

**IO1 Report: Cybersecurity Competence Framework**

**Work package methodology**

**InCyT – Interdisciplinary Cyber Training**

**Authors: Ileana Hamburg, Fikret Öz, David Sommer**

Table of contents

[1. Introduction: Cyber Attacks and Frameworks 4](#_Toc100654148)

[2. Existing Frameworks 5](#_Toc100654149)

[3. The Erasmus+ project InCyT 6](#_Toc100654150)

[4. The structure, steps of the InCyT Cybersecurity competence framework - Output 1 and short description of the planed tasks and corresponding methodology 7](#_Toc100654151)

[4.1 Preparatory work 8](#_Toc100654152)

[4.1.1.2 Desk Research and Interviews 8](#_Toc100654153)

[4.1.1.2 Examples of References used by partners for Desk Research 11](#_Toc100654154)

[Germany 11](#_Toc100654155)

[Turkey 11](#_Toc100654156)

[Poland 11](#_Toc100654157)

[Romania 12](#_Toc100654158)

[4.1.2 Main aspects to be considered for building a Cyber security strategy and contribution of InCyT 12](#_Toc100654159)

[4.1.3 References 13](#_Toc100654160)

[4.2 Tasks planned in the proposal to be carry out in the next outputs and methodology steps 14](#_Toc100654161)

[4.2.1 Review of digital skills and other ones necessary in cyber security for SME managers and employees to avoid cyber-attacks – short Report. 14](#_Toc100654162)

[4.2.1.1 Background Information 14](#_Toc100654163)

[4.2.1.2 Description 14](#_Toc100654164)

[4.2.2 Information about existing cyber training approaches in SMEs 16](#_Toc100654165)

[4.2.2.1 Background Information 16](#_Toc100654166)

[4.2.2.2 Description 16](#_Toc100654167)

[Germany 17](#_Toc100654168)

[Turkey 17](#_Toc100654169)

[Poland 18](#_Toc100654170)

[Romania 19](#_Toc100654171)

[Austria 20](#_Toc100654172)

[Italy 20](#_Toc100654173)

[4.2.2.3 References 21](#_Toc100654174)

[4.2.3 Information about cyber curriculum in VET in partner countries 22](#_Toc100654175)

[4.2.3.1 Background Information 22](#_Toc100654176)

[4.2.3.2 Description 22](#_Toc100654177)

[VET Germany 22](#_Toc100654178)

[VET Poland 22](#_Toc100654179)

[VET Austria 23](#_Toc100654180)

[VET Italy 23](#_Toc100654181)

[VET Turkey 24](#_Toc100654182)

[VET Romania 25](#_Toc100654183)

[VET Denmark 26](#_Toc100654184)

[4.2.3.3 References 29](#_Toc100654185)

[4.2.4 Opportunities for improvements of training by using interdisciplinarity and mentoring 30](#_Toc100654186)

[4.2.4.1 Background Information 30](#_Toc100654187)

[Mentoring in Germany 31](#_Toc100654188)

[Mentoring in Poland 32](#_Toc100654189)

[Mentoring in Italy 32](#_Toc100654190)

[Mentoring in Turkey 33](#_Toc100654191)

[Mentoring in Romania 35](#_Toc100654192)

[Mentoring in Denmark 36](#_Toc100654193)

[Mentoring in Austria 38](#_Toc100654194)

[4.2.4.2 References 39](#_Toc100654195)

[4.2.5 A short plan for an interdisciplinary learning and mentoring methodology 40](#_Toc100654196)

[4.2.6 A plan curriculum for a such interdisciplinary training to be adapted in each partner country 44](#_Toc100654197)

[4.2.7 Mentor handbook 47](#_Toc100654198)

[4.2.8 A short plan and adapted methodology for a special interdisciplinary course in VET and an European Methodology 49](#_Toc100654199)

[References 51](#_Toc100654200)

# 1. Introduction: Cyber Attacks and Frameworks

It is known that a competency framework is regularly used by companies to understand their skills-based requirements, necessary competences, skills of employees as well as gaps. When a competency framework is developed taking into consideration company profile and employee interests, it can improve performance and provide clarity for each individual role requirement and develop talent within the workplace.

In the last years, due also to many cyber attacks, cybersecurity frameworks are adopted particularly by large organizations (businesses, NGOs, and other entities) or by state actors.

A successful cyber attack can cause major damage to company business. It can affect its bottom line, as well as company business' standing and consumer trust. The impact of a security breach can be divided into three categories: financial, reputational, and legal.

Cyber attacks often result in substantial financial loss arising from stealing corporate information, financial information (e.g., bank details or payment card details), money, disruption to trading (e.g., inability to carry out transactions online), loss of business or contract. Businesses that suffered a cyber breach will also generally spend money associated with repairing affected systems, networks, and devices.

Cyber attacks can damage company business' reputation and the trust customers have for the company. This could potentially lead to, loss of customers, loss of sales and reduction in profits. The effect of reputational damage can even impact on company suppliers, or affect relationships with partners, investors and other third parties involved in company business.

So, data protection and privacy laws require to manage the security of all personal data company hold (of own staff or customers). If this data is accidentally or deliberately compromised, and company does not deploy appropriate security measures, it may face regulatory sanctions.

It is important to manage the risks accordingly. After an attack happens, an effective [cyber security tool or an incident response plan](https://www.nibusinessinfo.co.uk/content/cyber-security-incident-response-plan) i.e. by using a cyber consultant can help to:

* reduce the impact of the attack
* report the incident to the relevant authority
* clean up the affected systems
* get company business up and running in the shortest time possible.

It is necessary to invest in user training and education in the field of cyber security to avoid attacks and develop awareness for a cyber strategy in own organization on an ongoing basis.

Usually, a cybersecurity framework is a set of best practices and documented processes which are used for IT security policy making within an organization.

But unlike traditional policy related strictly to the legal field, a cybersecurity framework should also include **documented examples** of issues to be avoided through these policies and of the proper processes and ways to implement the security policies described in the framework. It’s at the same time a guide for employees and users, as well as a compelling compendium for best security practices which can be consulted by authorized external parties (like the authorities).

A cyber security competency framework can also help to a better evaluation of competencies necessary to avoid attacks, of gaps and measures to improve the situation.

Despite increased awareness and bold efforts, highly significant and increasing shortages of cybersecurity professionals in the European Union and of knowledge and skills of employees to avoid cyber attacks worldwide are known, and these shortages continue to present major problems for public and private sectors. “Strategies for Building and Growing Strong Cybersecurity Teams” (ISC) CYBERSECURITY WORKFORCE STUDY 2019, estimates that there are 2.8 million cybersecurity professionals globally, while the gap is actually 4.07 million. The study notes that the current gap in Europe is 291,000, and this number has doubled since the years before.

There are several cyber security frameworks which could help to improve this situation but not the cyber security competency frameworks already created and available for organizations to access in order to create their own version. There are various factors for this situation: the different national regulations for IT security across the world, as well as the specific threats. Many countries with a strongly developed expertise prefer to create their own set of regulations and documents, but many countries and small and medium companies (SMEs) need help in this context.

# 2. Existing Frameworks

Most of existing cybersecurity frameworks are developed by state actors and national intelligence agencies, to serve the big companies and institutions in that country. There are also cybersecurity frameworks developed internally, by big tech companies who prefer to develop their own, or to have one perfectly adapted to their specific scenarios. But only very big companies have the manpower, know-how and necessity to create their own cybersecurity frameworks. A unified set of practices and regulations serves as a common map and reference point for threat forensics but can help to overcome a security incident crisis. Some of known cyber security frameworks are

**Payment Card Industry Data Security Standards (PCI DSS)** targeted at the payment card industry and impact any e-commerce business, as well as the financial sector.

**US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF)** it has rapidly become very popular outside of this niche too. Many traditional businesses and large organizations adopted the NIST CSF gladly in a bid to strengthen their overall IT security, and it continues to garner the highest level of interest from late comers.

**Center for Internet Security Critical Security Controls (CIS)** deals with the most common forms of data breaches and attacks, in a hierarchy of priorities. While immensely valuable and popular because of it, the CIS framework is not intended to be the sole depositary of cybersecurity practices. It’s most often adopted alongside the NIST CSF.

**Control Objectives for Information and Related Technologies (COBIT)** is issued by ISACA (a non-profit organization known as “Information Systems Audit and Control Association”). The organization is praised for bridging the gap between government and business needs in its cybersecurity standards. The latest update of the framework was released in 2012, though, so depending on your sector of activity, you might need to consider a newer set of procedures.

**International Standards Organization (ISO) frameworks ISO/IEC 27001 and 27002** issued by the prestigious ISO, these cybersecurity frameworks have the advantage of being recognized almost everywhere in the world, unlike the U.S.-centric NIST and CIS options. Another plus of the ISO compliance rules for cybersecurity is that they’re not targeted solely at medium and large companies but can easily be adapted to small businesses too.

**The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework)** is a reference resource that classifies the typical skill requirements and duties of [cybersecurity](https://www.techtarget.com/searchsecurity/definition/cybersecurity) workers. The framework allows workforce developers, job seekers and educators to explore specific work roles as well as the skills, abilities and knowledge tied to each work role.

**SPARTA Cybersecurity Skills Framework (SPARTA CSF)** is proposed based on the structure of the NICE Framework, amended with EU specifics. The Framework is tested and validated for applicability, adaptability by industry and academia. Emerging threats are discussed with the further need to be incorporated into the Framework.

**The NIST National Initiative for Cybersecurity Education (**NICE) emphasizes that a critical step should be taken to address the shortage of “people with the knowledge, skills and abilities to perform the tasks required for cybersecurity work”. Such a group includes “technical and non-technical functions that are occupied by knowledgeable and experienced employees”. However, it is difficult to create a workforce with the necessary interdisciplinary skills and to solve the problem of communication between educators, researchers and people using information technologies. Cooperation and communication between these groups is necessary. One problem is that companies, especially SMEs with fewer resources, need help assessing the skills and skills gaps of their employees, using digital methods to improve the existing situation, and organizing training opportunities to reskill their employees.

**The REDCYBERSG Erasmus + project** does not develop a Cybersecurity framework but aims to improve cybersecurity management skills of SMEs by filling gaps in SMEs in partner countries and to provide a comprehensive guide for integrating best practices into their procedures in order to mitigate cyber risks. This is achieved by focusing on such direct target groups as VET teachers and trainers, SME managers and employees and other stakeholder organizations related to the SME sector, which can make use of the developed intellectual outputs respectively by educating students (future employees, as SMEs represent 99% of all businesses in the EU), training employees or, in case of stakeholder organizations, by sustaining and disseminating information regarding the education and training solutions.

# 3. The Erasmus+ project InCyT

The project would like firstly to develop a Cybersecurity framework that provides a mechanism for vocational and educational training (VET) and SME business to describe the competencies and skills that cybersecurity professionals, rather than professionals, are required to have in order to prevent cyberattacks. Taking into account the advantages of interdisciplinary training and mentoring programs, particularly in the area of cyber security, the team project develops, and tests digitally supported interdisciplinary training programs and a collaborative e-learning platform for SMEs. This training program will be customized for vocational training and for development of a European transferability model.

**Outcomes of the project will be:**

* methodology of a Cybersecurity framework for implementation,
* training (courses),
* opportunities for improvements of these by using interdisciplinarity and mentoring,
* learning and mentoring methodology,
* proposals for VET and an European approach,

**and the products:**

1. A framework.
2. A digital Interdisciplinary Cybersecurity training material for SMEs supported by mentoring and an adapted methodology for a VET special course.
3. A digital platform to support the training.
4. A report how interdisciplinary skills provide advantages for SME and VET and how to adapt the program for VET.
5. The European transferability model for the tested interdisciplinary training and mentoring.

This paper will present the Methodology used for the InCyT Cybersecurity framework. The Framework will be developed and validated interactively in cooperation with employees of some SMEs selected by partners and cyber consultants. The proposal of European Commission i.e., The Digital Competence Framework 2.0 (Dig Comp 2.0 https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework) will be used particularly in order to prepare employees for digital transformation within the training program which will be developed in InCyT. [DigComp 2.0](https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model) identifies the key components of digital competence in 5 areas which can be summarised as below:

1. **Information and data literacy**: To articulate information needs, to locate and retrieve digital data, information and content. To judge the relevance of the source and its content. To store, manage, and organise digital data, information and content.
2. **Communication and collaboration**: To interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity. To participate in society through public and private digital services and participatory citizenship. To manage one’s digital identity and reputation.
3. **Digital content creation**: To create and edit digital content To improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied. To know how to give understandable instructions for a computer system.
4. **Safety**: To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion. To be aware of the environmental impact of digital technologies and their use.
5. **Problem solving**: To identify needs and problems, and to resolve conceptual problems and problem situations in digital environments. To use digital tools to innovate processes and products. To keep up-to-date with the digital.

# 4. The structure, steps of the InCyT Cybersecurity competence framework - Output 1 and short description of the planed tasks and corresponding methodology

**This intellectual output will be a Framework, which provides a mechanism for SME companies and VET to describe necessary skills, competences, gaps and improve their digital skills in cyber security and connected disciplines. The main objectives are:**

1. Description of the necessary skills and competences, digital skill gaps and other ones necessary in cyber security for professionals, not professionals and future entrepreneurs in order to avoid cyber-attacks.
2. Review the training needs of SMEs in this context and help them to improve this situation.
3. Provide a robust methodology for achieving necessary skills through interdisciplinary training and mentoring and a curriculum.
4. Adapt the methodology for VET.

