Deliverable D.T.4.3.1 . - Curriculum on EQF level 5 in English

Curriculum “IT security Specialist” (working version)

This curriculum is for continuing training for IT specialists on IT security field.

Name of the curriculum	**ICT Security Specialist**
Amount	30 ECTS
Aim and outcomes of the curriculum	• *recognise the basics of information security management* • *apply the processes ensuring IT systems security and participate in the design and development of those processes* • *establish and maintain positive business relationships between stakeholders deploying and complying with organizational processes* • *manage IT systems in a secure manner and participate in the design and development of those systems*
Modules	1. Information Security Management - 5 ECTS (HBC) 2. Business Continuity Management - 5ECTS (TPT) 3. Customer Service / Service Delivery - 5ECTS (TPT) 4. Securing IT Solutions - 15ECTS (RTC)
Requirements to start the study	Person who have EQF level 4 “IT specialist” qualification competencies
Requirements to complete the study	*Documentation and project outcomes that meet the given criteria.*

Implementation plan of Module 1:

No	**Module name**			**Amount**
1	Information Security Management			**5 ECTS**
Aim: to form a managerial level of understanding of information security and to align information security with business strategy and ICT strategy.				
Requirements to start the module:				
Outcomes	**Assessment criteria**	**Study methods**	**Assessment methods and tasks**	**Subject (themes, issues, topics)**
1. gives input to development of organisation's information strategy	• Explains the role of information from the strategic viewpoint. • Explains strategic alignment between business and ICT strategic convergence • Describes ecosystem cyber securityh	Lectures Project / Case work Presentation	Project work and documentation: "Improvement project of ICT Security policies"	• Information management • Information security management • Safety modelling • ecosystem cyber security • strategic alignment
2. implements organisation's information strategy	• Knows strategic threat modelling and understands competitive advantage of information • Uses safety modelling.	Lectures Project / Case work Presentation	Project work and documentation: "Strategic alignment of cyber security, ICT and business"	• strategic alignment • strategic convergence • strategic threat modelling and competitive advantage on information
3. Monitors and takes action against intrusion, fraud and security breaches or leaks.	• Explains roles & stakeholders in information technology. • Can do vulnerability and threat assessment as part of business impact analysis.	Lectures Lab Project/ Case work Presentation	Project work and documentation: implementation and testing of vulnerability. Documentation on data management plans & data classification	• Roles in information technology • Vulnerability assessment • Data management • Threat assessment • Risk assessment

	• Explains how data is to be managed in the organization according to its security documentation. • Can do information security audit			• CIA triad-confidentiality, integrity, and availability • Information security audit •
4. Follows best practices and standards in everyday work.	• Explains best practices of IT management by using some well-known framework (e.g. ITIL) • Explains Information security management standards (e.g. ISO/IEC 27001/27002) • Follows organization's documented best practices and standards in everyday work. • Follows local and international law in everyday work.	Lectures Project / Case work Presentation	Project work and documentation: Improve processes and procedures based on ISO/IEC 27001/27002.	• ITIL framework • ISO/IEC 27001/27002 • Local and international law
Evaluation of module:	During the module students work in teams with different kind of documentation which describes policies, procedures and processes in a given organization. The student understands the relation between organization/company strategy and the strategic role of information. Teams have to implement information security policies and can monitor and take actions against all types of security breaches. Teams have to prepare business continuity and disaster recovery actions. The evaluation is based on the documentation and lab work outcomes that are presented. Grading of this module is non-distinctive, student will pass the module if all assessment criteria are fulfilled the minimum required level.			

