
# Curriculum

## English Version 2.0

Lifelong Learning Programme

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## 0. Introduction

This curriculum shall serve teachers in the field of Information Security Management as a handbook on how to organise a course on Information Security Management designed for owners / managers and employees of small and medium sized enterprises (SME)[1]. It is designed and meant to give ideas and serve as a good practice example. The organisation of an individual course nevertheless will require adaptation and modification of the provided structure and concept in regard of individual needs. If participants require a more individual attendance or if some of the listed units are of more interest to the learners than others, the teacher is always free to set priorities according to target group needs.

This curriculum consists of five main building blocs:

1. the **course description** (chapter 1) providing an overview of the central learning objectives of the workshop;
2. the **macro planning** of the workshop (chapter 2) including details of the 3 training levels to be achieved, learning objectives of each level, as well as suggestions on how to split the learning content between online and face-to-face sessions;
3. the **description of assumed target group pre-requisites** per training level and the conditions regarding the learning environment (chapter 3);
4. the **description and reasoning of methods** to be applied throughout the training (chapter 4);
5. a suggestion and example for the organisation of the **blended-learning approach** (chapter 5).

## 1. Course description

The aim of this course is to support owners or managers of small and medium enterprises in the planning and implementation of an adequate information security concept. Throughout the course this target group shall gain a basic understanding and knowledge of information security, its requirements and juridical framework, strategic and organisational approaches and practical measures. In order to meet different company's pre-requisites and needs the course is divided in 3 Levels:
Level 1: Generic
Level 2: Intermediate
Level 3: Advanced

After completing Level 1 participants will have a general understanding of what Information Security Management is and why it is important for companies.
Level 2 will provide participants with an overview of some measures to be taken.
Participants completing Level 3 will be in a position to take over the role of the Information Security Officer for their company.

[1] According to EU definition



Lifelong Learning Programme

The main characteristics of the profile of an Information Security Officer can be summarized as follows:

- ability to prevent as much and as well as possible
- determination and efficacy in taking decisions
- two way communication (top down and bottom up)
- ability to delegate and involve staff
- ability to identify and listen to weak signals
- ability to make a “team”
- participated involvement in business issues, as a flexible, innovative function that is continually better integrated to support the business
- adoption of a “facilitator” role and not that of an obstacle
- strong attention to anomalies that are brought to his/her attention
- rigour and objectivity in measuring results
- primary role in security training and communication programmes

**The Information Security Officer** should be able to:

1. understand basic concepts of IS and its importance for an SME;
2. communicate the "value of security" in the company by improving the perception and knowledge of safety with specific internal "marketing and communication" activities;
3. ensure that the centrality of the human component is maintained in security processes, encouraging structured training plans for different professional families to work in safety;
4. analyse in detail the general "as is" business situation to obtain an overview of the entire defined organizational structure and technological architecture in place;
5. know what ICT the company has and the different types of possible attacks;
6. identify potential risks and the most appropriate countermeasures to mitigate effects, taking into account the constraints and opportunities imposed by law;
7. prepare the organization to address and manage emergency situations and possible subsequent crises;
8. manage a business continuity plan to recover and continue business activities after an attack.



Lifelong Learning Programme

## 2. Macro Planning

In order to contextualise the learning process the workshop is divided into three main areas of practice: PLANing, RUNning and MANAGEing the information security management concept. The areas of practice follow, in their overall content structure, the pedagogical concept of a so-called "complete action" which is considered to be a circle consisting of the steps: informing, planning, deciding, doing, controlling and evaluating.