**The planned tasks**

* Review of digital skills and other ones necessary in cyber security for professionals and not professionals to avoid cyber-attacks.
* Analyze the gaps in this context in SMEs in partner countries by using short Interviews and Desk research.
* Describe the existing training (courses) in SMEs Framework.
* Analyze the teaching curriculum in VET in partner countries Additionally to experience of VET project partners, each partner will do short discussions with VET institutions from own country.
* Identify opportunities for improvements of these by using interdisciplinarity and mentoring Literature recherche and Examples of such programs (very few exists) will be used.
* Develop an interdisciplinary learning and mentoring methodology.
* Develop a plan curriculum for such an interdisciplinary training to be adapted in each partner country. Research results and Experience of such partners (i.e., the coordinator) will be used for the curriculum.
* Adapted methodology and curriculum for a special interdisciplinary course in VET will be developed.
* Plan of a methodology for a cooperative mentoring program HE and VET because mentoring is not used within VET will be developed.

## 4.1 Preparatory work

### 4.1.1.2 Desk Research and Interviews

**Background information**

The project partners decided to do a common preparatory work including:

Short interviews with Cyber Consultants for SME (2 in each partner country) in order to decide which training modules are necessary and will be developed in O2 and short Desk-Research studies within the project partner countries to describe the situation about Cybersecurity measures in their countries and necessary new ones to avoid cyber attacks. Main aspects to be considered and contribution of InCyT

**General Overview on the SMEs in the Partner Countries**

SMEs are a backbone of the economy with respect to the number of employees and number of companies. But research in SMSs regarding IT-security and Cyber-Security is mostly underdeveloped. A transfer of measures and strategies developed for big companies is less feasible since the SMSs haven’t got personal and resources to deal with it. Our project aims to deliver a substantial contribution to deal with Cyber-Security challenges in SMEs.

Previous research on SMEs Cyber Security shows that such companies are increasingly confronted with problems associated with IT-Security issues. Literature reviews highlights especially two major reasons why SMEs should deal with Cyber Security and take it seriously:

* SMEs are increasingly target for Cyber Attacks, small size is a misconception, on the contrary, they have less personal, financial means, skills and other resources to protect themselves
* They are confronted with intensified national and international compliance rules and regulations with respect to IT- and Cyber-Security with duties and penalties.

**General trends:**

* SMEs are using increasingly digitalisation and IT-Software and IT-Infrastructure (PCs, Tablets, mobile phones and increasingly cloud solutions (i.e. Microsoft 365, Google Suit G, etc.).
* Digitalisation is a cost factor and requires investments in infrastructure, personal and software.
* On the other hand, thanks to the digitalisation consumer and business relationships are getting extensive impulse with respect to sales and getting turnover via online sales and connectivity. In some sectors, calls for business bids take place only online. Several studies confirm an increase of productivity. Due to globalisation, it is also expected that this process will intensify.
* Disruptive tendencies in some sectors became visible and SMEs are increasingly confronted with intensified competence from abroad. The future of SMEs will depend on how they find and adjust appropriate solutions.

**IT-Security:**

* SMEs in general **underestimate** the IT-risks. Due to small size, they regard IT-problematic as an issue especially for big companies. They wouldn’t be a real target for dangerous cyber attacks. The fact is: computer viruses, trojans, pushing mails etc. are affecting increasingly SMEs and they are not immune against them.
* Internet of things, cloud solutions, Industry 4.0 etc. constitute new challenges for the SMEs, although not widespread but being increasingly applied.
* They also **overestimate** own possibilities to defend against such attacks. SMEs, mostly, don’t operate in a secure environment with limited number of own servers in a closed server system anymore. E-mails, cloud storage and operating systems, connection with costumers and business partners via internet build new challenges to IT-Security and make them vulnerable to cyber risks.
* Many SMEs haven’t got their own IT-Specialists or own IT-Departments. Internal training and the use of external consultation are underdeveloped.
* Mostly, they haven’t got a digitalisation strategy in general and IT-security strategy in special. Most investments are done in dies field by implementation of new hardware and software or successively updating existing IT-Structure. In many companies, several different IT-infrastucture and software systems may exist parallel to each other.
* Lacking IT-Security awareness and interest on the behalf of employees as well as employers and decision makers in general.
* Lacking Check-Lists and underuse of training measures to increase sensitivity regarding IT-Security.

**Driving Forces for IT- and Cyber-Security**

* Cyber-Attacks can cause irreparable damages and block the company.
* To fix such problems would cost, require long time and would endanger functioning and even existence of the company.
* Challenges to fulfil severe **compliance** regulations and rules at national and international level: EU-IT-Security regulations require extensive use of security systems as well data protection systems.
* In addition, business partners may require the fulfilment of such compliance regulations in order to make business together at all. Documentation and safety of consumer data and other documents must be secured and use of certain security systems would be required.

The **objective** of the desk research is to get a general overview on the Target group “SMSs” in the partner countries. The information gathered in the desk research will be used to design the web-pages in order to stress the importance of the SMSs as well as issues and challenges related to Cyber-Securtiy in general. The partners will also get an overview from the desk research about structure of SMEs in the partner countries.

1. **Analysis of the risk situation: What IT security gaps have SMEs?**

* Based on analysis of studies, reports and statistics a general overview about the situation and structure of in SMSs as well as essential risks and problems with respect to Cyber-Security.
* What are the major risks in the SMSs?
* Statistics and Surveys related to problems and risks regarding Cyber-Security.
* Are there any difference between big companies and SMSs on Cyber-Securtiy attacks?
* What type of risks and attacks are peculiar to SMEs?
* What kind of measures are taken in the SMEs to protect themselves?
* What kind of skills are needed?
* What kind of external and internal training programs do exist? Is there a lack of know-how about IT security and lack continuous training in this context?
* Awareness in the SMEs: Effects of digitization (including dangers) not known by employees, and they are not prepared.
* Are they prepared for targeted attacks on reputable customers?
* Is there lack of specialized employees in Cyber (IT) Security?
* Is there any IT security concept?

1. **Measures and programs in the partner countries**

* Are there any information sources in the partner countries with respect to IT-Security especially for the SMEs? The collection the links for such information sources can be done and presented in InCyT web-site. For example, national sources about regulations and EU-compliance and data security issues.
* If any, what kind of Funding Programs for Cyber Security measures do exist? List of such programs designed for SMEs, content, application requirements, form and type with corresponding internet links can be given.
* Are there accessible public information sources for employees?

**Questions for InCyT expert Interviews**

Besides desk-research, Interviews with IT CONSULTANT EXPERT OF CYBERSECURITY build second source for generating overview of Cyber-security issues in SMEs. The experts to be chosen must be a professional that support the companies to prevent cyberattacks. In each partner country, IT-consultant experts are interviewed to get in-dept insights for Cybersecurity in SMEs, their problems and their needs.

**Questions:**

* What are the main IT problems for a company?
* According to your experience, how much companies weight cybersecurity among the IT problems they can have?
* What are the main cybersecurity risks for a company? What are the most vulnerable sectors from a cybersecurity point of view in a company?
* According to your experience, are companies aware of their cybersecurity weaknesses? What can be done to make companies really aware of the risks they are facing?
* What are the best practices that a company should put in place to reduce the risk of cyberattacks?
* According to your experience, are managers trained to face cybersecurity treads?
* What are the cybersecurity competences that a manager should have?
* According to your experience, are staff (excluded IT) trained to face cybersecurity treads?
* What are the cybersecurity competences that the company staff (excluded IT) should have?
* According to your experience, what is the most efficient type of cybersecurity training for companies? (Theoretical lessons in the classroom / online, presentation of case studies, problem solving, cyberattack simulations, etc.)

**Sources:**

* Country specific secondary statistics from official sources, studies, surveys and reports.
* Interview with 2-3 IT-Consulting companies in partner countries which would have information based on own experience with respect to SME specific IT-Security (Problems, major issues, solutions).

**Output:**

4-5 Pages Report will be prepared in each partner country which highlights dimensions of cyber security problems in SMEs. In addition, it will deliver an overview of support programs with links and short description of the content of those links, where the visitors of the project web-portal would get in-deep information, beyond the training modules which will be developed in the framework of the project. Protocol of Interviews in thematic order. A Cross-Country-Report will be the major output based on Desk-Research in partner countries and the thematic results of expert interviews. The report will be published in project web portal for wide audiency

### 4.1.1.2 Examples of References used by partners for Desk Research

##### Germany

* Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S., & Henseler-Unger, I.(2017).Aktuelle Lage der IT-Sicherheitin KMU.https://www.it-sicherheit-in-der-wirtschaft.de/ITS/Redaktion/DE/PDF-Anlagen/Studien/aktuelle-lage-der-it-sicherheit-in-kmu-langfassung.pdf?\_\_blob=publicationFile&v=3
* PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC). (Februar2017).
* Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheitimdeutschen Mittelstand.vonhttps://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf

##### Turkey

* <https://data.tuik.gov.tr>
* https://www.savunmatr.com Turkey Cyber ​​Risk Perception Survey, TUSIAD, 2020, <https://tusiad.org/tr/yayinlar/raporlar/item/download/9428_0ff86134737e19b44a7425cb059f44f8>
* <https://tubitak.gov.tr>

##### Poland

* Skowrońska, A. Tarnawa: Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce, 2021, <https://www.parp.gov.pl/component/site/site/raport-o-stanie-sektora-msp-w-polsce>, Access: 28 January 2022.
* Cyberbezpieczeństwo polskich firm 2021, https://www.computerworld.pl/whitepaper/3727-Cyberbezpieczenstwo-polskich-firm-2021.html
* Raport roczny z działalności CERT Polska, Krajobraz bezpieczeństwa polskiego Internetu 2020, NASK – Państwowy Instytut Badawczy, <https://cert.pl/uploads/docs/Raport_CP_2020.pdf>

##### Romania

* Information & Communication Technology in cybersecurity - Romania,[Romania - Information & Communications Technology (ICT) (trade.gov)](https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict)
* Romania: From "Hackerville" to Cybersecurity Powerhouse, [Romania: From ‘Hackerville’ to Cybersecurity Powerhouse | Balkan Insight](https://balkaninsight.com/2020/03/27/romania-from-hackerville-to-cybersecurity-powerhouse/)
* Cyber Security training courses in Romania,[Cyber Security Training Courses in Romania (nobleprog.ro)](https://www.nobleprog.ro/en/cybersecurity-training)

### 4.1.2 Main aspects to be considered for building a Cyber security strategy and contribution of InCyT

SMEs in particular are objectives for criminal activities connected with these problems. In contrast to large corporations, their resources are limited - and hackers know that! The SMEs are the backbone of the economy in Europe, i.e. over 99 percent of companies in Germany, Poland are SMEs. More than half of the workforce are employed by SMEs. Therefore, it is necessary to help SMEs to avoid cyber attacks.

Arguments for cyber security measures

* Securing livelihoods.
* Avoiding Penalties: there are a number of laws, regulations, and standards that businesses must follow.
* Opportunity to win customers and keep them in own company. Customers expect their data to be safe with a company they trust with this data.

Cyber security should become part of the company strategy, so that the topic “security” is always considered in all planning activities, provided with its own budget and continuously developed in the future.

For the establishment and development of an efficient and effective cyber security strategy, the activities should focus, i.e., on three fields of action: (1) technology, (2) processes and organization and (3) specialist staff. Some examples are the followings:

**Technical measures**

* Use of virus protection programs and firewalls.
* Regular roll-out of software updates and patches.
* Regular creation of backups and the mirroring of these backups on another medium.
* Use of passwords and ideally even multi-factor authentication.
* Use of role-based authorization management.
* Use of encryption mechanisms, i.e., the encryption of e-mails or the use of a VPN connection when employees access the company network from home or on the move.
* Financial subsidies that SMEs could use for digitization and security measures from a wide range of subsidy funds.

**Processes and organizational measures**

* Get all employees on board because the human factor is now the biggest weak point in the company when it comes to protecting data and IT systems.
* Sensitize employees to the topic of cyber security, to create an awareness of the dangers and to arouse motivation and personal responsibility of employees. Regular awareness campaigns and training are urgently required for this purpose.
* IT staff should receive regular training. They should be equipped with the necessary skills, time resources to keep the IT infrastructure up, and running in day-to-day business and to be able to take care of the introduction and implementation of a cyber security strategy.
* Creation of behavioural guidelines for employees, such as password guidelines or guidelines for the use of mobile devices, but also the preparation of IT security concepts and emergency plans.

**Personnel measures**

* Invest in specialized staff with knowledge and experience in the areas of IT security and data protection.
* Use experts to help to build a cyber-security strategy.

Cooperation and communication between educators, researchers and people using information technologies these groups is necessary. One problem is that companies, especially SMEs with fewer resources, need help assessing the skills and skills gaps of their employees, using digital methods to improve the existing situation and organizing training opportunities to reskill their employees. The following picture shows some activities in this context which will be supported by the project InCyT.



### 4.1.3 References

Leeser, Daniel Christian (2020). Digitalisierung in KMU kompakt: Compliance und IT-Security (IT kompakt), Springer Vieweg.

OECD (2021).The Digital Transformation of SMEs, <https://www.oecd-ilibrary.org/sites/bdb9256a-en/1/3/2/index.html?itemId=/content/publication/bdb9256a-en&_csp_=42ee43b7fa49ef116a6caf8c78b53d84&itemIGO=oecd&itemContentType=book>, 14.03.2022.

## 4.2 Tasks planned in the proposal to be carry out in the next outputs and methodology steps

### 4.2.1 Review of digital skills and other ones necessary in cyber security for SME managers and employees to avoid cyber-attacks – short Report.

#### 4.2.1.1 Background Information

This report is based on preparatory work of partners in form of short desk research and interviews with consultants for cyber security in SMEs in project partner countries. It uses also references listed at the end of the report. The information will be used within O2 for the development of two training modules: for managers and employees.

#### 4.2.1.2 Description

**Existing competences of managers and needs**

**Existing competences**

Managers usually have no training regarding cybersecurity threats, since they consider this is a special field of IT training. In many companies there is not a cybersecurity expert and managers sometimes start understanding the need for security and the risks if security is not addressed. There is an improvement over the past years, i.e. related to such measures within health, financial sector, and logistics, but in many other sectors managers do not have the necessary training nor knowledge to address security as needed. They are not aware of training and have less time. In many companies managers do not understand the necessity of a cyber security strategy and security training for them and employees dedicated to IT and specially cybersecurity aware.