Teaching materials:	

Implementation plan of Module 2:

No	**Module name**			**Amount**
2	**Business Continuity Management**			**5 ECTS**
Aim:	The module is designed to give student overview change management, configuration management and business continuity management. The Student understand why configurations and changes need to be managed to ensure secure IT operations.			
Requirements to start the module:				
Outcomes	**Assessment criteria**	**Study methods**	**Assessment methods and tasks**	**Subject (themes, issues, topics)**
1. ensures efficient control and scheduling of software or hardware modifications	• Documents all activities during installation and records deviations and remedial activities • Analyses the impact of functional and technical changes	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Project work and documentation: "Planning hardware and software changes"	• Configuration Management • Service Asset and Configuration Management
2. minimizes service disruption as a consequence of changes	• Complies with appropriate security standards and change control procedures to maintain integrity of the overall system functionality and reliability • Prepares Change Request if needed • Gives input to development of change management process	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Project work and documentation: "Implementing hardware and software changes"	• Change management
3. identifies and escalates potential service level	• verifies that integrated systems capabilities and	Lectures Reading	Project work and documentation:	• Capacity management

failures and security risks	efficiency match specifications • monitors security controls • analyses the company critical assets and identify threats, weaknesses and vulnerability to intrusion or attack	Discussion in group Lab Project/ Case work Presentation	"Vulnerability assessment"	• Vulnerability management
4. ensures that security risks are analyzed and managed with respect to enterprise data and information	• conducts risk management audits and act to minimise exposures • creating or improves risk management plan to identify required preventative actions	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Project work and documentation: "Risk management"	• Risk management
5. manages business continuity and disaster recovery plans	• participates in creating and management processes of disaster recovery business continuity plans • validates disaster recovery plan to ensure that this is up to date and reflects reality •	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Project work and documentation: Business continuity plan and disaster recovery plan	• Disaster recovery plan • Business continuity plan • Planning process
Evaluation of module:	During the module student's work in teams with different kind of projects which are related with configuration management, change management and business continuity management. The student understands the relation between reliability of organization/company services and need to ensure that all changes are well documented. Teams have to prepare real configuration management database, change management solution and create and test disaster recovery plan.			

	Grading of this module is non-distinctive, student will pass the module if all assessment criteria are fulfilled the minimum required level.
Teaching materials:	

Implementation plan of Module 3:

No	**Module name**			**Amount**
3	**Service Delivery**			**5ECTS**
Aim:	The module is designed to give student overview of service delivery process. Main focus of this module are incident management, problem management and customer support.			
Requirements to start the module:				
Outcomes	**Assessment criteria**	**Study methods**	**Assessment methods and tasks**	**Subject (themes, issues, topics)**
1. responds to user requests and issues by recording relevant information and assures resolution or escalates incidents	• deploys support tools to systematically trace source of error or technical failure • analyse symptoms to identify broad area of user error or technical failure • escalates complex or unresolved incidents	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Discussion: "What is incident, problem and failure?" Project work and documentation: "Incident management in an IT organization"	• Incident management • Customer management
2. identifies and resolves the root cause of incidents	• identifies and classifies incident types and service interruptions • identifies potential critical component failures and take action to mitigate effects of failure	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Project work and documentation: "Finding root causes of incidents"	• Incident classification • Problem management
3. determines documentation requirements taking	• keeps documentation aligned to the solution during the entire lifecycle	Lectures Reading Discussion in group	Project work and documentation: "Building	• Document management

into account the purpose and environment to which it applies	• keeps up-to date organization security documentations	Lab Project/ Case work Presentation	a knowledge base for an organization"	• Document management systems • Knowledge management systems
4. ensures that stakeholder needs, concerns or complaints are understood and addressed in accordance with organizational policy	• understands customer needs • communicates security requirements to other departments • explains the needs for security operations	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Role play: "Communication with a end-user" Project work and documentation: "Building a communication framework for security related announcements"	• Customer support • Communication management
5. Tracks reliability and performance data against SLA	• maintains monitoring and management tools • analyse service delivery provision and report outcomes to senior colleagues	Lectures Reading Discussion in group Lab Project/ Case work Presentation	Project work and documentation: "Application Performance Management"	• Systems monitoring • Security measures management • Service delivery management
Evaluation of module:	During the module student's work in teams with different kind of projects which are related with incident management, problem management and customer support. The student understands the relation between organization/company services and need for good customer support, the student understands need to document incidents and problems. The Student can explain the needs for security operations. Teams have to prepare real incident management solution which need to be supported by knowledge management system to help reduce the workload of customer support. Grading of this module is non-distinctive, student will pass the module if all assessment criteria are fulfilled the minimum required level.			
Teaching materials:				

Implementation plan of Module 4:

No	Module name	Amount
4	**Securing IT solutions**	**15 ECTS**
Aim:	The module is designed to teach and practically train students in IT solution security. This involves secure computer network solutions; server, workstation and mobile device security; disaster recovery and cloud computing solutions security.	
Requirements to start the module:	EQF level 4 qualification competences in ICT field (e.g. Computer systems technician).	