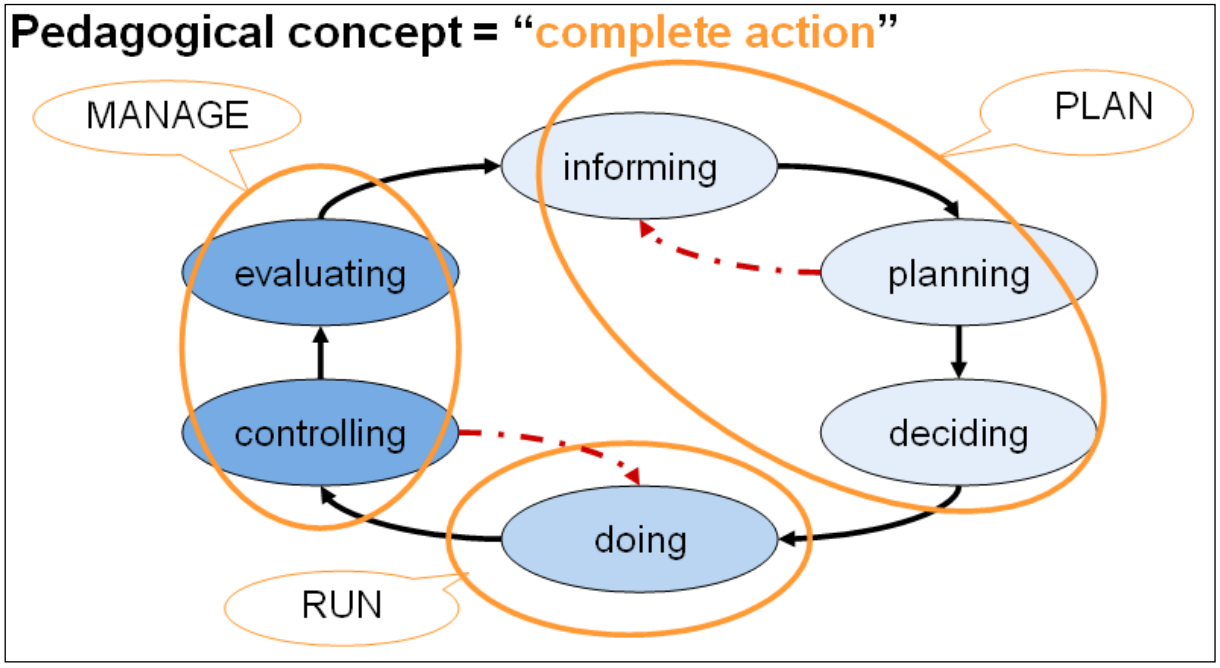


Image 1: Areas of Action and Complete Action

### 2.1. Areas of Practice

- *Plan* – Planning / Decision – Analysis of the IS requirements and design of the IS concept (informing, planning, deciding)
- *Run* – Operative sub-processes – providing, obtaining and maintaining the necessary measures, processes, infrastructure, Know-how (running / doing)
- *Manage* – optimize controlling, monitoring, and business processes – testing, evaluating, adapting, optimizing measures, development of contingency plans (controlling, evaluating)

### 2.2. Training levels

The workshop is divided into 3 training levels: generic, intermediate and advanced, which are taught online and face-two-face (F2F). The allocated amount of learning units per level and the distribution of online and face to face units are to be understood as a suggestion.



Lifelong Learning Programme

Level 1: Generic
*Target Audience*: The generic level addresses owners / managers and employees of SMEs.

*Objective / Learning Outcome*: The main objective is to raise awareness of Information Security Management and to provide practical knowledge and skills on how to respect Information Security in daily routines. The generic level covers parts of PLAN and RUN and consists of 15 learning units.

Level 2: Intermediate
*Target Audience*: The intermediate level addresses owners and managers of SMEs who are responsible for the organisation of Information Security Management and are in charge of decision making.

*Objective / Learning Outcome*: Within the intermediate level pre-knowledge in the field of Information Security and ICT is not required. It is the objective of the intermediate level to train participants to be able to plan and organise IS in close co-operation with external IS experts. The intermediate level provides a deeper understanding of PLAN and RUN and consists of 15 learning units.

Level 3: Advanced:
*Target Audience*: The advanced level addresses owners / managers of SME who have some pre-knowledge in ICT and in basic Information Security correspondent to Level 1 and 2.

*Objective / Learning Outcome*: It is the objective of the advanced level to train participants to be able to organise and implement IS measures themselves, at least to a great extent. The advanced level provides a deeper understanding of MANAGE and consists of 10 units.

The following image summarises and visualises the structure of training levels and distribution of online and F2F units.

| Field of Action / Level | Generic | | Intermediate | | Advanced | | |
|---|---|---|---|---|---|---|---|
| Units | online | F2F | online | F2F | online | F2F | |
| PLAN | 6 | 4 | 6 | 4 | | | |
| RUN | 3 | 2 | 3 | 2 | | | |
| MANAGE | | | | | 6 | 4 | |
| Total | 9 | 6 | 9 | 6 | 6 | 4 | |
| | | **15** | | **15** | | **10** | **40** |

Image 2: Structure of Training Levels



Lifelong Learning Programme

### 2.3. Systematic structure of each area of action

The macro planning is described in the following table providing the following information:

- allocated training level,
- area of practice and allocated number of units,
- name of the different learning units,
- duration of each part, where 1 unit equals 45 minutes,
- competencies achieved throughout the given units,
- suggestions on learning content suitable to promote the named competencies
- suggestions on which learning content could be taught online and which face-to-face

Level 1: Generic

**Plan (10 Units)**

| **Field of Action**<br>**Learning Unit** | **Competencies** | **Learning Content**<br>**F2F** | **Learning Content**<br>**Online** |
|---|---|---|---|
| Informing –<br><br>Understanding the necessity of IS<br><br>2 Units | The participants understand the necessity to implement IS in their company.<br><br>They are aware of potential risks coming along with neglecting IS.<br><br>The participants are aware of legal demands and requirements as well as possible sanctions.<br><br>They have an overview of relevant rules and regulations on **national** level. | • Potential risks<br>• Possible consequences of neglecting IS<br>• Relevant rules and regulations, standards as well as related sanctions<br>• Techniques and methods to stay up-dated (e. g. newsletter, RSS feeds) | INSEMOT Module 1 – Front Office |
| Informing –<br><br>Assessing and evaluating IS needs of own company<br>Risk Analysis<br><br>1 Unit | The participants know relevant ICT interfaces of information assets. | • Risk analysis<br>• Identifying EDP interfaces of relevant business processes | |

| | | | |
|---|---|---|---|
| Planning –<br><br>Defining strategic IS objectives<br><br>1 Unit | The participants are able to define strategic objectives of IS implementation.<br><br>The participants are able to define criteria for measure results.<br><br>Participants are able to prioritise objectives. | Exercise on SMART IS objectives<br>• How to phrase SMART objectives<br>• ABC-prioritisation of objectives<br>• Phrasing objectives under consideration of IS Basics | INSEMOT Module 3 – Back Office |
| Planning –<br><br>IS measure catalogue<br>- on system level<br><br>2 Units | The participants are aware of workplace related IS measures and are able to implement them. | Hands on practical IS measures<br>• How to create a secure password<br>• How to configure the screen safer | INSEMOT Module 1 – Front Office<br>INSEMOT Module 4 – IT-Room |
| Planning –<br><br>IS measure catalogue<br>- on technological level<br><br>2 Units | The participants garner an overview of important IS measures on network and Internet level. | • Secure use of web browser<br>• Secure Internet use<br>Secure e-mails | INSEMOT Module 4 – IT-Room |
| Planning –<br><br>IS measure catalogue<br>- on human level<br><br>2 Units | The participants understand the importance of the factor “human” in the IS context. | • Defining requirements e. g. regarding work place | INSEMOT Module 1 – Front Office<br>INSEMOT Module 2 – Back Office |
| End of Module / Module exam | The participants draft an IS measure catalogue including | | |

| | | | |
|---|---|---|---|
| | implementation planning and methods and reason their decision in regard of companies information assets, requirements to ensure maintenance of business activities and cost-effect-ratio. | | |

**Run (5 Units)**

| **Field of Action**<br>**Learning Unit** | **Competencies** | **Learning Content**<br>**F2F** | **Learning Content**<br>**Online** |
|---|---|---|---|
| Doing –<br><br>Clarifying preconditions for implementation<br><br>1 Unit | The participants have an overview of up-to-date security technology such as authentication and cryptography techniques. | • Current IS technology and its functions | INSEMOT Module 1 – Front Office<br>INSEMOT Module 4 – IT Room |
| Doing –<br><br>Designing emergency measures and Back-up concept<br><br>1 Unit | The participants are aware of measures to be taken in case of data loss, system fallout or else in order to reactivate business activities in due time. | • Reason and intended purpose of emergency concepts<br>• Requirements towards emergency measures<br>• Requirements towards data back-up | INSEMOT Module 3 – IS Office<br>INSEMOT Module 4 – IT Room |
| Doing –<br><br>Support and Maintenance<br><br>1 Unit | | • Support interval<br>• Up-dates | INSEMOT Module 4 – IT Room |
| Doing –<br><br>Implementing controlling measures<br><br>1 Unit | The participants have a general overview of controlling measures. They are able to differentiate between these measures. | • Choosing measures and assessing pros and cons | INSEMOT Module 3 – IS Office |

| | | | |
|---|---|---|---|
| Doing –<br><br>Implementing tests<br><br>1 Unit | The participants are aware of tests suitable to evaluate the effectiveness of IS measures. | • How to react on changing security requirements | |
| End of Module / Module Exam | Drafting a criteria catalogue on implementing IS in own company<br>Identifying and describing especial sensitive assets | | |