**Necessary competences**

Managers need to understand high level risks of cyber attacks in their organizations and the related threats but also potential measures to mitigate or minimize risks. They need to have a management system in place to continuously monitor and address those risks.

Every manager should at least know about current attack methods, the business models of the attackers (to better understand the motivation of the attackers), responsibilities of IT staff (being any kind of IT expert doesn’t mean that this person knows anything about IT security), the most important security measures and if they are implemented at their company together with legal requirements.

Managers should understand that cyber risks should be included as part of corporate risk management and a cyber security strategy is necessary as a part of company strategy and a special budget should be allocated.

Knowledge about Incident Handling + Business Continuity and Disaster Recovery Strategy but at least having a playbook to follow in case of an incident is necessary.

Compliance to ISO27001-5 or CIS Controls or any standard related to security + ITIL or COBIT or ISO 20000 and the channels through which information flows into and out of an organization’s information network should be known. Managers are responsible for observing all of the operations occurring across the network and managing the infrastructure that facilitates those operations. This means implementing software upgrades when necessary and performing maintenance and upkeep on computer hardware systems. Managers (or together with cybersecurity experts) have to ensure that they have an efficient amount of resources dedicated to critical tasks.

Technical skills are important, but also a solid set of soft skills to complement the technical ones, i.e. ability to manage stakeholders without risks is necessary. Managers need to take responsibility, know good practices regarding cybersecurity, trust his team and be able to pay attention to security details.

Another dimension of understanding the importance of cyber awareness for company is to support the staff who are in managerial positions today but who did not grow up with the internet, to adapt to the cyber change. Understanding that the cyber field is a new field of struggle and raising awareness of various opportunities and threats will remove a very important obstacle for cyber security for both the public and private sectors. It has been experienced that even in industries that work closely with technology, it is a time-consuming and sometimes unsuccessful process for managers to adopt the security dimension of the digital world. The biggest shortcoming is the lack of follow-up and awareness at the management level about what sectoral and operational cyber threats are. For this reason, comprehensive awareness trainings for senior management can cause a serious leap in cyber security at the corporate level.

**Existing digital and cyber competences of employees**

In general, the answer about existing competences at SME staff is negative. It is positive only in some limited cases for example in strategic sectors such as health and critical infrastructure. Many employees have not necessary digital competences in connection with security i.e. protecting data and devices they work. There are no such cybersecurity competencies required even in existing job offers.

Most of the employees do not participate in aware training for cyber security. Usually employees are trained in being aware about password security, sometimes about phishing threats. Employees do not take the time to focus on cybersecurity and managers do not help them in this context, i.e. offering on-the job training, more information and necessary time. Some employees have little knowledge of the IT technology they use, system updates, antivirus systems, backups, use of the cloud, exchange of passwords. Attackers often try to exploit the fewer skills employee/manager have to gain access to the company information. In many companies employees do not know the company’s cybersecurity rules and guidelines (if they exist) and what measures apply if security incidents occur.

While companies expect their employees to improve themselves regarding cyber security, they are afraid to allocate an extra budget and time for this. They expect employees to acquire these skills outside of work. This situation lead to the fact that employees do not know cyber security rules in their working life.

**Necessary competences**

Staff must understand attack patterns (social engineering attacks) and cybersecurity risks and threats, particularly related to their daily business and processes. They need to fully understand what consequences result from their cybersecurity wrong doings and how they can omit mistakes.

Staff need awareness training about the most common attacks, recognise and mitigate them or inform the manager/IT company expert. Staff should have knowledge about data protection, social engineering, phishing techniques.

Establishing a Cyber Security Committee that will work on the development and strategies of cyber risks in each company, including officials from human resources, operations, legal and other business units, and keeping in touch with a regular meeting calendar can be an effective form of management of cyber attacks.

### 4.2.2 Information about existing cyber training approaches in SMEs

#### 4.2.2.1 Background Information

This task is based on the information collected by the partners from discussions with SMEs representatives and literature research. This information will be used at the development of Training Modules within O2.

#### 4.2.2.2 Description

Cybersecurity awareness is achieved in large companies by using special courses and training, but a not inconsiderable amount of effort is required for the introduction and ongoing further development. On the other hand, security awareness usually goes hand in hand with technical and organizational regulations and measures to protect information, which usually exist in big companies but in many SMEs lack. In SMEs, cybersecurity awareness is often not required either by a regulator or by special additional requirements. In this context, certification according to standards, norms and frameworks often occurs on a voluntary basis or to increase reputation. Motivation and importance of digital and cybersecurity training in SMEs should exist because: e.g., in Germany 60% of employed persons work in SMEs (Federal Statistical Office, 2021).

* The degree of digitization in SMEs is considerable.
* For individual employees, the recognition and validation of digital learning experiences is also important since it enhances their opportunities on the labour market.
* People and vendors are one of the most critical factors in the “cyber defence chain”.
* Cyber-attacks on small and medium-sized businesses increased.
* Phishing and a lack of understanding of risks are on the rise.

But unfortunately:

* The role of employee skills in cybersecurity is undervalued in SMEs.
* Many SMEs (i.e., 89% of all companies in Germany), survived without regular security certifications (Status 2020).
* Budget for information/cyber security including training is very small – (e.g., less than 5%¨ of IT expenditure in most companies in Germany).
* Training methods often do not fit the specific needs of SMEs. Training programmes and methods available on the market are too often unsuited to the size and needs of SMEs185, both in content and in form.
* The continuous development of skills and knowledge of managers is therefore of crucial importance. As compared to managers in larger companies, those in SMEs less often have an initial training period in management and security.

Literature addressing differences between SMEs and large companies in terms of cybersecurity training of employees and managers is very limited. In the field of research, SMEs are already specifically addressed, but there are no experience reports from training campaigns, which were originally used for a large company and then adapted for an SME.

##### Germany

Since 2015, the Economic Affairs Ministry has set up a total of 26 Mittelstand 4.0 centres of excellence which provide the Mittelstand (SMEs) with information and specific support about digitalisation. A combination of regional centres of excellence in all parts of Germany and specific thematic centres (i.e, Open Competence Center for Cyber Security in Sigmaringen) delivers a wide range of support for all sorts of sectors and corporate needs. Workshops, training sessions, practical tests, webinars and surgeries: all of the services offered by the centres of excellence are impartial, easy to understand and designed specifically with small and medium-sized enterprises in mind. The Federal Ministry for Economic Affairs and Energy ensures the services can be used free of charge.

**Companies**

* Salzerfilm Marcus Wildelau & Daniel Blazek, Bielefeld
* Microsoft Deutschland GmbH Köln, Holzmarkt 2a

**Example of Content of training**

* Introduction to IT (cyber) security management
* Risk management approaches
* Creation of a security concept in company
* Practical development using a case study
* Computer and network security
* Protection of communication infrastructures
* Basics of attack detection
* Attacks on the Internet
* Secure email encryption

##### Turkey

Aksigorta, in cooperation with Boğaziçi University, provides free online education project services in the field of digital security with an understanding of social benefit. With the Digital Security Platform, which was established with a very rich content, it is aimed to increase the awareness of SMEs against the risks in the digital world and to have a safe digital experience.

In cooperation with Türk Telekom and Istanbul Chamber of Commerce, support is provided for the digitization of SMEs. With the free platform, which can be accessed at www.dijitalkobim.org, it is aimed to meet the digital transformation needs of 430,000 SMEs in Istanbul. The platform facilitates the digital transformation of businesses by providing training and consultancy services in 9 different transformation areas to SMEs in the manufacturing and service sectors.

**Example of Content of training in Turkey**

* Basic Network Concepts (OSI, TCP-IP, LAN, WAN, IP, DPI, Router, Switch, Firewall, DNS, DHCP, Protocols, etc.)
* Active Directory, LDAP, Kubernet, Micro Services, etc.
* Secure File Transfer Product Description and Application
* Network Firewall Policy Management Product Description and Application
* Cyber Security and Types of Attacks
* Concepts of Information Security
* Corporate Security Concept

**Examples of Types of Suitable training for managers and employees in SMEs**

Results of interviews done in InCyT partner countries show that the best company security awareness strategy including training depends on the organization, its structure and culture. Some forms of suitable training are classic theory-based training, either online or in the classroom, simulation of real attacks so that learners can understand how the attackers work and why they should change the way they used their systems or shared information until now, case studies, presentation of methods for problem solving.

Role of training will be to:

* Make Cybersecurity Clear To Employees
* Encourage Taking Great Care Over own Devices
* Teach Employees How to Spot Suspicious Activity
* Reinforce Confidentiality
* Examine Individual Cases of Cybersecurity Breaches.
* Provide employees with the ability to create complex and unique passwords (Secure password and authentication)
* Provide employess with the ability to securely store sensitive files (Digital File Security)
* Invest in penetration test findings
* Test and refine cyber incident response plan
* Prepare a cyber risk assessment as part of enterprise risk management.

##### Poland

According to data obtained from interviews done in InCyT project with two experts it should be emphasized that the global awareness in cybersecurity among SME’s in Poland is very low. It is a consequence of existence many self-employment companies where there is only one employee and micro family companies where there is no sufficient amount of available resources to ensure expected security level. The best situation is when the company serves outsourcing services related to processing of financial data. This is mostly due to regulations forced by GDPR laws.

**Examples of cybersecurity content training in Poland**

There aren’t many free trainings for SME’s related to cybersecurity, however we can indicate that there are some on-line courses (for example given by networkexpert.pl) mostly related to general topics like:

How to monitor security incidents?

* Security Operations Center - a real shield that protects your network.
* Security product portfolio - a broad view of security.
* Free Cybersecurity course for executives.
* Cybersecurity Training - Introduction to Cybersecurity.
* How to eliminate problems with the management and monitoring of the subscriber's wi-fi quality?
* IT security audit.

In the case of commercial trainings the offer is much wider and the costs are not very high. Approximately this is around 150-250€ per person. Among SME companies that offer such trainings we can indicate: networkexpert.pl, 4itsecurity.pl, niebezpiecznik.pl. The offered training are:

* Cybersecurity in practice. How to secure your workplace yourself?
* Cybersecurity training for the Board / Management / Employees
* Cybersecurity training for technical departments
* Training in OT Security - Protection of industrial networks
* Training in ICT security monitoring - SIEM, SOC, traffic monitoring
* Cybersecurity training - Cisco Firepower
* 802.1x training - NAC authentication system

The topics given in these trainings are related to some generals and to specific software/hardware details:

* Secure passwords and authentication.
* Test and refine cyber incident response plan.
* Cyber risk assessment.
* Cybersecurity as part of enterprise risk management.
* Special technical solutions related to protect companies resources.
* Increase of security awareness in company.
* Practical use of GDPR law.

##### Romania

Digitalisation is one of the main challenges – if not the biggest challenge – for Romanian business at the moment. Especially for SMEs, which are a heterogeneous group. In digitalisation, there are “front-runners” developing new technologies and those which have to adapt to new technologies.

Moreover, SMEs are not homogenous in terms of internal capacity and resources either, ranging from microenterprises to medium sized companies. Therefore, challenges are different and SMEs need different support measures according to the level of digitalisation and size.

To face digitalisation, SMEs needs are enabling legal framework which must be flexible enough, technology neutral and future-proof. Additionally, it needs to ensure fairness, transparency and a level playing field for all companies.

In order to support SMEs in the digital transformation, it was launched DIHs at regional level (Digital Innovation Hubs) and a program to strengthen the development of the craft sector / creative industry sector. The aim is to raise awareness about digital opportunities and to inform and guide SMEs in their digital transformation.

In order to meet its objectives, the program has set some initiatives which are described.

**Example of content of training in Romania:**

* Introduction to cybersecurity; basics of attack detection.
* Testing the security of the digital environment.
* Safely doing business on the internet.
* Introduction on ICT.
* ICT in start-ups companies.
* Basic Network Concepts and Security.
* Creation of a security concept in company (server, web, e-mail, network, protocols, hubs, etc).
* Secure email encryption.
* Risk management approaches.

Austria

Several companies offer training in Cyber Security, especially in the SME area: SBA Research offers trainings ranging from awareness to various certifications like CISSP, CISM and CISA. The CIS -Certification & Information Security Services GmbH not only organizes an annual symposium on cyber security, but offers a wide range of different certifications like Information Security Manager or Auditor according to ISO 27001, as well as company trainings and company certifications. Also other companies like Con.ect offer trainings, often with the support of external trainers. In addition, there exist several low-level entry points for SMEs that provide selected content free of charge, often in the form of Webinars or video lectures. The “Digitalization Hub Ost” (DI-HOST) is an example for such a project funded by the FFG, the national research funding agency, that focuses on providing such services, including Workshops and lectures on interesting new technologies. In addition, the “Future Network CERT” offers free Workshop and lectures on various topics, including Cyber Security by inviting experts in selected fields. In addition, the state of lower Austria provided a video lecture series for secure home office for SMEs in 12 parts, together with the St. Pölten UAS. In addition, the chamber of commerce regularly provides free Workshops and lectures on emerging trends in IT Security. In addition, the Wirtschaftsforschungsinstitut WiFi provides low-level courses on various topics and tools for both, private persons, as well as unemployed in the course of their re-employment trainings.

**Exemplary content trained in Austria**

* Awareness and basic security trainings, focusing on employees.
* Workshops targeting schools and educational personal.
* Secure homeoffice and emerging trends in IT Security targeting decision makers.
* Technical certifications like CISCO, CCNA, CCNP or ethical hacker CEH.
* Tools like Wireshark Scripting.
* Company certifications according to standards like ISO27k certifications.
* Personal certifications in the area of security management like ISM, CSM, CISSP.
* University degrees as offered e.g. by the St. Pölten UAS amongst others.

