condensing information, developing solutions, and making decisions related to compliance management.<br>**Can**<br>- implement the procedures described in legal documents.<br>- identify critical data and information units that require special protection or treatment.<br>- analyse and map the processes related to the flow of information in the organization.<br>- recognize potential risks and threats to information security and data protection in the internal processes of organization.<br>- develop compliance management related solutions to practical, operational, or conceptual problems in a wide range of daily working routines.<br>- understand the purpose of compliance policy guidelines and update them in emergency situations.<br>- apply analytical and critical thinking skills in identifying the strengths and weaknesses of potential solutions to compliance management related problems. |

| | |
|---|---|
| | - summarize the information in convenient and meaningful way.<br>**Personal Competence**<br>**The participants are able to**<br>- work in a structured way with a focus on details.<br>- recognise the responsibilities belonging to the tasks and be confident in the interaction with others.<br>- handle tasks independently and demonstrate willingness to learn.<br>- |
| **Recommendations for Learning & Teaching** | Process documentation with the help of real-world examples.<br>Exercises on documentation in the EDP system in free form and with the help of text modules. |
| **Literature & Further Resources** | Agostinelli S., Maggi F.M., Marrella A., & Sapio F. (2019) Achieving GDPR Compliance of BPMN Process Models. In: Cappiello C., Ruiz M. (eds) Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, 350, 10–22. Springer, Cham. https://doi.org/10.1007/978-3-030-21297-1_2<br>Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In Proceedings Financial Cryptography and Data Security, 18 [Online]. Available: https://pure.itu.dk/ws/files/84212312/On_Purpose_and_ny_Necessity.pdf<br>Besik, S. I., & Freytag, J. C. (2020). Managing Consent in Workflows under GDPR. In J. Manner, S. Haarmann, S. Kolb, O. Kopp (Eds.): 12th ZEUS Workshop, ZEUS 2020, Potsdam,Germany, 20-21 February 2020, (pp. 18-25).<br>Blanco-Lainé, G., Sottet, J. S., & Dupuy-Chessa, S. (2019, November). Using an enterprise architecture model for GDPR compliance principles. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 199-214). Springer, Cham.<br>EU-GDPR. (2019). EU GDPR portal. [Online]. Available: https://eugdpr.org.<br>Kammüller, F., Ogunyanwo, O.O., & Probst, C.W. (2019). Designing data protection for GDPR compliance into IoT healthcare systems. Computer Science. arXiv:1901.02426.<br>Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. In 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering |

| | |
|---|---|
| | Languages and Systems (MODELS), Munich, Germany, 2019, (pp. 1-11). doi: 10.1109/MODELS.2019.00-20.<br>Wichmann, J., Sandkuhl, K., Shilov, N., Smirnov, A., Timm, F., & Wißotzki, M. (2020). Enterprise Architecture Frameworks as Support for Implementation of Regulations: Approach and Experiences from GDPR. Complex Systems Informatics and Modeling Quarterly, (24), 31-48. |
| | |

## 6.4 LU4 – ICT Procurement

| Learning Unit 4 | ICT Procurement |
|---|---|
| **Description Generale / Output** | Produrre raccomandazioni riguardo agli articoli da acquistare considerando i requisiti di sicurezza delle informazioni e di protezione dei dati dell'azienda. |
| Number di codice | LU 4 |
| Tipo | Obbligatorio – da definire |
| Volume | Ore – da definire |
| **Competenze da acquisire** | I partecipanti imparano a capire l'importanza del sistema di approvvigionamento per sostenere l'implementazione della sicurezza delle informazioni e della protezione dei dati. Imparano come mettere le proprie competenze a disposizione del processo di approvvigionamento dell'azienda. I partecipanti sono in grado di esercitare un'influenza sull'acquisto di nuove tecnologie e macchinari e di valutare l'adeguatezza e l'utilizzo in termini di protezione dei dati e linee guida di sicurezza delle informazioni dell'azienda. |
| **Risultati di apprendimento** | **Competenze Tecniche**<br>**I partecipanti**<br>**Imparano**<br>- sui requisiti di sicurezza e sulle specifiche dell'azienda per quanto riguarda le nuove attrezzature.<br>- sulle specifiche dell'hardware esistente e l'urgenza di al-terle con la nuova tecnologia.<br>- sull'inganno dei fornitori di servizi e delle attrezzature per le violazioni del GDPR.<br>**Possono**<br>- .<br>comunicare efficacemente con gli altri.<br>- preparare e presentare una breve presentazione (relazione/procedura/processo/strategia) dedicata alla valutazione della tecnologia o dei macchinari che devono essere acquistati.<br>- trasferire informazioni da diversi impiegati/reparti sulle loro necessità e poi dare la raccomandazione sull'acquisto.<br>- raccogliere informazioni complete sulla tecnologia/macchinari acquistati.<br>- trovare informazioni legali e tecniche rilevanti e prendere decisioni basate su questa indagine.<br>- intraprendere azioni sugli obiettivi e le procedure definite a livello strategico per mobilitare le risorse e perseguire le strategie stabilite.<br>- pianificare e gestire le risorse sotto vincoli di budget e di tempo e raggiungere gli obiettivi stabiliti facendo uso del monitoraggio dell'avanzamento del progetto e dei controlli di qualità |