Level 2: Intermediate

**PLAN (10 Units)**

| **Field of Action**<br>**Learning Unit** | **Competencies** | **Learning Content**<br>**F2F** | **Learning Content**<br>**Online** |
|---|---|---|---|
| Informing –<br><br>Understanding the necessity of IS<br><br>1 Unit | The participants have an overview of relevant rules and regulations on **international** level. | | INSEMOT Module 1 – Front Office<br>INSEMOT Module 3 – IS Office |
| Informing –<br><br>Assessing and evaluating IS needs of own company<br>Risk Analysis<br><br>2 Units | The participants are able to identify information assets and pivotal business processes and to assess and evaluate them in regard of their relevance in maintaining business activities and competitiveness.<br><br>The participants are able to estimate and number the extent of a potential loss or damage. | Risk analysis<br>• ABC-prioritisation of business processes and information assets<br>• Ascertaining time remaining to act after ICT fallout or data loss<br>• Naming and estimating potential loss | INSEMOT Module 2 – Back Office |
| Planning –<br><br>IS measure catalogue<br>- on system level | The participants know security measures integrated on system level and are able to adjust and configure them. | Hands on practical IS measures<br>• How to configure the operating system | INSEMOT Module 4 – IT Room |

| | | | |
|---|---|---|---|
| 2 Units | The participants have an overview of ICT solutions suitable to supplement system based security measures.<br><br>The participants understand the principle of user roles. | • Malware detection<br>• User roles and their rights and obligations<br>• ICT solutions for IS | |
| Planning –<br><br>IS measure catalogue<br>- on technological level<br><br>2 Units | The participants understand the principles of network security. | • Firewall | INSEMOT Module 4 – IT Room |
| Planning –<br><br>IS measure catalogue<br>- on human level<br><br>1 Unit | Participants are aware of measures suitable to supplement technical IS solutions such as internal communication, good examples, rewarding. | • Defining rules and regulations along with sanctions and how to communicate them<br>• Measures to raise awareness and motivate employees on IS<br>• Understanding the need to train employees | INSEMOT Module 2 – Back Office |
| Deciding –<br><br>Determining cost-effect-ratio<br><br>2 Units | The participants are able to determine the cost-effect-ratio of single IS measures and are able to decide on measures to be implemented. | • Calculating costs of single IS measures<br>• Estimating the effect of single IS measures<br>• Estimating the potential financial risk of damages to or loss of information assets and comparing it to | INSEMOT Module 2 – Back Office |

| | | | |
|---|---|---|---|
| | | costs of IS measures | |
| End of Module / Module exam | The participants draft an IS measure catalogue including implementation planning and methods and reason their decision in regard of companies information assets, requirements to ensure maintenance of business activities and cost-effect-ratio. | | |

**RUN (5 Units)**

| **Field of Action**<br>**Learning Unit** | **Competencies** | **Learning Content**<br>**F2F** | **Learning Content**<br>**Online** |
|---|---|---|---|
| Doing –<br><br>Clarifying preconditions for implementation<br><br>1 Unit | The participants are able to activate different reporting systems. | • Working principles and function of operating systems. | INSEMOT Module 4 – IT Room |
| Doing –<br><br>Designing emergency measures and Back-up concept<br><br>2 Unit | The participants are able to decide on suitable measures for their company. | • Business continuity plan | INSEMOT Module 3 – IS Office |

| | | | |
|---|---|---|---|
| Doing –<br><br>Support and Maintenance<br><br>1 Unit | The participants understand requirements towards effective and efficient IS Management support and maintenance.<br><br>The participants are able to develop a suitable management concept and to implement it. | • Support interval<br>• Up-dates | INSEMOT Module 3 – IS Room<br>INSEMOT Module 4 – IT Room |
| Doing –<br><br>Implementing controlling measures | The participants are able to define criteria to control the operation of IS measures. | • Defining controlling intervals<br>• Defining controlling criteria | INSEMOT Module 3 – IS Office |
| Doing –<br><br>Cooperation with experts<br><br>1 Unit | The participants are able to define to what extend and for what task cooperation with external experts is necessary.<br><br>The participants are able to phrase a call to buy in external expertise and to compare different tenders. | | |
| End of Module / Module Exam | Drafting a criteria catalogue on implementing IS in own company<br>Identifying and describing especial sensitive assets | | |