##### Italy

In Italy, data show that SMEs are increasingly victims of cyber attacks, so training on cybersecurity is an increasingly important issue. Therefore, today there are many VET providers offering different types of courses on vocational training. The courses offered by large US corporations (Cisco, Microsoft, etc ...) are very popular, but there are also courses developed by national or local realities. While these, on the one hand, are less internationally recognized, on the other they respond more specifically to the needs of local businesses.

Among the most relevant providers, the CLUSIT (Italian Association for Information Security), born in 2000, is the most numerous and authoritative Italian association in the field of information security. Today it represents over 500 organizations, belonging to all sectors of the Country-System. Among the activities, it provides specific training activities (Vertical activities and Ateliers), webinars and periodical reports on the cybersecurity in Italy.

Another relevant player at national level is CINI (National Inter-university Consortium for Informatics), made up of 49 public universities and involving over 1,300 professors. CINI established the Cybersecurity National Lab in 2019, which contributes to the creation of the national cybersecurity ecosystem, systematizing the excellence of cybersecurity research in Italy and offering its contribution to public and institutional decision-makers to secure the Italian cyberspace. and increase the competitiveness of the country system. The Cybersecurity National Lab has specific lines of action, carries out research, offers training, promotes calls and projects.

**Example of Content of training in Italy provided by Cybersecurity National Lab – basic level**

* Introductory Concepts (Introduction to Security, Cybersecurity - Definition and Relevance).
* Social Engineering (Social Engineering - Attack Vectors, Social Engineering - Prevention).
* Cryptography (Introduction and History of Cryptography, Symmetric Cryptography, Asymmetric Cryptography and Key Exchange, Steganography and Watermarking).
* Virus & Malware (Viruses and Malware, Access Control and Password Management, Secure Web Access, Cookies and Sessions).
* Digital signature & SPID (Hashing, MAC and Digital Signature, Public Digital Identity (SPID) & PEC).
* Privacy & GDPR (Privacy, Personal Data, GDPR).
* Ethical Aspects (Ethics and Security, Data protection and the limits of hacking).
* Legal Aspects (Criminal law on the web - IT crimes, Unauthorized access).

**Example of Content of training in Italy provided by Cybersecurity National Lab – advanced level**

* Network Security (Fundamentals of Computer Networks, Network Traffic Analysis with Wireshark).
* Cryptography 1 (Introduction to cryptography, History of cryptography, Perfect secrecy and one-time pad, Stream ciphers, Block ciphers in the real world).
* Cryptography 2 (Key Exchange Problem, Number Theory Hints, Easy Problems and Hard Problems, Diffie-Hellman Key Exchange, Public Key Cryptography and RSA, Integrity, Authentication and Non-repudiation).
* Web Security 1 (Introduction to http, The Web Browser, Authentication, User Session).
* Web Security 2 (Back-end, Database and SQL, Injections, SQL Injections, Command Injections).
* Software Security (Memory space, Reverse engineering techniques, Buffer overflows).

#### 4.2.2.3 References

Deutsche Telekom. (2019). *Telekom legt aktuelle Zahlen zur Cybersicherheit vor*. Retrieved from. <https://www.telekom.com/de/medien/medieninformationen/detail/telekom-legt-aktuelle-zahlen-zur-cybersicherheit-vor-573046>

ENISA (2021). Cybersecurity guide for SMEs - 12 steps to securing your business: <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>

Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S., & Henseler-Unger, I. (2017). *Aktuelle Lage der IT-Sicherheit in KMU.*

Kassner, M. (2021). 6 cybersecurity training best practices for SMBs. Tech Republic. Retrieved from: <https://www.techrepublic.com/article/6-cybersecurity-training-best-practices-for-smbs/>

Poriete, A. (2021). Retrieved from: The Best Practises for Cybersecurity Training in SMEs https://realbusiness.co.uk/the-best-practises-for-cybersecurity-training-in-smes

World Republic News (2021). 6 best practices for cyber security training for SMEs Retrieved from: <https://worldrepublicnews.com/6-best-practices-for-cyber-security-training-for-smes/>

### 4.2.3 Information about cyber curriculum in VET in partner countries

#### 4.2.3.1 Background Information

This task is based on information collected by project partners within discussions with VET representatives, old projects and literature recherche. Detailed analysis will be done within O5.

#### 4.2.3.2 Description

##### VET Germany

In schools as well as in companies, it is primarily the task of the administrator to ensure the security of the IT infrastructure, but poorly informed users also pose a certain security risk. This is not the only reason why IT security should also be a topic in teacher training courses, in teacher training and in the classroom teaching and learning within VET. Knowing some technical and security risks of using computers and learning suitable avoidance strategies are an important aspect of dealing competently with digital media, so the issue of data and devices also in VET protection plays a central role also in VET. Since the introduction of the EU General Data Protection Regulation (EU-GDPR), schools have to consider some security issues and implement, if possible, innovations in their programs. Learners in secondary schools and vocational training schools should be made aware of safe surfing on the Internet and deal with creating secure passwords, protecting personal data on the Internet and dealing with phishing and computer malware in specialist lessons. Some Best practices of courses in VET schools Business college in Geilenkirchen The IT Essentials course provides a comprehensive introduction to the IT and an in-depth look at PCs, hardware, and operating systems. Course participants will learn how various hardware and software components work, the basics of networking computer systems, and best practices for maintenance, operational security, and data security.

**OHM Professional School Nuremberg**

With the IT Security Engineering course, learners will acquire comprehensive knowledge of the security aspects of software and digitalization. This allows learners to guarantee IT security from development to ongoing operation of systems and applications. Upon completion, learners will be able to identify and monitor security properties and vulnerabilities in applications, systems and IT landscapes. can formulate security requirements in a structured manner, recognize and eliminate security risks and develop defense measures.

##### VET Poland

Taking into account historical conditions it can be shown that the current general situation of vocational education in Poland is caused by decline of vocational education at the end of the 80s when the importance of vocational training was totally marginalized and even some operational schools were closed. A negative image of the “inferior school choice” was created and it is still quite strong among teens. Many believe that only universities can provide a good level of education despite the fact that there are many private universities that cannot ensure an appropriate level of training. Many universities give to the job market young people rather with so-called general education and many of these people cannot find their place in the labour market.

In Poland the existing education system is undergoing many structural changes, however this causes some problems. The VET system in Poland has too frequent variability, the lack of close cooperation with the labour market and the lack of a coherent teachers’ education trainings of vocational subjects. VET is facing some challenges nowadays including: the increase of interest in vocational education and the involvement of employers in organizing practical trainings, adjusting the curricula to the labour market current needs and existing challenges, the improvement of VET teachers’ competences, the increase of the high-quality infrastructure in vocational schools.

Some best practices of courses in VET schools As a best practice in this field, we can indicate the program CYBER-MIL z klasą (CYBER-MIL with class) https://www.cyber.mil.pl/cyber-mil-z-klasa/, which is based on the running in secondary schools - in the form of a pedagogical experiment - classes with the “Cybersecurity and modern information technologies” profile. However, this is rather program related to military aspects of cybersecurity but not to existing problems in SMEs. There are 16 schools from all over Poland, one from each province, qualified to participate in the project. The curriculum will cover such subject areas as: basics of cryptography, history of cryptography, basics of algorithmics, basics of cybersecurity, data and information security management, algorithms and cybersecurity, data management and information security, risks management in the field of cybersecurity, information systems security and cryptographic aspects of data protection, design and implementation of local area computer networks and administration of computer networks. Learning in such a classroom will enable students to acquire knowledge and competences in the area of contemporary digital threats, risk management in the field of cybersecurity, information systems security and cryptographic aspects of data protection. The list of schools that are included in this project is here: https://www.wojsko-polskie.pl/u/c5/9d/c59dcb14-f20c-4ac5-b9fa-a0746f4e62b0/wykaz\_szkol\_zakwalifikownaych\_do\_programu.pdf

##### VET Austria

**Best practices in Austria**

One of the primary providers of a broad range of different interdisciplinary education, the Future Network CERT and CON.ECT can be taken. They provide a wide range of courses related to almost all topics of IT, with a special focus on security, ranging from very technical aspects to awareness related lectures. With their round table on security trends, they provide a very good overview on recent developments in the area of cyber security for SMEs, especially covering new relevant attack vectors and technologies. The current curriculum covers legal issues like paying ransom in cases of ransomware with fiscal relevant information, the protection of AI systems against attacks, as well as protection on cyber physical systems including autonomous driving. Other round tables focus on more organizational security related issues, especially new norms and standards relevant for the industry. The format is free for SMEs and provides ample opportunities to talk to actual experts in the field, with the possibility to do follow-ups in other formats.

##### VET Italy

In 2018, the Legislative Decree 101/2018 came into force: as required by the European Regulation 2016/679 (GDPR). This Decree aligns the Italian legislation on personal data to the European one. It was not a simple bureaucratic adjustment as the decree updated the data protection system previously in force in Italy. Legislative Decree 101/2018 requires a concrete assumption of responsibility by the person in charge of data control within the companies, as established by the GDPR. This applies both to incidents caused by companies themselves and to cyberattacks aimed at extorting data.

Italian Istituti Tecnici Superiori - ITS (advanced technical schools) are the segment of non-university tertiary training that responds to the demand of companies for new and high technical and technological skills to promote innovation processes. They represent an opportunity of absolute importance in the Italian training panorama as an expression of a new strategy based on the connection of education, training and work policies with industrial policies, with the aim of supporting interventions aimed at the productive sectors with particular reference to the innovation and technology transfer needs of small and medium-sized enterprises. One of the subject areas of ITSes is Cyber Security and Cyber Defense. These ITSes (e.g. ITS Angelo Rizzoli – Milan) train Cyber Defense specialists: professionals capable of identifying and documenting the security levels of the infrastructures, recognizing a cyber attack and managing the various phases of response to an incident. The specialists are trained to use the methodologies and tools for cyber security, independently assessing the validity of the results provided by the IT systems security monitoring tools. Moreover they learn to acquire the evidence and traces left in a compromised system to perform some basic digital forensic analysis operations.

**Best practices in Italy**

Fortunately, many other institutions are available to guide companies and schools in order to build this *security sensitivity*. Among all the tools available, the National Framework for Cyber Security and Data Protection issued by the CIS (Cyber Intelligence and Information Security) of Sapienza University in collaboration with the already mentioned CINI.

Some institutions (e.g. the University of Turin and the University of Tor Vergata in Rome) require all their personnel or specific categories to assess their security sensitivity by proposing short online courses and requesting them to pass an exam afterwards, otherwise they will not be able to access the information system of the institution or the computer center.

##### VET Turkey

Course curricula are prepared centrally in Turkey and the same courses and contents are taught in all cities. The Ministry of National Education is responsible for the preparation and implementation of the course curricula. Within the scope of Turkey's 2023 digital transformation targets, the process of updating the course contents and curricula started in 2019. In this context, Cyber Security is taught as a course taught in the field of Information Technologies in vocational high schools. Currently, the cyber security course is taught in the 10th grade and for 5 hours a week.

The course syllabus is as follows:

|  |  |
| --- | --- |
| Unit Name | Course Hours |
| Introduction to Cyber Security | 10 |
| Information Gathering Techniques | 25 |
| Penetration Testing Techniques | 30 |
| Sniffing Methods and Practices | 15 |
| Encryption Techniques | 15 |
| Password Attacks | 10 |
| DoS and DDoS Attacks | 15 |
| SQL and Man in The Middle Attacks | 10 |
| Wireless Network Security | 10 |
| Web Security | 25 |
| Total Course Hours | **180** |

**Best practices in Turkey**

Since the issue of cyber security is one of the most important strategic positions of the countries, Turkey has established a Vocational High School that provides special education in the field of cyber security. Established in Istanbul, this vocational high school trains cyber security experts by selecting students who are interested in cyber security and have a very high success rate. This school is also supported by the private sector and the defense industry, and laboratory and trainer support is provided. Students complete their internship activities by going to businesses 3 days a week in the 12th grade. In this way, their practical skills are also developed (<https://teknoparkistanbul.meb.k12.tr/>)

##### VET Romania

**Analyse of the teaching curriculum in VET in Romania**

This analyse study addresses the relationship between learning outcomes and curriculum policies and developments in vocational education and training (VET). The concept of ‘outcomes’ is not new to education and training; what is now evident is its greatly increased prominence over the past few years in national and European VET policies and in any discussion about curriculum reform.

Undoubtedly, developments linked to the European framework on key competences for lifelong learning (2006) and the implementation of the European qualifications framework (2008) had a decisive influence on this curriculum development discourse. Curriculum is increasingly seen by stakeholders as a dynamic framework guiding teaching and learning processes and as a steering mechanism for quality. It features in key Romanian policy documents as a new consensus for contributing to Europe 2020, the European strategy for smart, sustainable and inclusive growth. Findings of empirical research widely recognise that curriculum relevance is a condition sine qua non, not only for improving the human capital potential of education and training graduates but also for retaining learners in education and training systems. The endemic irrelevance of curriculum may be one of the greatest obstacles to matching education and training provision successfully to learner and labour market needs.

Adopting a learning outcomes approach when developing curricula, valuing what a learner knows, understands and is able to do on completion of a learning process – irrespective of how, when and where this learning takes place – is seen by many European countries as an effective way to avoid such potential mismatches and promote active learning and inclusive teaching. For VET providers and employers, outcome-oriented curricula can offer a valuable platform for bridging the worlds of education, training and work, providing a common language between competences acquired in learning and the needs of occupations and the labour market.

**Experience of VET project partners,**

Romanian VET offers diverse paths for learners. It comprises professional and technological programmes, regularly updated to combat low participation in lifelong learning and early leaving from education and training. As many EU countries, Romania has an ageing population. This has an impact on VET, with an 8.5% decrease in the number of VET upper secondary schools since 2012/13. Efforts are being made to increase student participation, enable access to VET, and improve its quality and its relevance to the labour market. Recent system developments include the introduction of a dual VET form: it complements the work-based learning tradition in school-based programmes and aims at making VET a more attractive option for learners, while adapting training better to employer needs.