| | |
|---|---|
| | **Competenze Personali**<br>**I partecipanto sono in grado di**<br>- conoscere le soluzioni di mercato esistenti per il problema dell'azienda.<br>- dedicarsi ai dettagli (legali e tecnici).<br>- mostrare fiducia e responsabilità nella comunicazione con le parti interessate. |
| **Raccomandazioni per formazione ed addestramento** | . Documentazione dei processi con l'aiuto di esempi reali.<br>Esercizi sulla documentazione nel sistema EDP in forma libera e con l'aiuto di moduli di testo. |
| **Letteratura & altre fonti** | Australian Government: Digital Transformation Agency (2021). ICT procurement [Online]. Available: www.dta.gov.au/help-and-advice/ict-procurement.<br>Moses, M. (2019). Procurement Process and ICT. Zerite Network [Online]. Available: http://zeritenetwork.com/procurement-process-and-ict/.<br>European Commission (2016). Best practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in: 2-year project completed [Online]. Available: ec.europa.eu/digital-single-market/en/news/.<br>Dovgalenko, S. (2020). The Technology Procurement Handbook: A Practical Guide to Digital Buying. London: Kogan Page. |
| | |

## 6.5 LU5 – Sensitisation and Influencing

| Learning Unit 5 | Sensitisation and Influencing |
|---|---|
| **General Description / Output** | **Conduct (informational) activities to sensitise employees for security risks in their working routine and to spread awareness among the workforces.** |
| Code number | LU 5 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participant learns to understand the importance of sensitizing employees and members of the board regarding data protection and information security concerns. They will learn to raise awareness for common threats and build capacities among the workforce to detect likely threats in their daily working routine. Participants will be capable of conducting analysis about the level of awareness in the firm and to implement corresponding awareness rising measures. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- about basic guidelines of the GDPR.<br>- how to handle with potential processes and personnel vulnerable to attacks or loss of sensitive information and data.<br>- how auditing measures can be implemented.<br>- about communication techniques and channels.<br>- how to implement change strategies.<br>**Can**<br>- find the relevant source of legal knowledge.<br>- cooperate with others in the broadest sense of the term in order to identify the need for change, inspire and instruct and assist in its implementation.<br>- communicate effectively with others by choosing not only the type of message but also its scope and importance to the circumstances.<br>**Personal Competence**<br>**The participants are able to**<br>- adapt to changing conditions and circumstances by working in an organised manner and keeping a distance which allow for proper self-assessment. |

| | |
|---|---|
| | - being an example for other employees following their ethical code of conduct and show responsibility. |
| **Recommendations for Learning & Teaching** | Combine theoretical knowledge and approach with practical examples like gut-check measures and how to stage incidences, e.g.:<br>- Fake USBs<br>- Instances of Human Engineering<br>- Sending fake e Mails<br>Apply interactive teaching methods (ex. group-work, discussions, case analysis, simulation role-playing, etc.) |
| **Literature & Further Resources** | IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.).<br>Clarke, N., Furnell, S. (2020). Human Aspects of Information Security & Assurance (14th ed.). Plymouth: Centre for Security, Communication & Network Research.<br>i-scoop (o.J.). GDPR awareness: a matter of people, culture, leadership and acting now [Online]. Available: https://www.i-scoop.eu/gdpr/gdpr-awareness/.<br>Kefron - The Information Management People (o.J.). Why Maximizing Staff Awareness Is The Key To A Smooth GDPR Transition [Online]. Available: https://www.kefron.com/blog/why-maximizing-staff-awareness-is-the-key-to-a-smooth-gdpr-transition/.<br>European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: www.enisa.europa.eu<br>General Data Protection Regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/ |
| | |