Level 3: Advanced

**Manage (10 U)**

| **Field of Action Field of Action** | **Competencies** | **Learning Content F2F** | **Learning Content Online** |
|---|---|---|---|
| Controlling –<br><br>Documentation of IS measures<br><br>1 Unit | The participants understand the necessity of IS measurement documentations.<br><br>The participants know and understand requirements towards this documentation. | • Use and purpose of the documentation<br>• Requirements towards documentation<br>• Intervals for actualisation | INSEMOT Module 3 – IS Office |
| Controlling –<br><br>Recognising employees training needs<br><br>2 Units | The participants understand and know why and when training needs are likely to occur.<br><br>They are able to define requirements towards a suitable training together with their employees.<br>The participants know where to find information and or consultation on qualification. | • Methods to assess current training needs<br>• Information sources and consultation on ISM qualification | INSEMOT Module 2 – Back Office<br>INSEMOT Module 3 – IS Office |
| Controlling –<br><br>updating juridical basics of IS<br><br>1 Unit | The participants know sources to garner information on juridical updates.<br><br>The participants are able to | Information sources and juridical basics regarding ISM | |



Lifelong Learning Programme

| | | | |
|---|---|---|---|
| | evaluate implemented IS measures in regard of juridical changes and to adjust them accordingly. | | |
| Evaluating –<br><br>Evaluating and adjusting strategic ISM concept<br><br>2 Units | The participants are able to adjust the strategic ISM concept in regard of changing business processes, technological frame conditions or juridical requirements | • Principles of strategic ISM<br>• Intervals for evaluating and adjusting IS strategies<br>• PDCA Method | INSEMOT Module 3 – IS Office |
| Evaluating –<br><br>Future orientation<br><br>2 Units | The participants are able to assess and evaluate the potential impact of technological evolution and other innovations on business processes and organisation.<br><br>The participants are able to draft change management on mid-term horizons. | • Current trends, e. g. mobile working, cloud computing<br>• Problems which might occur while implementing trends<br>• How to decide which trends to follow | |
| Evaluating –<br><br>Audits / QM<br><br>2 Units | The participants are able to assess the effectiveness of IS steering tools.<br><br>The participants understand use and purpose of audits and are able to estimate the information value of a certificate. | • Use and purpose of audits<br>• Informative value of certificates<br>• Requirements towards audits<br>• Juridical basics | |

| | | | |
|---|---|---|---|
| | The participants know criteria to pay attention to while commissioning an audit. | | |
| End of Module / Module Exam | Reflection of ISMS and emergency concept and measures to update / optimise IS strategy and operation | | |

# 3. Prerequisites and Conditions

## 3.1. Participants prerequisites

The description of the assumed prerequisites of the participants is described as follows taking into account any characteristics of the target group which might influence – either positively or negatively – the learning process. Each trainer, using this curriculum, is kindly advised to adjust target group specifications if necessary.

**Generic Level:**

- owner / executives / co-working partners
- employees
- no previous IS knowledge
- basic ICT skills / basic knowledge of how to use ICT
- men and women
- heterogeneous age structure - the younger, the more likely advanced ICT skills can be assumed
- various educational levels / apprenticeship training / skilled worker / academic degree / Master of Crafts diploma etc.
- participants are usually fulltime employed / working

**Intermediate Level:**

- owner / executives / co-working partners
- basic ICT skills / basic knowledge how to use ICT
- men and women
- heterogeneous age structure - the younger, the more likely advanced ICT skills can be assumed
- various educational levels / apprenticeship training / skilled worker / academic degree / Master of Crafts diploma etc.
- participants are usually fulltime employed / working
- learning outcomes of Generic Level are pre-requisites

**Advanced Level**

- owner / executives / co-working partners
- basic to intermediate IS pre-knowledge
- Intermediate to advanced ICT skills / intermediate to advanced knowledge of how to use and manage ICT, Network management etc.
- men and women
- heterogeneous age structure - the younger, the more likely advanced ICT skills can be assumed
- various educational levels / apprenticeship training / skilled worker / academic degree / Master of Crafts diploma etc.
- participants are usually fulltime employed / working
- learning outcomes of Intermediate Level are pre-requisites



Lifelong Learning Programme

### 3.2. Frame Conditions

The learning environment is described in regard of any condition which might influence – either positively or negatively – the learning-process respectively of what is needed to support either face-to-face or online learning. The following aspects are meant as examples and require adjustment to given conditions.