‘Connecting education!’ is one of Romania’s priorities during its first Presidency of the Council since it joined the European Union (EU) in 2007. It is underpinned by principles engaging with each other like cogs, across all levels and types of education and training from early childhood education to adult learning: excellence, inclusion and mobility. Vocational education and training (VET) for young people and adults has a strategic role to play in this endeavour. The Presidency’s focus on excellence and key competences, as well as upskilling and reskilling of adults, highlights crucial features for VET: open to all, of high quality, responsive to current demand and forward looking.

Romania’s challenges and its national priorities for initial and continuing VET –improving its relevance and quality – are closely linked to those at EU level. By constantly adapting its diverse VET system with vocational, professional and technological paths, the country aims to reduce early leaving from education and training and boost participation in adult learning; these are two areas with considerable scope for improvement in relation to other Member States. Promoting upskilling programmes, reintegrating adults into education and training through second chance programmes, and expanding apprenticeships and other work-based learning schemes are measures that have the potential to bring about change.

##### VET Denmark

**Information about cyber curriculum in VET in Denmark**

**Perceived barriers in the implementation of digital security**

The analysis indicates that many Danish SMEs do not have a sufficient level of digital security, it is with 6 pct. of Danish SMEs, which indicate that they have experienced challenges in using IT security solutions. This may be because it is mainly companies that work focused with implementation of security solutions that encounter challenges. It is especially larger companies that have experienced challenges. It’s interesting, as are the big companies has the highest level of digital security. This may be because companies need to have employed with digital security to meet challenges in applying IT security solutions. The numbers can therefore reflect that the big challenge in the future still lies in getting the companies to get eyes up to the subject.

The challenges related to implementing IT security solutions are:

|  |  |  |
| --- | --- | --- |
| 1 | Other obstacles, limitations or challenges | 48% |
| 2 | Lack of IT knowledge and skills to handle IT security solutions | 48% |
| 3 | Uncertainty about the company's gain from investing in IT security | 47% |
| 4 | Lack of financial resources for investment in IT security | 30% |
| 5 | Lack of specific IT security solutions in the market | 21% |

Among the 6 per cent who have experienced challenges, it is primarily challenges with a lack of competencies and knowledge of IT security as well as uncertainty about the financial gain from investing in digital security they mention. This indicates that there is still a need to disseminate knowledge about digital security to Danish SMEs.

**What kind of external and internal training programs do exist? Is there a lack of know-how about IT security and lack continuous training in this context?**

Both private and public institutes/VET/professional high schools/ universities offer education at basic, bachelor and master levels, so companies and authorities have the opportunity to qualify and train IT security personnel and managers to tackle the growing pressure on cybercrime.

The number courses offered is rising, and SMEs can have financial support to improve their IT competences and development of the company. And there is an increasing awareness of the need to address the cyber security – but there is still a “long way to go” as described.

Courses are offered to both employees, management and board members. There is accessible public information sources for all, incl. some basic free of charge training to some type of employees (AMU).

**Measures and programs in Denmark**

The Danish Business Authority works to ensure that companies' utilization of digital opportunities goes hand in hand with digital security and data protection. If digitalisation is to continue to translate into growth, it requires trust in companies' digital systems and data management.

Digital security and responsible data management can create a new competitive advantage for the Danish business community, because companies that are skilled at protecting their data are considered credible partners. The goal is therefore better use of data within the framework of the legislation.

The Danish Business Authority works both to create the best framework for companies and to protect users' privacy when, among other things, roaming the internet. They support companies in the implementation of the Data Protection Regulation (GDPR) and work to strengthen the level of knowledge and information about digital security and personal data among small and medium-sized enterprises.

On the website of the Danish Business Authority, there are a number of information and tools for the SME on how to improve their cyper security:

**Digital security and responsible data use**

Find guidance and tools on digital security and report breaches of IT security. Read about the Business Forum for Digital Security and a brand for IT security and responsible data use.

**Read about digital security and responsible data use**

Personal data security in the telecommunications area

Providers of electronic communications services must meet a number of requirements to secure users' personal data. Read about the legislation and see what it means for you as a provider.

**Read about personal data security in the telecommunications area**

Personal data for companies

How do you handle personal information in your company? Test it on the Privacy Compass and get help complying with the data protection rules.

**Go to privacykompasset.dk**

Test your company's digital security

Is your company vulnerable to cybercriminals? Test it on the Security Check and get a personal report on how you can increase the digital security in your company.

**Go to safetystjekket.dk**

Good advice on digital security

On this information portal on digital security, the Danish Business Authority has compiled a number of action-oriented advice that can strengthen the IT security in your company.

Check your company's IT security

Become wiser about the company's risk profile

Get around 17 important IT security topics spread across 5 themes

Get a unique report that shows exactly where it is most important to invest

**Go to tryggdigital.dk/virksomhed**

Rules for using data

Brugdata.dk provides an overview of what companies may and may not do when they collect, store, pass on and protect data, and when companies use data for marketing in Denmark.

**Go to brugdata.dk**

Further, all SMEs can be supported by the 5 regional business centres (Erhvervshus), which offer all companies in the free and impartial sparring on digitization. SMEs can also gain new knowledge and concrete tools through events and in-depth program courses - always with respect for your time, and targeted at your unique company's challenges and ambitions. The program runs come all the way around the IT and cyber security. Everything that shall drive the company, develop or consolidate the company, and perhaps lift the growth: Short events, physical as well as virtual, concentrated, new nourishment for professionalism is offered. Program courses and events on digitization offer:

**Digitization boost**

With Erhvervshusene's nationwide program DigitizationBoost, your company gets the opportunity for up to 33% co-financing of development hours to develop new products, solutions or concepts within digitization and Industry 4.0.

**Scaling Through Digitization and Internationalization**

The Erhvervshus offers scaling courses that improve your company's prerequisites for success with digitization, exports and other internationalization.

**Become: Digital**

Stay: Digital is an offer for those who have plans to make your business more digital, but do not quite know how to make digitalization a reality. Get specialist help for a specific problem.

“With Become: Digital, you get help with the digital challenges that stand in the way of your company's productivity. Maybe you dream of going from handwritten timesheets to digital time recording, or maybe you need training in a new storage system.

We offer co-financing of 50% of up to DKK 100,000 for specialist help or peer training. Your company must co-finance 75% of the amount applied for in the form of hourly co-financing. This means that the participating employees must invest hours in the course, which corresponds to 75% of the amount applied for. There is a participation fee of 6% of the amount applied for. We hold your hand throughout the process - also in the application process, where you are free to contact us for help with the application form” .

Some of the best practices on Cyber Security education

1.

Aalborg University

Fredrik Bajers Vej 7K

DK-9220 Aalborg Ø

Tlf.: +45 9940 9940

Mail: [aau@aau.dk](mailto:aau@aau.dk)

Aalborg University's master's program in Cyber Security is an interdisciplinary master's program with roots in several different research environments at Aalborg University. The education is in English and is about prevention, detection and management of cyber threats and cyber attacks on different types of systems. The training in Cyber Security gives the student the skills to deal with the challenges that companies, and institutions face in connection with an increase in cyber-attacks.

2-years master study program.

<https://youtu.be/KmoZwgsovh4>

2.

It-sikkerhed - [Københavns Erhvervsakademi i København](http://www.kea.dk)

It-sikkerhed - [Zealand - Sjællands Erhvervsakademi i Næstved](http://www.zealand.dk/)

It-sikkerhed - [UCL Erhvervsakademi og Professionshøjskole i Odense](http://www.ucl.dk/)

It-sikkerhed - [UCN i Aalborg](file:///C:\\Users\\user\\InCyT%20Project%20Dropbox\\Gabriel%20Vartopeanu\\PC\\Downloads\\ucn.dk)

It-sikkerhed - [Erhvervsakademi Aarhus i Aarhus](http://www.eaaa.dk/)

The professional bachelor's program in IT security is a top-up for the business academy programs Computer Science and IT technologist. Competencies in governance, including the good procedures for avoiding attacks as well as forensic, which is about how to solve and document attacks. As a graduate, you can apply for jobs such as Information Security Officer, IT security consultant, IT security engineer.

2-years BA study programme. In the third semester, you must do an internship in a company. Here you get the opportunity to link the theoretical knowledge you have gained in the first and second semester with practical experience.

#### 4.2.3.3 References

CEDEFOP (2010). Learning outcomes approaches in VET curricula; A comparative analysis of nine European countries. Retrieved from: <https://www.cedefop.europa.eu/files/5506_en.pdf>.

CEDEFOP (2019). Vocational education and training in Romania. Retrieved from: <https://www.cedefop.europa.eu/en/publications/4171>.

cyVETsecurity (2018). Joint VET curriculum in cybersecurity Retrieved from: <http://www.cyvetsecurity.eu/wp-content/uploads/2019/11/O1_Joint-VET-curriculum-in-cybersecurity-EN.pdf>.

Erasmus + (2021). AWARE - Enhancing the level of cybersecurity awareness in VET related to digital transformation. Retrieved from: <https://www.eurosc.eu/en/projects/vet/317-aware-enhancing-the-level-of-cybersecurity-awareness-in-vet-related-to-digital-transformation>.

Global IT Factory (2021). VET Curriculum Management. Retrieved from: <https://globalitfactory.com/cms-function/vet-curriculum-management>.

Mossop, L., Dennick, R., Hammond, R. & Robbe, I. (2013). Analysing the hidden curriculum: use of a cultural web. Retrieved from: <https://onlinelibrary.wiley.com/doi/full/10.1111/medu.12072>.

OAC Curriculum (2021). Retrieved from: <https://www.openaccess.edu.au/curriculum/vet/vet-subjects/certificate-iii-in-information-digital-media-and-technology-cyber-security>

Radu, G. (2014). Work Based Learning in Romanian Initial VET - Goals, Success Factors and Challenges. Retrieved from: <https://www.archive.erisee.org/sites/default/files/Gabriel%20Radu,%20Regional%20coordinator%20at%20the%20National%20Centre%20for%20TVET%20Development,%20Romania.pdf>.

### 4.2.4 Opportunities for improvements of training by using interdisciplinarity and mentoring

#### 4.2.4.1 Background Information

This task uses the experience and publications of the coordinator and some partners with advantages of interdisciplinary training and mentoring also tested in other projects, literature research and discussions with experts at different events. The information will be used in O3 and O4 at the development of Interdisciplinary training.

“Real world problems rarely arise within orderly disciplinary categories, and neither do their solutions” (<https://www.masterstudies.com/article/why-are-interdisciplinary-skills-in-management-and-technology-important/>). The modern workplace is changing; it follows that the workforce must change, too. Interdisciplinary skills are considered one of the essential  attributes for the employees of today and tomorrow. The results of an interdisciplinary approach are widely beneficial. When employees can understand and make connections across different tasks and different knowledge and skills, they embark on a path to more rewarding lives and employment opportunities.

National Initiative for Cybersecurity Education (NICE) underlines that in many crucial areas an “integrated cybersecurity workforce” is necessary also due to many cyber-attacks. For example every work role in the apparently technical “Securely Provision” workforce category, requires quintessentially non-technical knowledge of “laws, regulations, policies, and ethics as they relate to cybersecurity and privacy”. The question, then, is how to produce a workforce with these inter-disciplinary skills.

Vocational Education and Training (VET) has an important role in this context and try to encourage the economic, social and technological development of companies, also within their  education but they should be more flexible by using also interdisciplinary teaching and learning methods. The learners develop an interdisciplinary understanding, learn to integrate areas of their expertise and discipline-specific ways of thinking. This increases cognitive abilities and critical thinking  more than through single disciplinary means. Evaluation of learner’s performance in developing interdisciplinary competencies can take a holistic view, including a look into the learning environment and learning outcomes, and facilitate interactive, effective and active learning. Companies should organize interdisciplinary learning for their employees and developing of their innovative skills. Studies have demonstrated that learning is positively associated with different forms of innovation in companies.

Learners should have the opportunity to apply acquired knowledge through experience and practice. Experiential learning theory underlines that students can achieve more when living concrete experiences and reflecting upon them. Active learning in the form of digital supported experiential interdisciplinary projects make the training more engaging for both trainers and students and also contribute to cultivate students’ communication skills, teamwork ability, creativity and critical thinking (https://www.abacademies.org/articles/experiential-interdisciplinary-approach-to-teaching-a-case-of-collaboration-between-entrepreneuship-and-media-production-7006.html). Learners experienced interactions with customers and applied knowledge of the market, industry, product, customers strategies into practice. This process engages  learners in the learning process. The acquisition of understanding about business and complex dynamics between businesses should be combined with traditional pedagogy. The interdisciplinary experiential teaching model implies that learning becomes a process; knowledge is created through the transformation of experiences acquired by students and teachers through the interaction between all involved in the educational process within a realistic environment (<https://www.abacademies.org/articles/experiential-interdisciplinary-approach-to-teaching-a-case-of-collaboration-between-entrepreneuship-and-media-production-7006.html>).

Mentoring is an experienced method of supporting more individual learning also to achieve personal and career competences for new professions. There are research papers on mentoring outcomes in general but there is little research if mentoring is used in VET. Mentoring offers a number of benefits for employees training in companies.

In connection with digitalization, education and training programs for employees and VET need to offer employees and future one’s opportunities to learn about and work with new technologies. The EU has been active in stimulating the use of digital technologies in all kinds of education, including through the development of the EntreComp: The Entrepreneurship Competence Framework ([https://publications.jrc.ec.europa.eu](https://publications.jrc.ec.europa.eu/)) and DigComp 2.1: The Digital Competence Framework for Citizens (https://publications.jrc.ec.europa.eu).

##### Mentoring in Germany

Mentoring is used in Germany as a career development tool. One-to-one mentoring involves a time-limited, informal transfer of experience and knowledge between a (professionally) experienced person (the mentor) and someone who is less experienced (the mentee). Mentoring is particularly valuable during an individual's transition phases, such as when starting a new career, re-entering employment and changing job or location. Mentoring can help people make considered decisions on future career paths in these situations. Experienced mentors use conversations, guidance and introductions to appropriate networks to support mentees in their professional development. Yet mentoring does not merely yield valuable advantages for mentees, mentors too can benefit from it.