## 6.6 LU6 – Education and Training

| Learning Unit 6 | Education and Training |
|---|---|
| **General Description / Output** | **Create training plans for the company in order to be able to regularly train the employees with regard to information security and data protection.** |
| Code number | LU 6 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of education with regards to data protection and information security requirements. They learn to educate both themselves and employees of the firm. Participants will be capable to consult reliable sources and to derive training needs upon consultation or interaction with employees. Participants learn to prepare training material and train employees to incorporate adequate working routines in their daily work. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- where to find national legal documents regulating information security and data protection (basics of the GDPR).<br>- how to prepare training material and how to provide training to incorporate adequate working routines.<br>- how to mentor individual employees.<br>**Can**<br>- introduce to employees how to practically apply national legal documents in the field of information security and data protection following the guidelines of GDPR.<br>- convince employees of the importance of continuous training in both areas by active awareness raising.<br>- mentor and support individual employees regarding identified training needs.<br>- develop solutions to practical, operational, or conceptual problems which arise in the execution of work in a wide range of contexts.<br>**Personal Competence**<br>**The participants are able to**<br>- independently organise training sessions within the company in a structured way with a focus on current needs. |

| | |
|---|---|
| | - self-reliantly communicate with colleagues and the management by being confident in the interactions.<br>- recognise the responsibility belonging to the task and motivate employees to learn. |
| **Recommendations for Learning & Teaching** | Documenting information security and data protection difficulties encountered in daily business to plan and implement appropriate training measures. |
| **Literature & Further Resources** | Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company.<br>Da Veiga, A., Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, (49), 162–176. doi: 10.1016/j.cose.2014.12.006.<br>Peacock, M., Steward, E. B., & Belcourt, M. (2019). Understanding Human Resources Management. Nelson: Nelson College Indigenous.<br>Ryan, L. (2010). Corporate Education: A Practical Guide to Effective Corporate Learning. Salisbury: Griffin Press.<br>Osborne, B. (2020). 10 Benefits of Security Awareness Training [Online]. Available: https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/.<br>GDPR informer (2017). Data Protection Training: 10 Tips for Your Staff [Online]. Available: https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff. |
| | |

## 6.7 LU7 – Security Testing

| Learning Unit 7 | Security Testing |
|---|---|
| **General Description / Output** | **Install a firewall and anti-virus software. Perform updates and apply basic methods to test the security of software used in the firm and produce a corresponding documentation.** |
| Code number | LU 7 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of testing existing ICT infrastructure for their vulnerability in the face of technological developments. They learn to use (or understand with an external support) penetration testing tools to ensure the security of firewalls and communication channels.<br>There is an infinite number of ways to break an application. And, security testing, by itself, is not the only (or the best) measure of how secure an application is. But it is highly recommended that security testing is included as part of the standard software development process. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- about Network security: This involves looking for vulnerabilities in the network infrastructure (resources and policies).<br>- about System software security: This involves assessing weaknesses in the various software (operating system, database system, and other software) the application depends on.<br>- about Client-side application security: This deals with ensuring that the client (browser or any such tool) cannot be manipulated.<br>- about Server-side application security: This involves making sure that the server code and its technologies are robust enough to fend off any intrusion.<br>**Can**<br>- build tests to determine the security of the software product.<br>- adapt the existing framework.<br>- access computer system or network with authorization.<br>- ensure the systems to avoid steal or destroy data.<br>- perform most of the breaking activities with permission from the owner.<br>**Personal Competence**<br>**The participants are able to** |

| | |
|---|---|
| | - recognise the documentation of processes as a starting point for further working steps.<br>- work in a structured way with a focus on details.<br>- recognise the responsibility belonging to the task and be confident in the interaction with others. |
| **Recommendations for Learning & Teaching** | Most types of security testing involve complex steps and out-of-the-box thinking but sometimes, it is about simple tests that help expose the most severe security risks. |
| **Literature & Further Resources** | Dekkers, C., McCurley, J., & Zubrow, D. (2013). Measures and Measurement for Secure Software Development. Pittsburgh: Carnegie Mellon University.<br>Dowd, M., McDonald, J., & Schuh, J. (2007). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Boston: Addison-Wesley. |
| | |