- Minimum number of participants = 7-10
- requirements towards the classroom teaching phase (training centre facilities):
  - regular seminar setting (e. g. beamer, laptop, internet connection, flip chart, metaplan material);
  - room for group work
- requirements towards the online teaching phase (participants):
  - PC or Laptop with flat rate Internet connection, actual browser,
- requirements toward the online teaching phase (teacher):
  - tutor
  - help desk
- heterogeneous structure enterprises ICT structures = individual requirements of IS concept



Lifelong Learning Programme

# 4. Methodology to be used

The methods to be employed within the workshop shall support students in building and expanding the following basic skills:

- ability to analyse the current situation in the organisation
- ability to recognize needs and possibilities for optimisation
- ability to identify training and consulting needs
- being able to define requirements regarding IS
- controlling and monitoring implemented solutions / processes and being able to recognize needs to act
- documenting processes

The following examples of methods can be employed in the classroom in accordance with the provision of appropriate methodological skills and as to support the described learning objectives:

- Meta Plan
- Mind Mapping
- Cause and Effect Diagram (also Ishikawa diagram)
- 4-field method
- PDCA Method according to ISO
- role based interaction (role playing)
- “virtual” company with lacks in IS Management
- etc.

## 4.1. Preparation for self-dependent learning

As not every learner is already familiar with online-based training settings respectively self-dependent learning, it might be necessary to support learners. The following measures might serve as suggestions on this matter:

- organization of lessons along the stages of a “complete action” (inform, plan, decide, execute, monitor, evaluate)
- setting thematic priorities in consultation with the study group
- provide learning strategies supporting and fostering reflection and analysis of past learning behaviour
- provide methods by which learning needs (own and of others, such as employees) can be detected
- Sufficient time schedule for the treatment of individual topics / modules
- Variety of methods and forms of social interaction (e. g. individual learning, teamwork, creativity techniques, structural and organizational methods, analytical methods, decision making tools)



Lifelong Learning Programme

### 4.2. Direction of Participants

As the course is designed for a target group bringing in general work experience, it is important to tie up these experiences in the training design. This could be done by the following:

- up-taking and active involvement of participants prerequisites and previous knowledge
- considering individual operational processes and structures of different companies
- using appropriate examples and analogies

### 4.3. Objective agreement with participants

Furthermore the agreement of learning objectives at the beginning of the course is a useful method to tie up prior experiences and competencies:

- query participants needs and expectations towards the workshop
- agree in writing, what topics can be covered and which could not
- appointing input expected by participants
- clarifying support requirements
- defining and agreeing on common rules for working together

### 4.4. Distribution of Activities

As learners should be activated and supported to learn self-dependent, the following distribution of activities between teacher and students is helpful:

- teacher plans and prepares lessons, selects methods, provides materials and media and defined tasks
- teacher should not act as lecturer; basic information should primarily be distributed via Internet together with self-tests and short exercises to secure learning progress; face-to-face teaching situations shall primarily be used for practical transfer of previously learned information and for more complex exercises securing the ability to transfer newly gained knowledge to new situations
- teacher moderates the learning process, i. e, he/she observes, provides guidance and assistance as needed
- learner is actively involved in the learning process using provided media and materials and performing learning tasks

### 4.5. Learning Difficulties to be expected

Due to heterogeneous learning groups and different pre-conditions of each participant, the occurrence of learning difficulties is most likely. According to the course topics the following aspects are most likely to be sources for difficulties:



Lifelong Learning Programme

- ICT expertise
- Legal issues
- Heterogeneous prerequisites of participants
- Participants will most likely not be willing to reveal own companies IS issues

### 4.6. Assessment and Exam Preparation

As it is the aim of this curriculum to provide a situated and practice orientated training, the assessment and examination – if implemented – should also mirror this approach.

- comprehension questions following newly gained knowledge, such as multiple choice (e. g. part of the WBT)
- Transfer of knowledge / application of knowledge in changed contexts (e. g. as part of classroom instruction)
- application of knowledge in complex projects, such as drawing up a security concept for the company as a final module
- presentation and discussion of the results in front of teachers and / or study group



Lifelong Learning Programme

## 5. Blended Learning

The course is planned as a so called blended learning approach, meaning that some units shall be thought face-to-face and some online.
The present curriculum was designed in a way that approximately 1/3 of the training (16 Units) shall be thought face-to-face and 2/3 (24 Units) shall be thought online. The following image provides a suggestion on how this could be organised. The structure is not compulsory but shall serve as an example or guideline.