Some benefits for mentors could be:

* Access to fresh knowledge and current developments,
* Insights into processes and working practices,
* Social and leadership skills training,
* Contacts and networks.

Advantages for mentees are:

* Familiarisation and feedback,
* Reflection and improved self-assessment,
* New contacts and networks,
* Access to experience and know-how,
* Understanding the unwritten rules.

A wide variety of topics can be discussed in a mentoring relationship, such as career goals and planning, job application strategies, development of personal skills like soft skills, leadership skills or intercultural communication, subject-specific topics, self-marketing strategies, networking and much more. Mentors contribute their wealth of individual experience and expertise and in the best case they are also able to respond to topics involving equal opportunity and social integration.

Examples of Mentoring programs in Germany:

GDEXA offers a free mentoring program for new arrivals in Germany, in which experienced personalities from the IT industry provide groundbreaking assistance with their personal stories on the subject of "education in Germany.

The Leopoldina fellowship program also includes a mentoring program. Participation is voluntary for all scholarship holders.

The Mentoring consists of the Leopoldina recommending an Academy member (mentor) from the appropriate section to the scholarship holders (mentees) on request and arranging for them to be available for mentoring. This is possible for both the postdoctoral students abroad and the returnees. It serves to promote the individual's professional development while maintaining academic independence.

The mentoring program of BPW Germany is one of the central offers for BPW members. It brings together women who are looking for professional support with women with professional experience.

In most cases, the professional reorientation of the mentees is in the foreground. With BPW mentoring, we have set ourselves the goal of supporting motivated BPW women from all sectors and professional positions in their professional development and career planning, including management tasks.

##### Mentoring in Poland

An example illustrating the use of mentoring by new small and medium-sized enterprises is the nationwide “Mentoring and Coaching Program”, which is a joint initiative of the Autokreacja Association and the Academic Incubators of Entrepreneurship. The target group of the program are young entrepreneurs aged 18–35 who are supported for 6 months by experienced businessmen acting as mentors. The scope of assistance includes running and developing a small enterprise, including such areas as: supporting a young entrepreneur in developing and implementing a business plan, transferring knowledge and helping in establishing business contacts, monitoring the company's development and solving problems, consulting and motivating.

According to the study given in [1] in the case of Poland we can indicate that:

* There is a high effectiveness of mentoring for talent development management as well as succession planning and management.
* One of the most important advantages of mentoring is the practice of measuring the effects of achieved results, such as: the level of achievement of business goals and results, and monitoring the progress in the development of skills and knowledge.
* In companies where there are no formal mentoring processes, as many as 63% of respondents see the need to implement such activities.
* 53% of companies use or plan to use a tool to manage and monitor progress resulting from arrangements in the mentoring process.
* In companies where mentoring is not used, respondents indicate the need to increase the level of its use, e.g. for young people who report the need to work with a mentor, not a manager, in all surveys.
* In companies where mentoring processes do not operate, respondents see a great need to implement them and use experts working in the company as mentors.
* The respondents also see the need to build a culture of sharing knowledge, especially for succession and ensuring the development of the best and most committed employees.
* The respondents see the need for mentoring to strengthen both employees for development (59.2%) and managerial staff (40.8%) and all employees in new roles.

It is assumed that such activity is one of the best effective among others.

[1] Mentoring in practice, HRM Partners, 2016, <https://www.promentor.pl/download/badanie-mentoirng-praktyce/>

##### Mentoring in Italy

In-depth knowledge of the Company is essential to allow the security specialist to assess the problems it may encounter and the related consequences. This knowledge is all the more thorough and precise the longer the security expert is working at the Company itself. The task of the internal experts is to implement an initial security of the system, to implement (when possible) and in any case maintain the defensive countermeasures that external consultants indicate, the consultants having a wider visibility of the national and international situation. It is not considered appropriate to set up a team of people with exclusively complementary skills (in economics, information technology, and in law) as they would not be able to speak the same language and would have distorted views of the problems, creating other problems as well. For the same reason, the personnel must have a deep technical background, to be complemented with economic and legal notions (not the opposite). The main skills must be in IT and the others a needed addition, not the opposite. The expertise of the in-house expert does not require in-depth theoretical notions such as cryptography or particular low-level investigation skills (software analysis and / or reverse engineering ability), but rather technical skills in installing and validating software and hardware equipment. The ability to carry out periodic penetration tests using out-of-the-box software is an important skill, but similar activities carried out periodically by a team of professionals is needed. Knowledge of national and international laws is essential in order not to make errors in implementing security policies, configuring devices, etc. therefore notions of law informatics are essential.

An example illustrating the use of mentoring in cybersecurity training is Deep, the Cybersecurity Bootcamp powered by Talent Garden in partnership with Var Group and Yarix. Among the most innovative blended training courses in circulation, the program combines the deep digital network of the Talent Garden network with the experience in the cybersecurity sector of the Cybint Solution learning platform, an Israeli Ed-Tech company specializing in international military security. A total of 14 intense but fascinating course weeks, which will prepare the students for entry level roles in cybersecurity, a fast-growing, high-paying industry with rapid career progression. Thanks to the close partnership with the Community Cyber Strategy Initiative, Deep students will be able to count on an individual mentorship path with a career advisor who will guide the students step by step. They will learn to value their experiences and tell their story, they will build their own network and in this way they will find a precious bridge to the job market. Mentorships will take place during your studies and the students will also have the opportunity to join their network.

##### Mentoring in Turkey

Although different mentoring practices are encountered today, mentoring models in general can be listed as follows (Crisp and Cruz 2009, p.529):

* One to One Mentoring,
* Peer Mentoring,
* Group/team mentoring (Group-Team Mentoring),
* Reverse Mentoring,
* Self Mentoring.

One-on-one mentoring is the classic and most basic mentoring model; It is the sharing of knowledge and experience by an older person (mentee) with a younger person (mentee). It is a preferred approach in the training of new managers, especially in the business world. Peer mentoring involves peers with similar conditions supporting each other in the learning process, and it is common practice in educational institutions. Team or group mentoring is a process in which at least 3-4 people with different characteristics interact, it is preferred in terms of increasing interaction and sharing. In the opposite direction, it is the young who have experience in mentoring, not the old. Especially recently, the new generation (Internet generation) can access information more easily and be more experienced than the elderly in the use of computers and technology. On the other hand, self-mentoring is the individual carrying out the process in line with certain goals. The most commonly used mentoring models in the literature are one-to-one mentoring, group mentoring, and peer mentoring.

E-Mentoring In the face-to-face mentoring practices, inappropriate matching, inadequate timing of the meetings, geographical barrier, neglect of the mentee by the mentor and not meeting the expectations, the feeling of inadequacy in the mentors, and the presence of a small number of mentors and mentee, etc. It is stated that various problems are encountered (Watson, 2006, p.175). As a result of the integration of new technologies, electronic mentoring (e-mentoring) emerges as a flexible alternative (sometimes complementary) to traditional face-to-face mentoring (Single and Single, 2005, p.301; Shresta, et al., 2009, p.122) . E-mentoring is important because it allows the sharing of information and experience regardless of time and geographical location and offers easy and different interaction methods independent of social prejudices. In addition to eliminating the status difference more easily, the e-mentoring process provides flexibility in the response time compared to face-to-face mentoring and offers the opportunity to reach more people (Akin and Hilbun, 2007, p.2).

E-mentoring offers some features that are not found in face-to-face mentoring, and e-mentoring conducted in online environments provides new alternatives because it is accessible to individuals. Especially online discussion, email, etc. vehicles have become very preferred as they remove the time and space limitations. Therefore, the problem of accessibility is solved with e-mentoring. However, individuals included in the e-mentoring program must have knowledge and skills related to the technology/software used at a certain level. In addition, effective strategies should be developed in e-mentoring practices and appropriate arrangements should be made for the online environment (Ensher, et al., 2003, p.265-279).

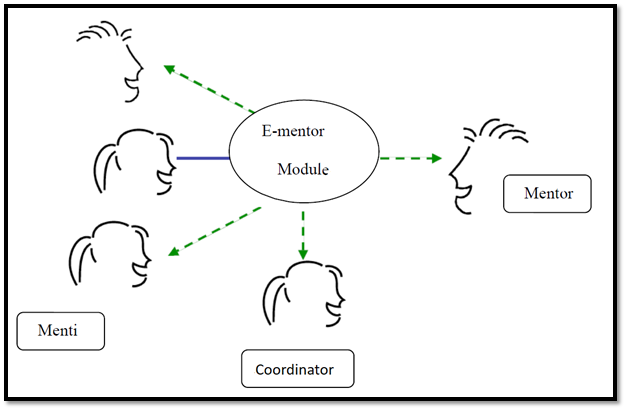
****

Figure 1: E-mentoring Model

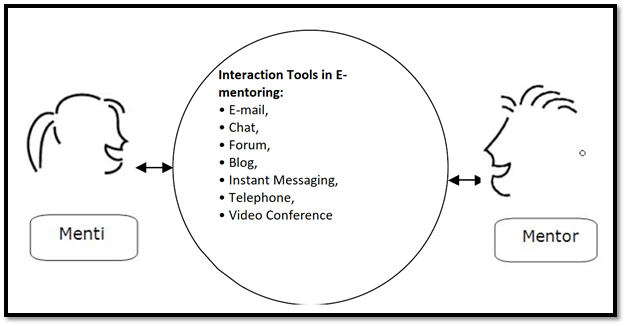
****

Figure 2: E-Mentoring Interaction Tools

##### Mentoring in Romania

VET in Romania comprises the following main features:

* + VET has a double role: promoting economic and social development in the country; it supports addressing challenges linked to very low participation in lifelong learning and a high share of early leavers from education and training;
  + Training standards were updated in 2016 to increase the relevance of qualifications to the labour market.

Since 2017/18, a dual form of initial VET has also been available; participation is growing but still low.

Distinctive features:

Distinctive features of initial VET are its inclusiveness, with pathways among different levels of learning and between vocational and more academic tracks, and its focus on easing progression and avoiding dead ends. Reflecting the double role of VET in promoting economic as well as social development, initial VET’s main goals are to ensure:

* + learners’ personal and professional development;
  + equal access opportunities to VET;
  + high-quality provision, organization and development.

Initial VET qualifications are based on training standards which describe the training process in units of learning outcomes and include, for each unit, an assessment standard. The standards were revised in 2016, to help increase VET labour market relevance by ensuring a better match between qualifications and the reality of working life after graduation. In line with guidelines adopted by the National Authority for Qualifications, procedural arrangements have been put in place to create a network of providers acting as validation/assessment centres. These centres are active in more than half of the counties.

Examples of such programs.

Initiatives and measures for the improvement and promotion of Vocational Training:

* Unified Vocational Training System.
* First Strategic Plan of the Educational System for Vocational Training.
* Draft Organic Law on Education.
* Permanent Collaboration Framework for Vocational Training.
* National Scholarship System and Study Grants Reform.
* Measures and actions against COVID-19 in Education Centres during the 2020/2021 school year 2019.
* First Strategic Plan of the Educational System for Vocational Training 2019-2022.
* Authorized military educational training centres to provide Vocational Training education.
* New Higher Vocational Training degree.
* Funding for Workshop Schools and Craft Houses and for Employment Workshops.
* Draft Law on Education.
* National strategy to prevent and fight poverty and social exclusion (2019-2023).

##### Mentoring in Denmark

There are identified three main levers based on input from a wide range of experts, scientists, entrepreneurs and lead users[[1]](#endnote-1):

**1. Cybersecurity competences**

To raise competences at all levels, we must 1) include cybersecurity in common education and regulate cyber security training requirements for companies and professions; 2) continue campaigning for a better general understanding; 3) invest in public research relevant to cybersecurity and 4) increase collaboration across sectors.

**2. Secure traffic and networks**

Today, the focus is mainly on securing the perimeter of organisations. In an increasingly open internet, security solutions must emphasise safe traffic and individual usability. To this end, we must invest in focused research, set national standards and stimulate innovative cross-disciplinary solutions.

**3. Security by design**

Many products lack cybersecurity measures by default, which increases the vulnerability to cyberattacks. We should develop a new production paradigm based on security by design through national standards and certifications, continuous development of best practices in different industries and promotion of usability in cybersecurity solutions

The efforts to grow skills are no different from other educational areas. We suggest the following actions:

• Include cybersecurity in basic education and regulate cybersecurity training requirements for companies and professions.

• Develop national campaigns to push awareness among companies and individuals to increase the understanding of cybersecurity and data privacy. The campaigns should emphasise that cybersecurity is not something you complete but an ongoing process.

• Invest in scientific competences to drive the development of both cybersecurity and the business it generates.

• Increase collaboration across authorities, companies and scientists to combine knowledge, experience and resources and thereby create better cybersecurity solutions.

**Next steps?**

The above recommendations can be put into practice in several ways. We suggest to:

• Teach cybersecurity in primary schools. This can be done by having a cybersecurity theme as part of the education in computational thinking as these two subjects are related.

• Guide companies towards educating people who have tasks that are related to managing data or systems on cybersecurity, including contingency plans in case of a breach.

• Develop specialised cybersecurity education as part of professional training for professions that include handling of personal data or navigation in complex systems, for example nursing or shipping.

• Set a goal for the number of students that should take a specialised cybersecurity education and create incentives for the universities to reach this number.

• Create deeper knowledge within cybersecurity by investing more resources in public research and innovation within:

- Identity and access management

- Trustworthy computing

- Network security

- Cryptology

- Security in socio-technical systems

• Establish targeted and strong public-private partnerships that include authorities, companies and research institutions, for example anonymised learnings from GDPR incidents and threat intelligence.