## 6.8 LU8 – Encoding

| Learning Unit 8 | Encoding |
|---|---|
| **General Description / Output** | **Work on securitisation of mobile devices, communication channels and data storage units via passwords or other means of authentication.** |
| Code number | LU 8 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of password encoding for their vulnerability in the face of technological developments. They learn to use (or understand with an external support) password encoding tools to ensure the security of firewalls and communication channels.<br>Password Encoding is the process in which a password is converted from a literal text format into a humanly unreadable sequence of characters. If done correctly, it is very difficult to revert back to the original password and so it helps secure user credentials and prevent unauthorized access to a website. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- about Literal Values: Passwords were stored in literal text format in databases without any encoding or hashing. As databases need authentication, which nobody except the admins and the application had, this was considered safe.<br>- about Encryption: It is a safer alternative and the first step taken towards password security.<br>- about Hashing: To combat these attacks, developers had to come up with a way to protect passwords in a database in such a way that they cannot be decrypted.<br>- about Salting: To combat the appearance of rainbow tables, developers started adding a random sequence of characters to the beginnings of the hashed passwords.<br>- about Password Encoders: It provides multiple password encoding implementations to choose from. Each have their advantages and disadvantages, and a developer can choose which one to use depending on the authentication requirement of their application.<br>**Can**<br>- educate the team on password encoding best practice.<br>- educate the team on cyber security.<br>- decide what password types not to use. |

| | |
|---|---|
| | - define the right way to generate encoding processes.<br>- eliminate complex passwords.<br>- strongly reduce the risk of copying a password.<br>- ensure password auditing and accountability.<br>**Personal Competence**<br>**The participants are able to**<br>- recognize the documentation of processes as a starting point for further working steps.<br>- work in a structured way with a focus on details.<br>- recognize the responsibility belonging to the task and be confident in the interaction with others.<br>- manage the main requested tasks with a good level of autonomy.<br>- emphasise their social competences (soft skills, empathy and communication in particular). |
| **Recommendations for Learning & Teaching** | Most types of encoding processes involve complex steps and out-of-the-box thinking but, sometimes, it is simple tests like the one above that help expose the most severe encoding risks. |
| **Literature & Further Resources** | Kaliski, B. (2000). Password-Based Cryptography Specification Version 2.0. RFC Editor, US. https://doi.org/10.17487/RFC2898.<br>Mourouzis, T., Pavlou, K. E., & Kampakis, S. (2018). The Evolution of User-Selected Passwords: A Quantitative Analysis of Publicly Available Datasets. Computer Science. arXiv:1804.03946.<br>Barbero, G., Trasselli, F. (2015). Manus OnLine and the Text Encoding Initiative Schema. Journal of the Text Encoding Initiative, (8), 1-16. doi: 10.4000/jtei.1054. |
| | |

## 6.9 LU9 – Data Management

| Learning Unit 9 | Data Management |
|---|---|
| **General Description / Output** | **Conduct routinised back-ups of data and apply methods of proper conduct under GDPR to the data processing in the firm.** |
| Code number | LU 9 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of storing and processing data and information according to agreed guidelines. They learn about proper conduct with Data under consideration of the GDPR. Participants will be capable to evaluate the storage and processing of physical and electronic data in the firm and to identify potential misconduct. Participants learn to suggest alteration in the firms processes in order to mitigate these risks. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- how to define the information needs required for the successful process: what kind of data are being processed within the organization and what storage techniques should comply with the respective regulations.<br>- rules, how to determine the volume and purpose of personal data storage and processing operations.<br>- how to organize and apply data management in the company: adapt to the change; apply analytical thinking; develop solutions; perform project management tasks independently.<br>- different techniques and communication styles in order to obtain necessary information about storage.<br>**Can**<br>- determine the volume and purpose of personal data that are being stored/processed within the organization.<br>- create regular backups in order to minimise the risk of losing valuable data and information.<br>- work within the group to efficiently extract information to improve processes.<br>- plan and manage various resources and monitor the data management process in order to achieve a specific goal.<br>**Personal Competence**<br>**The participants are able to** |