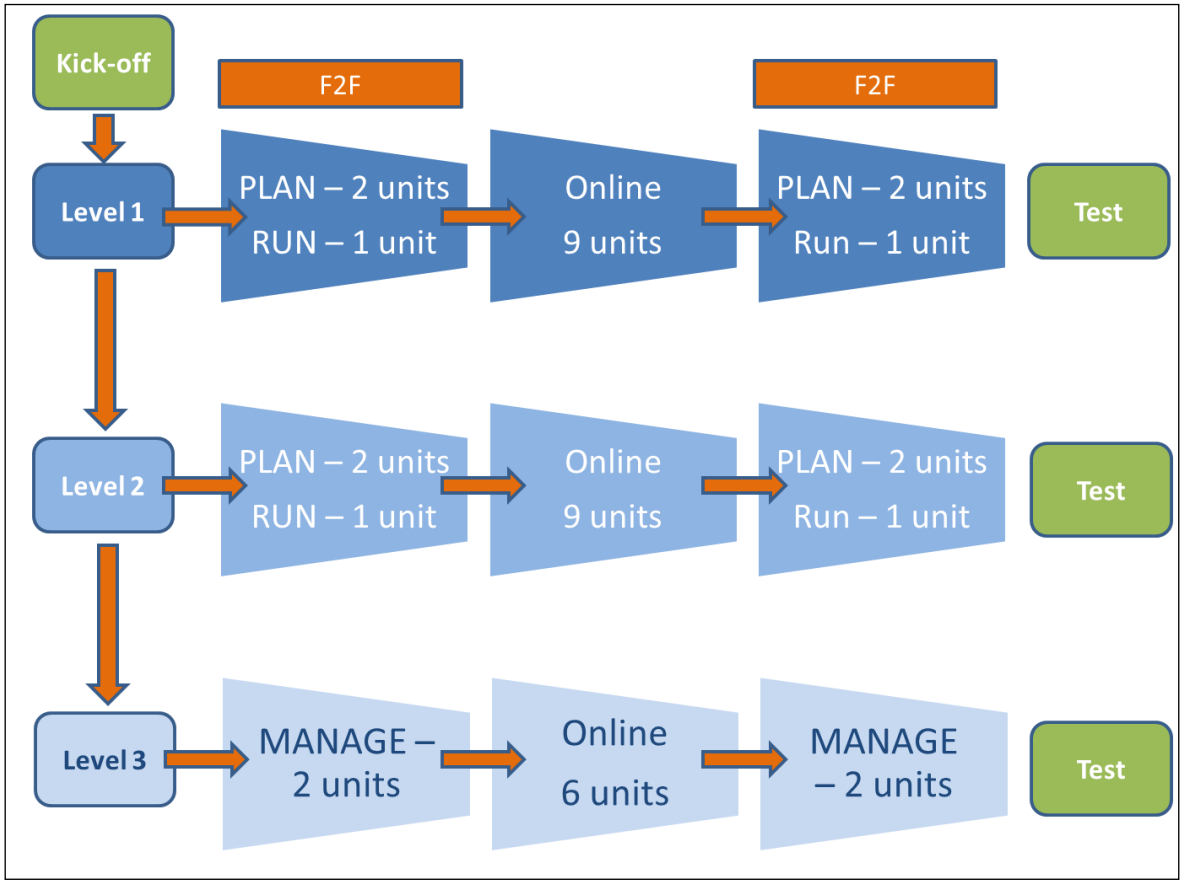


Image 3: Blended Learning Solution

In regard of different target group needs and expectations a different distribution of online and face-to-face units is certainly possible.

As participants might not be familiar with either blended learning in general or the e-learning environment in particular, it is recommended to start with a kick-off during which both should be explained and introduced. Also the kick-off is an opportunity for participants and trainers to get to know each other. Time necessary for the kick-off is not contained in the planned 40 training units.

At the end of each level a test is recommended to ensure that learning objectives have been achieved by the participants. The tests could also serve as basis for a certificate. Time for the testing is not contained in the planned 40 training units.



Lifelong Learning Programme