The table suggests more detailed recommendations for scientific areas that are worth investing in.

|  |  |
| --- | --- |
| **Identity**  **and access**  **management** | • Identification (including national electronic id systems)  • Authentication (including biometrics)  • Privacy by design (including privacy enhancing technologies, attribute-based  credentials and zero-knowledge protocols)  • Access control policies and mechanisms |
| **Trustworthy**  **computing** | • Security by design (including security engineering and programme/protocol  security) especially in relation to Internet of Things  • Computational trust and trust management systems  • Autonomous component security (defence in depth). |
| **Network**  **Security** | • Intrusion detection systems (including detection of malware/ botnet/ exfiltration/ etc.)  • Anomaly detection systems  • Security through decentralisation and shared ledgers, for example blockchain. |
| **Cryptology** | • Light weight cryptology  • Quantum and Post-quantum cryptology  • Secure multi-party computation  • Security of critical systems. |
| **Security in**  **socio-technical**  **systems** | • Security and the law  • Security usability  • Data ethics and social acceptability, for example personal data in research |

Recommended study plan for Master in Cyber Security



The study program for the Master in Cyber Security consists of 8 taught courses and 2 projects (incl. the final Master Project). The total workload is equivalent to one year of full-time work, but the study program is designed so that the courses and projects are taken over a 2 year period, with the possibility to develop an individual study plan that extends the program for up to 4 years in total. All of the taught courses on the Master in Cyber Security can be taken individually.

**Cyber Security mentor and mentoring**

1. Struggling to learn Cyber Security on your own? Get trained by industry-leading Cyber Security experts to mentor you towards success. Land your dream career in tech. Build something extraordinary. And have fun doing it[[2]](#endnote-2).

2. Women4Cyber[[3]](#endnote-3) is an initiative that aims to help fill the gender gap of cybersecurity professionals in Europe. In pursuing this objective, our main goal is to encourage and promote the skilling, up-skilling, and re-skilling of girls and women towards cybersecurity education and professions.

3. Combitech[[4]](#endnote-4) Cyber Security Program is a one year talent program for you who recently graduated (with maximum one year of work life experience). As a participator in the program you will work together with senior consultants in customer projects and thereby contribute to a safer society. The Combitech Cyber Security Program covers both technical and business perspective with some possibility to go into depth in certain areas.

##### Mentoring in Austria

Mentoring in Cyber Security has been tried by several institutions, especially through training weeks for certifications. Furthermore, simulation games for organizational cyber security can be described as a kind of mentoring: During these games, typically the players are confronted with information that they have to classify and solve – some of these games include feedback cycles, where the same scenario is played out multiple times with e.g. changing information density, different (graphical) feedbacks and so forth. After each round, the players receive feedback from their respective mentors, not only on the final results of their analysis and the subsequently initiated actions, but also on their decision-making process [1]. The target of this games often does not lie in the actual solving of the issues at hand, sometimes them even being unsolvable, but rather on streamlining the decision-making process.

Mentoring is also a very important aspect of the “Digital Pro Bootcamp” programme of the Austrian research funding organization FFG [2] – a program that targets SMEs as trainees and universities as trainers with the following training strategy:

* The training starts at a low to moderate level of knowledge and consist of a pre-phase that provides study material in order to eliminate knowledge gaps. Mentors are available in this phase in order to provide support in case of questions.
* The actual training is divided into two parts:
  + Knowledge transfer by teaching, typically using a combination of frontal teaching and exercises.
  + The direct application of the newly generated knowledge in a project, where one trainee works on his/her own project, supported by a mentor.
* The training plan is very dense, typically 9 weeks of training within 3 months time-span, thus the name “bootcamp”.
* After the training sessions, the projects are continued with the SME partners of the trainees, where the mentors build the bridge to the universities – transforming a teaching activity into a research project.

Furthermore, several universities provide dual study programmes [3}], where a student is not only doing courses at the university, but is also applying the leaner knowledge in a partner company in the course of a real-world (dual) project. These projects are typically mentored by two mentors, one from inside the university and one from the partner company conducting the project. This is especially valuable, as the side parameters and the requirements for carrying out the projects works in a real world environment, thus making the results as applicable as possible in actual products and services.

Also, with respect to increasing the number of female researchers in MINT, the FFG proposed the FEMTECH mentoring internships [4], where female tech students work on projects in tech companies, including direct mentoring by the company itself, but also supervision of the program through specialized FEMTECH mentors.

#### 4.2.4.2 References

Akin, L. ve Hilbun, J. (2007). E-mentoring in three voices. *Online Journal of Distance Learning Administration, X*(I).

CEDEFOP (2021). Improved VET learner feedback. Retrieved from: <https://www.cedefop.europa.eu/de/news/romania-improved-vet-learner-feedback>

Cheng, M., 2014. An undergraduate cyber-physical systems course. In CyPhy Wksp, p. 31-34.

Corbett, A.C. (2005). Experiential learning within the process of opportunity identification and exploitation. Entrepreneurship Theory and Practice, 29(4), 473-491.

Crisp, G. ve Cruz, I. (2009). Mentoring college students: A critical review of the literature between 1990 and 2007. *Research in Higher Education . 50*(6). 525-622

Ensher, E.A., Christian, H. ve Blanchard, A. (2003). Online mentoring and computer-mediated communication: New directions in research. *Journal of Vocational Behavior,* 63, 264–288

Fayolle, A., & Gailly, B. (2008). From craft to science: Teaching models and learning processes in entrepreneurship education. Journal of European Industrial Training, 32(7), 569-593.

Hamburg I. (2020). Creating innovative structures in workplace and vocational digital learning to ensure social distancing, ICDS 2020: The fourteenth international conference on digital society 3. 124-127.

Hamilton, E. (2011). Entrepreneurial learning in family business: A situated learning perspective. Journal of Small Business and Enterprise Development, 18(1), 8-26.

Kolb, D.A. (2014). Experiential learning: Experience as the source of learning and development. FT press.

Kram, K. (1985). Mentoring at Work. Glenview, IL: Scott, Foresman.

LERU (2016). Interdisciplinarity and the 21st century research-intensive university. 7 .

Single, P.B., ve Single, R.M. (2005). E-mentoring for social equity: Review of research to inform program development. *Mentoring and Tutoring, 13*(2), 303-322.

Watson, S. (2006). Virtual Mentoring in Higher Education: Teacher Education and Cyber- Connections. *International Journal of Teaching and Learning in Higher, 18*(3), 168-179.

### 4.2.5 A short plan for an interdisciplinary learning and mentoring methodology

**InCyT training methodology**

InCyT Interdisciplinary training model

**Interdisciplinary Training and Mentoring**

Entrepreneurs, and future ones, need complex ways of thinking and the ability to understand and integrate knowledge from different sectors, which requires interdisciplinary learning. Mazur (2015) argues that complex engineering problems require an interdisciplinary situation to be created in an almost natural way. Within an interdisciplinary approach, learners should integrate information from different disciplines and subject areas. They develop an interdisciplinary understanding, learn to integrate areas of their expertise and discipline-specific ways of thinking. This increases cognitive abilities and critical thinking more than through single disciplinary means (Pettermann & Kenedy, 2003). Evaluation of learners performance in developing entrepreneurial competencies can take a holistic view, including a look into the learning environment and learning outcomes, and facilitate interactive, effective and active learning.

Vocational Training (VET) try to encourage the economic, social and technological development of companies, also within entrepreneurship education but they should be more flexible in the methods they use. Companies should organize interdisciplinary learning for their employees and developing of their innovative skills. Studies have demonstrated that learning is positively associated with different forms of innovation in companies (Kafetzopoulos & Gotzamani, 2015). Learners should have the opportunity to apply acquired knowledge through experience and practice. Experiential learning theory underlines that students can achieve more when living concrete experiences and reflecting upon them. Active learning in the form of digital supported experiential interdisciplinary projects make the training more engaging for both trainers and students and also contribute to cultivate students’ communication skills, teamwork ability, creativity and critical thinking (https://www.abacademies.org/articles/experiential-interdisciplinary-approach-to-teaching-a-case-of-collaboration-between-entrepreneuship-and-media-production-7006.html). Students experienced interactions with customers and applied knowledge of the market, industry, product, customers strategies into practice. This process engages students in the learning process. The acquisition of understanding about business and complex dynamics between businesses should be combined with traditional pedagogy. The interdisciplinary experiential teaching model implies that learning becomes a process; knowledge is created through the transformation of experiences acquired by students and teachers through the interaction between all involved in the educational process within a realistic environment (https://www.abacademies.org/articles/experiential-interdisciplinary-approach-to-teaching-a-case-of-collaboration-between-entrepreneuship-and-media-production-7006.html).

Mentoring is an experienced method of supporting more individual learning also to achieve personal and career competences for new professions. There are research papers on mentoring outcomes in general but there is little research if mentoring. Mentoring offers a number of benefits for employees training in companies. Interdisciplinary team mentoring has gained importance in recent years, reflecting the need for a change in mentoring orientation because different entrepreneurial developments and fields are increasingly multidisciplinary. Interdisciplinary mentorship and networks of mentors can produce synergy in groups, generate innovative ideas and complex solutions to challenges, and create opportunities for collaborations and work.

**Learning methods**

Learning pathway

It is assumed that the InCyT training programme, will be structured across two modules, where each module consists of a number of units and topics:

* Information Security for Managers,
* Information Security for Employees.

So far it was proposed to introduce the following units, however some of them can be changed or renamed after first experiences with SME’s.

**Course schedule**

The course schedule begins with an introduction webinar, followed by the deployment of each module, where each module takes place over a 7-week schedule.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Module | Module Week | Learning Unit | Learning Activities | Assignments |
| Introduction | Week 0 | Introduction webinar | Webinar | None |
| Information Security for Managers | Week 1 | Introduction into Information Security, internal control systems | Webinar, Reading | Goal setting and alignment of business & IT strategy |
|  | Week 2 | Information security management | Webinar, analysis of ISO27001 | IS Policy & InfoSec Roles |
|  | Week 3 | Information security management | Webinar + exercise | Asset management |
|  | Week 4 | Information security management | Webinar + exercise | Control design & Measurement of effectiveness |
|  | Week 5 | Cyber risk and resilience | Webinar + exercise | BIA |
|  | Week 6 | Cyber risk and resilience | Webinar + exercise | Risk Assessment |
|  | Week 7 | Third party / vendor security | Webinar + exercise | Procurement requirements |
| Information Security for Employees | Week 1 | Introduction into Information Security, internal control systems | Webinar + exercise | Elaboration of sec controls |
|  | Week 2 | Cryptography Fundamentals | Webinar + exercise | Evaluation of techniques in use |
|  | Week 3 | Malware | Webinar + exercise | none |
|  | Week 4 | Security at business trips | Webinar + exercise | Comparison of best practices to actual state |
|  | Week 5 | Privacy & Data Protection | Webinar + exercise | Analysis of GDPR related issues and TOMs |
|  | Week 6 | Social Engineering / SPAM / Phishing | Webinar + exercise | Detection of social engineering practice |
|  | Week 7 | Security and Privacy in Social Networks | Webinar + exercise | Behavior analysis + short webinar on social networks security |
|  |  |  |  |  |

**Delivering the programme**

The first weeks should be dedicated to getting learners comfortable with the programme, the platform and collaborating online. If learners are not participating, they should be notified of the consequences (this should be detailed in the rules outlined in the induction week and referred to).

Each week the mentor should hold a short briefing of learners of what is required from them for that week (approx. 20 mins). This should be held online and should cover the following:

* What learning material they must cover for the week and a short summary of it.
* What tasks they must complete for the week.
* What assignment work needs to be completed.

The mentor should monitor the forums and answer learner queries ASAP. For all of the activities the mentor should ensure that all learners are participating. If learners are not actively participating the mentor should contact the learner to identify the reason why this might be happening and try to resolve any issues.

**Learner induction**

A learner induction session should be held place prior to the commencement of the programme. All learners should be notified of the date of the induction. It should cover the following topics:

* Overview of programme
* Demonstration of the Moodle platform
* Overview of schedule
* Overview of Assignments/Activities
* Expectations of learners during the programme (e.g. participation in online activities)
* Mentor name and contact details

Each learner should receive a copy of the course schedule for the programme and it should be made publicly available for all to refer to on the Moodle platform.

**Assignments**

Assessment of each module is based on Mentor Marked Assignments. The feedback on assignments should be provided within two weeks of the submission/deadline date. The key assessment tools are summarised, by module below:

|  |  |  |
| --- | --- | --- |
| **Module** | **Assignment** | |
|  |  |  |
| 1.2 |  |
|  |  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |

**Learning activities**

Learning activities occur throughout each of the modules to support learning, an outline of these activities by module is provided hereunder:

**Module 1**

|  |  |  |
| --- | --- | --- |
| **Unit** | **A#** | **Activity Detail** |
| Unit 1.1 Sources | 1 |  |
| Unit 1.1 Sources | 2 |  |

**Module 2**

|  |  |  |
| --- | --- | --- |
| **Unit** | **A#** | **Activity Detail** |
|  |  |  |
|  |  |  |
|  |  |  |

### 4.2.6 A plan curriculum for a such interdisciplinary training to be adapted in each partner country

In this section, we briefly outline the methodology, which was used to develop the training and the corresponding lectures.

Figure 1: Methodology

Based on the results (i.e. desk research, interviews, …) of the previous work packages, an in-depth analysis of the target group is performed. An output of this step are personas, which are representative for the corresponding target group.

Derived from the personas high level competences are elaborated. This way it is ensured that the developed modules and lectures are aligned with the identified training needs.

The next step in the process is dedicated to the determination of modules, which combine thematically matching courses. Beside high-level learning outcomes and content the module descriptions include additional information, such as workload information or recommended literature.