| | |
|---|---|
| | - work in a structured way with a focus on details.<br>- recognise the responsibility belonging to the task and be confident in the interaction with others.<br>- handle tasks independently and demonstrate willingness to learn. |
| **Recommendations for Learning & Teaching** | Combine theoretical knowledge and approach with practical examples. Apply interactive teaching methods (ex. group-work, discussions, case analysis, simulation role-playing, etc.) |
| **Literature & Further Resources** | Calabro, A., Daoudagh, S., & Marchetti, E. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems (91) [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306437919305216.<br>Guide on Good Data Protection Practice in Research (2019) [Online]. Available: https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf.<br>EU-GDPR. (2019). EU GDPR portal. [Online]. Available: https://eugdpr.org.<br>General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. |
| | |

## 6.10 LU10 – Role Based Access Control

| Learning Unit 10 | Role Based Access Control |
|---|---|
| **General Description / Output** | **Establish administrator accounts and restrict access-rights among employees according to defined security levels.** |
| Code number | LU 10 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of limiting accessibility to data, information, or physical infrastructure when possible, and to grant access only to a group of relevant employees. They learn how to establish appropriate restrictions according to a defined security level. Participants will be capable to assign roles within the firm to clearance levels and to make access to specific information traceable if necessary. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- how to identify the key operations with personal data that are being performed within an organization.<br>- how to establish the accessibility of information to specific groups of employees.<br>- how to establish appropriate restrictions according to the defined and agreed security levels when deemed necessary.<br>**Can**<br>- distinguish the roles of individual employees and groups in order to define their needs for various security levels (based on assigned security levels agreed with the management).<br>- find appropriate solutions for individual employees or groups in terms of access or restrictions and is able to justify them.<br>- manage individual user rights, which becomes a matter of simply assigning appropriate roles to the user's account, when roles are clearly defined (by the management).<br>**Personal Competence**<br>**The participants are able to**<br>- independently assign appropriate roles according to the specifications of the management (assigned security levels).<br>- self-reliantly communicate with colleagues and the management by being confident in the interactions. |

| | |
|---|---|
| | - autonomously recognise the responsibility belonging to the task and respect the needs of others. |
| **Recommendations for Learning & Teaching** | Learn/Teach about the three primary rules defined for RBAC: 1) Role assignment, 2) Role authorization, 3) Permission authorization. Think of the importance of sensitisation in role attribution and make clear agreements with the management. |
| **Literature & Further Resources** | Blokdyk, G., (2017). Role-based Access Control: A Successful Design Process.<br>D Ferraiolo, DR Kuhn, R Chandramouli, (2003), Role-based access control.<br>Benantar, M., (2006)., Access Control Systems: Security, Identity Management and Trust Models. New York: Springer.<br>Zhang, E. (2020). What is Role-Based Access Control (RBAC)? Examples, Benefits, and More [Online]. Available: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more. |
| | |

## 6.11 LU11 – Password Management

| Learning Unit 11 | Password Management |
|---|---|
| **General Description / Output** | **Establish passwords for individual access among employees and allow for a safe storage and recovery process.** |
| Code number | LU 11 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of centralising the management of password utilisation within the firm. They will learn how to define passwords which ensure authentication (among employees) and how to reset passwords. Participants learn how to structurally create, use/manage, store and change passwords of employees. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- about Password storage.<br>- about Password transmission.<br>- about Password guessing.<br>- about Password cracking.<br>- about Password replacing.<br>**Can**<br>- educate the team on password best practice.<br>- educate the team on cyber security.<br>- decide what password types not to use.<br>- generate complex passwords.<br>- harness the power of automation.<br>- eliminate complex passwords.<br>- eliminate the need for password resets.<br>- ensure password auditing and accountability.<br>**Personal Competence**<br>**The participants are able to**<br>- recognise the documentation of processes as a starting point for further working steps.<br>- work in a structured way with a focus on details.<br>- recognise the responsibility belonging to the task and be confident in the interaction with others.<br>- manage the main requested tasks with a good level of autonomy.<br>- emphasise their social competences (soft skills, empathy, and communication in particular). |

| | |
|---|---|
| **Recommendations for Learning & Teaching** | Password management with the help of real-world examples.<br>Exercises on documentation in free form and with the help of text modules. |
| **Literature & Further Resources** | Luca, M. (2008). Password Management for Distributed Environments. Saarbrücken: VDM Verlag Dr. Müller.<br>Smith, S. B. (2017). Password Manager: Keep Record of Internet User ID and Passwords in the Password Manage. Keep your internet login info in a safe offline location. CreateSpace: North Charleston. |
| | |