Starting from the modules, the individual lectures are planned in detail. For the description of the lectures, the following worksheet is used:

Table 1: Lecture description

|  |  |
| --- | --- |
| Lecture description | |
| Title of lecture |  |
| Prerequisites |  |
| Workload in ECTS |  |
| Position |  |
| Teaching methods |  |
| Examination |  |
| Learning outcomes |  |
| Learning content |  |
| Recommended Reading |  |

The next step in the process is the content creation according to lecture description. Depending on the teaching methods used, this can include videos, assignments, quizzes, …

The last step is the implementation and roll-out of the content. This also includes the evaluation of the learning packages.

**Current status**

Since the start of the project, the training requirements for SMEs have been identified, which lead to two main target groups, i.e. manager of SMEs and employees of SMEs. Starting with these two groups, we created high-level competence statements based on the Bloom taxonomy, which are further used to refine the structure of lectures and content:

* Manager
  + The participants are able to create and perform information security risk analyses to identify and assess risks. Furthermore, they can decide on actions to treat risks.
  + The participants know common vulnerabilities and threats.
  + The participants know basic structures, considerations and good practices of security management systems. Participants can define and monitor information security requirements.
* Employee
  + The participants possess the ability to behave in a secure manner (e.g. create strong password, identify phishing mails, update software and operating systems)
  + The participants know about actual threats in their working environment and are able to react on incidents.

Derived from the high-level learning objectives / competence profiles we decided to create to individual modules for both target groups.

|  |  |
| --- | --- |
| Module: Information Security for Managers | |
| Prerequisites | Leadership skills |
| Workload in ECTS | 15 |
| High-level learning outcomes | The participants are able to create and perform information security risk analyses to identify and assess risks. Furthermore, they can decide on actions to treat risks.  The participants know common vulnerabilities and threats.  The participants know basic structures, considerations and good practices of security management systems. Participants can define and monitor information security requirements. |
| High-level learning content | Standards and Best Practices in Information Security Management (ISO 2700x, COBIT, …)  Risk and Resilience Management  Third Party Security / Supplier Security |
| Recommended Reading | W. Easttom: Computer Security Fundamentals, Pearson, 2016  International Organization for Standardization, “ISO/IEC 270xx series,” ISO.  A. Shostack: Threat Modeling: Designing for Security, Wiley 2014  Bundesamt für Sicherheit in der Informationstechnik (BSI), “IT-Grundschutz-  Standards.” |

|  |  |
| --- | --- |
| Module: Information Security for Employees | |
| Prerequisites | None |
| Workload in ECTS | 15 |
| High-level learning outcomes | The participants possess the ability to behave in a secure manner (e.g. create strong password, identify phishing mails, update software and operating systems)  The participants know about actual threats in their working environment and are able to react on incidents. |
| High-level learning content | Security at business trips  Secure password practices  Social Engineering / SPAM / Phishing  Security and Privacy in Social Networks  Malware  Cryptography Fundamentals |
| Recommended Reading | Standards and Best Practices in Information Security Management (ISO 2700x, COBIT, …)  J. Katz, Y. Lindell: Introduction to Modern Cryptography, Taylor & Francis, 2014  Australian Cyber  Security. Step-by-step guides, <https://www.cyber.gov.au/acsc/individuals-and-families/step-by-step-guides> |

### 4.2.7 Mentor handbook

**Introduction**

The purpose of the InCyT project is to develop a cybersecurity competency framework that companies can use to describe and improve competencies and skills in order to develop a company's cybersecurity strategy and avoid cyber-attacks and VET to improve their education plans. Furthermore, digitally supported interdisciplinary learning programs and a mentoring one for SMEs employees, a digital platform for learning and cooperation for them, an adapted version for VET and a European transferability model will be developed and tested.

**Learning methods**

**Learning pathway**

The InCyT training programme, is structured across two modules, where each module consists of a number of units.

* Module 1
* Module 2

**Course schedule**

The course schedule begins with an induction webinar, followed by the deployment of each module, where each module takes place over a 7-week schedule.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Module | Module Week | Learning Unit | Learning Activities | Assignments |
| Induction | Week 0 | Induction webinar |  |  |
|  |  |  |  |  |

**Delivering the programme**

The first weeks should be dedicated to getting learners comfortable with the programme, the platform and collaborating online. If learners are not participating, they should be notified of the consequences (this should be detailed in the rules outlined in the induction week and referred to).

Each week the mentor should hold a short briefing of learners of what is required from them for that week (approx. 20 mins). This should be held online and should cover the following:

* What learning material they must cover for the week and a short summary of it
* What tasks they must complete for the week
* What assignment work needs to be completed

The mentor should monitor the forums and answer learner queries ASAP. For all of the activities the mentor should ensure that all learners are participating. If learners are not actively participating the mentor should contact the learner to identify the reason why this might be happening and try to resolve any issues.

**Learner induction**

A learner induction session should be held place prior to the commencement of the programme. All learners should be notified of the date of the induction. It should cover the following topics:

* Overview of programme
* Demonstration of the Moodle platform
* Overview of schedule
* Overview of Assignments/Activities
* Expectations of learners during the programme (e.g. participation in online activities)
* Mentor name and contact details

Each learner should receive a copy of the course schedule for the programme and it should be made publicly available for all to refer to on the Moodle platform.

**Assignments**

Assessment of each module is based on Mentor Marked Assignments. Feedback on assignments should be provided within two weeks of the submission/deadline date.

**Learning activities**

Learning activities occur throughout each of the modules to support learning, an outline of these activities by module is provided hereunder

### 4.2.8 A short plan and adapted methodology for a special interdisciplinary course in VET and an European Methodology

**Background information**

This Intellectual Output will develop a transferability model to allow the described skills to be transferred to a wider number of SMEs and adopted by VETs. This methodology can be used as a VET tool built on a such content to generate an effective achievement of knowledge and skills on cyber security substance for the benefit of the InCyT final target groups of beneficiaries.

**Purpose**

The VET methodology purpose is focused on a SMART knowledge and skills Cyber Security content to be achieved by the InCyT project beneficiaries. The VET methodology has to guide the InCyT project results towards accomplishment of the project specific objectives and to ensure that the project results are utilised fully in a variety of VETs and sectors and to raise awareness of the outputs of the project and recommend how they can be applied to other programs of different education organisations.

**Tasks**

The main objective of this Intellectual Output is to ensure that the project results can be used in the future by other education organisations. The main target of this Intellectual Output will be a report describing the process, results of the course developed and recommendations for the transferability of the course.

For the report building, the following tasks will be developed:

1. Surveys and interviews;
2. Analysis of existing entrepreneurship programs;
3. Elaboration of recommendations for the transferability;
4. Drafting of the Report
5. Peer review;
6. Completion and publication of the Report.

Other tasks developed and included in previous intellectual outputs will also be included in the IO5. In particular, the data analysis of IO4 will be especially relevant to be included in the IO5 Report and the results of survey to students developed after the course in IO4 will also be taken into account, together with the interviews to other target groups (which will be effectively developed in IO5).

**Task 1: Surveys and interviews**

This task has to analyse how the SMEs sector of each partner country adopted a specific development program to identify potential training programs to be implemented by the pilot courses developed and transnationally transferred along with the InCyT project life.

The results of these surveys will be especially useful as a complement of the conclusions and results of the data analysis developed in IO4.

The project partners will develop specific surveys which may be deployed as online surveys/ desk surveys, interviews and the personal and company details of all participants responding to the survey or interview will be treated anonymously or in person:

1. A first survey (survey Mentor) will be addressed to the mentors who participated in the project. This survey will also identify potential improvements and application of the course, from the mentors’ point of view. It will also include questions on the potential replicability and transference to other existing programs.

2. A second survey (survey VET) will be addressed to VET providers who did not participate in the pilot course. For this second group, a summary of the pilot course and results will be provided, together with questions aiming to raise opinions of potential programs where the pilot course modules or the ICT platform could contribute or be transferred. At least 3 VET providers per country to be interviewed.

3. Each partner will conduct a survey/ online meeting with the at least 3 SMEs whose employees have successfully completed the course (Survey SME) regarding how the program suits for the needs of their sectors.

The conclusions from the Learner Experience & Satisfaction Questionnaire (Survey Learner) will be included in this process to be analysed along with these three surveys. The results will be analysed, summarised and reported in a joint document, constituting an important base to develop the recommendations for the transference of the course.

Template for surveys in ANNEX1

**Task 2: Analysis of existing entrepreneurship programs**

The objective is to analyse existing entrepreneurship programs or other education courses to which the modules or the ICT platform piloted in IO4 could be transferred.

Based on the responses of the survey to VET providers from each partner country (survey VET), the partners will examine the potential entrepreneurship programs or any other education course where the modules and ICT tool developed in the project could be transferred (at least 3 programs in each country must be targeted), using a qualitative methodology of evaluating entrepreneurship programs (content analysis of programs and structured interviews).

Each partner will elaborate a list of the potential programs to target and stakeholders to which it would be necessary to contact in order to inform, at a later stage, details of the pilot course tested and its transferability potential for future implementation.

Template in ANNEX2

**Task 3: Elaboration of recommendations for the transferability**

Based on all the previous activities, this task aims to provide a series of recommendations on how to integrate the modules into entrepreneurship VET programs.

Each partner will elaborate a provisional list of recommendations based on all the previous analysis and conclusions from the surveys and interviews maintained with each target group.

**Task 4: Drafting of the Report**

The draft report to be developed will include InCyT project information, info about the platform and main indicators evaluated, a summary of VET systems and potential programmes to which the course could be transferred in each country and the recommendations for its transferability.

All the contributions from the previous tasks in IO5 will be compiled and integrated into the report, but also previous tasks in other Intellectual Outputs will be included, although they have not been replicated in IO5 tasks to avoid duplication of effort.

The Report contents are included in Annex 4.

**Task 5: Peer review**

Each partner will share the draft report with stakeholders (e.g. VET experts, Education Policymakers) in their region or country in order to obtain feedback and contributions that may eventually improve the report. The partners will exchange the conclusions of this peer review for the finalisation of the Report.

**Task 6: Completion and publication of the Report**

The partners will integrate the contributions by the consulted experts and stakeholders, resulting in the definitive Report document which will be published and delivered to main project stakeholders by direct communication and dissemination project tools used for.

**Key metrics of success for Task 1, 2, ….6**

for Task 1: Surveys and interviews

* Online surveys/interviews with SMEs / students who participated in the course (IO4), Online interviews with the mentors who participated in the course in the different countries, Online interviews with other VET providers who did not participate in the course but may support to identify programs to potentially transfer the project outcomes

for Task 2: Analysis of existing entrepreneurship programs

* Entrepreneurship programs identified where modules and ICT platform could be transferred and implemented, Stakeholders within entrepreneurship programs identified

for Task 3: Recommendations for the transferability report

* A number of recommendations to transfer InCyT course, modules and ICT platform to other existing entrepreneurship programs or additional education courses for

For Task 4: Draft Report

* A draft version of the Report ,

for Task 5: Peer reviews

* A series of contributions and amendments suggested by experts

for Task 6: Completion and publication of the Report ‘

* the Report ‘Integrating practical research skills into entrepreneurship education’ publication

**Outputs**

1. Work package methodology developed,
2. A number of surveys and interviews completed and reported,
3. A list of entrepreneurship programs identified for potential transfer of InCyT outcomes,
4. List of recommendations on how to integrate InCyT modules into sector specific VET programs,
5. Report

# References

European Commission (2018). Digital Education Action Plan. <https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_enin>.

European Commission (2018b). The Digital Skills and Jobs Coalition. In: *Publications Office of the European Union, Luxembourg*, <https://ec.europa.eu/digital-single-market/en/digital-skillsjobs-coalition>.

Elliott C., Mavriplis C. & Anis H. (2020). An entrepreneurship education and peer mentoring program for women in STEM: Mentors' experiences and perceptions of entrepreneurial self-efficacy and intent. *The International Entrepreneurship and Management Journal* 16 (1), pp. 43–67.

Golding C.(2009). *Integrating the disciplines: Successful interdisciplinary subjects. The centre for the study of higher education.*  The University of Melbourne.

Hamburg, I. (2020a). Interdisciplinarity, e-Mentoring and support of entrepreneurial research skills. In: *Advances in social sciences research journal 7, no. 4*, p. 298-309.

Hamburg I. (2020b).Creating innovative structures in workplace and vocational digital learning to ensure social distancing, ICDS 2020: The fourteenth international conference on digital society 3. 124-127. *Journal of Higher Education*, 78 (2), p.215-237.

Hamburg, I. (2021). Approaches to support learning in today ́s workplace. In: *VI International Scientific Conference Winter Session: Industry 4.0.* 8-11 December 2021, Borovets, Bulgaria, p. 284-288.

Kaundert, M., Ziegler, L., Pahi, T., Skopik, F., Leitner, M., Kieseberg, P., Schwanzer, B. & Kojo Ampia-Addison, J., (2018). Evaluierung des Cyber Lagebildkonzepts im praktischen Einsatz. In *Cyber Situational Awareness in Public-Private-Partnerships* (pp. 293-344). Springer Vieweg, Berlin, Heidelberg.

Klaassen, R. (2018). Interdisciplinary education: a case study” *European Journal of Engineering Educa* *Kram, K. (1985). Mentoring at Work. Glenview, IL: Scott, Foresman.*

Kolb, D & Fry, R.E. (1974). Toward an applied theory of experiential learning. *MIT Alfred P. Sloan School of Management*

Leeser, Daniel Christian (2020). Digitalisierung in KMU kompakt: Compliance und IT-Security (IT kompakt). Springer Vieweg.

Ragins, B. & Kram, K. (2007). *The Handbook of Mentoring at Work*. Thousand Oaks, CA: Sage.

OECD (2021):The Digital Transformation of SMEs. URL: https://www.oecd-ilibrary.org/sites/bdb9256a-en/1/3/2/index.html?itemId=/content/publication/bdb9256a-en&\_csp\_=42ee43b7fa49ef116a6caf8c78b53d84&itemIGO=oecd&itemContentType=book, (14.03.2022).

1. [↑](#endnote-ref-1)
2. [↑](#endnote-ref-2)
3. [↑](#endnote-ref-3)
4. [↑](#endnote-ref-4)