## 6.12 LU12 – Business Continuity Management

| Learning Unit 12 | Business Continuity Management |
|---|---|
| **General Description / Output** | **Establish guidelines and procedures for the emergence of possible contingencies.** |
| Code number | LU 12 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of conducting "what if" scenarios. They learn to analyse theoretical contingencies and to prepare strategic guidelines accordingly. The participants will be capable of establishing guidelines and to predefine measures in order to be prepared and to respond coordinated to new situations when they arise. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- how to find national documents and how to search for knowledge in national legal documents regulating security and data protection.<br>- simulation techniques to envision potential data breaches.<br>- how to deal with rules for risk assessment.<br>**Can**<br>- identify risks using different techniques and communication styles.<br>- implement rules of risk assessment acting with the approval of the management.<br>- plan and develop solutions adapting to circumstances and changes at organizational scale and implement them acting with the approval of the management.<br>- find new solutions based on analysis of previous events.<br>**Personal Competence**<br>**The participants are able to**<br>- work in unfavourable circumstances while being attached to the details.<br>- easily adapt to new circumstances.<br>- being an example for other employees following their ethical code of conduct and show responsibility.<br>- |
| | |

| | |
|---|---|
| **Recommendations for Learning & Teaching** | Theoretical practice of scenarios of different threats and risk situations. Working with examples from real situations. |
| **Literature & Further Resources** | Irwin, L. (2019). Why risk assessments are essential for GDPR compliance [Online]. Available: https://www.itgovernance.co.uk/blog/why-risk-assessments-are-essential-for-gdpr-compliance.<br>European Data Protection Board (2021). Guidelines 01/2021 on Examples regarding Data Breach Notification [Online]. Available: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.<br>European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Available: www.enisa.europa.eu.<br>Green, A. (2020). GDPR Data Breach Guidelines - COMPLIANCE & REGULATION [Online]. Available: https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule/.<br>General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/. |
| | |

### 6.13 LU13 – Mediation and Stakeholder Management

| Learning Unit 13 | Mediation and Stakeholder Management |
|---|---|
| **General Description / Output** | **Coordinate the needs of the firms' executives and employees, providing both parties with information and insights from within the firm.** |
| Code number | LU 13 |
| Type | Mandatory – to be defined |
| Volume | Hours - to be defined |
| **Action Competences** | The participants learn to understand the importance of coordinating with all stakeholders in the firm regarding their role and their impact on data protection and information security. The learn how to effectively communicate with different hierarchy levels (employees and management) and to align their needs and interests when changes to organisational routines occur. Participants will be capable of interacting with stakeholders in a diplomatic way and to deal with possible resistance towards the own influence. |
| **Learning Outcomes** | **Technical Competence**<br>The participants<br>**Know**<br>- how to find national legal documents, regulating information security and data protection and how to search for knowledge.<br>- which internal and external communication channels may apply acting with management approval and what risks are associated with them.<br>- which measures may be applied to observe, test and evaluate processes in the organization.<br>- which measures may be applied to assess risks and how to deal with risk assessment.<br>**Can**<br>- implement internal auditing measures (with management approval).<br>- plan and develop strategic solutions and then implement them acting with approval of management.<br>- install a preventive culture with support of management.<br>- identify, assess, and prioritise risks.<br>- create internal regulations at organizational scale and implement them (with management approval).<br>**Personal Competence**<br>**The participants are able to** |

| | |
|---|---|
| | - deal with change and adaptation.<br>- being creative and seeking to further development.<br>- rely on their own ethical code so that others can follow their example.<br>- |
| **Recommendations for Learning & Teaching** | Combine theoretical knowledge and approach with practical examples. Apply interactive teaching methods (e.g.: group-work, discussions, case analysis, simulation role-playing, etc.) |
| **Literature & Further Resources** | IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.).<br>General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/.<br>Gorondutse, A. H., & Hilman, H. (2016). Mediation effect of organizational culture on the relationship between perceived ethics and SMEs. Journal of Industrial Engineering and Management 2016, 9(2), 505-529.<br>Straight, J. (2018). GDPR compliance: Identifying an organization's unique profile [Online]. Available: https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/ |
| | |