Outcomes	**Assessment criteria**	**Study methods**	**Assessment methods and tasks**	**Subject (themes, issues, topics)**
1. Implements secure computer network solutions	• Describes potential types of attacks targeted to network solutions • Knows basic cryptographic techniques • Implements cryptographic techniques, algorithms and applications in computer networks. • Implements hardware and software solutions to mitigate OSI mechanism's and computer network vulnerabilities • Ensures protection of wireless networks with "encryption" and "password" systems • Encrypts network connections where it is necessary	Lecture Discussion in group Practice Video Lecture Reading Presentation	• Practical work in teams: "Security solutions of the OSI model layers" • Test: "Security of the OSI model" • Presentation: "Types of attacks to wireless networks" • Test: "Types of attacks to computer networks" • Practical work: "Advantages and vulnerabilities in the given computer network diagram." • Presentation: "Protection of various network equipment against unauthorised access" • Practical work: "Securing network devices"	• Design principles of the OSI model. • Most important problems related to security of the OSI model. • Protection from attacks that exploit OSI mechanism's vulnerabilities. • IP and MAC filters, IP addressing, security. • Security of wireless networks. • Protection against attacks to computer networks and telecommunication systems. • Basic cryptographic techniques.Types of encryption, their use in design of a secure connection.

	• Monitors operation of a computer network by use of various applications.		• Practical work: "Securing network solution"	• Classification of attacks on computer network.
2. Manages workstations and mobile devices in a secure manner	• Manages workstations using domain controller solutions • Lockdowns workstations to ensure their security • Implements domain security policies and divides workstations into security groups • Implements synchronisation, data security in various mobile devices and workstations.	Lecture Project work Reading Presentation	• Test – "Workstation security – client side" • Practical work - "Hardening workstations" • Practical work - "Mobile device security"	• Workstation lockdown solutions. • Central management of workstations • User – based security. • Mobile device security.
3. Applies security policies to ensure server security	• Configures firewall for server security • Ensures DNS and DHCP server protection. • Securing e-mail and web servers • Manages VPN policy. • Implements AAA model – Authentication, Authorisation, Accounting. • Implements disk encryption on server	Lecture Project work Reading Presentation	• Practical work: "Group policy" • Practical work: "DHCP and DNS protection" • Practical work: "Securing e-mail server" • Practical work: "Securing web server" • Test - "Firewall and VPN policy" • Practical work: "AAA implementation and security in directory service " • Practical work: "Secure remote access of serverg"	• Firewall configuration for server security. • DNS and DHCP – possible security issues and their solutions. • Securing web servers • VPN – configuration and policy. • Securing email and web servers • Authentication, Authorisation and accounting by using directory services. • Disk encryption solution in enterprise network. • Secure remote access of server

4. uses cloud solutions in secure manner	• Understands use of cloud computing technologies in protection of data transmission. • Understands connection security of cloud computing service providers. • Is able to cooperate with cloud computing service providers.	Lecture Video Lecture Presentation	• Team work: "Protection of connection of cloud computing service providers" • Practical task: “Using cloud computing to secure IT system”	• Cloud computing technologies. • Cloud computing service providers and types of services. • Connection security of cloud computing service.
5. Implements disaster recovery and backup solutions	• Configures file backup service. • Automates backup file storing in local or global network. • Protects backup servers from unauthorised use. • Is able to test and restore created backup	Lecture Video Lecture Reading Presentation	• Practical task: "Making backup files and storage of backup files" • Practical task: "Ensuring backup of network equipment configuration" • Practical task: "Protection of backup files" • Practical task: "Restoring backup" • Practical task: " backup restoration testing"	• Backup solutions and types of file backups. • Backup automation. • Protection of backup solutions. • Backup equipment monitoring. • Disaster recovery – restoration of backups. • Testing backup solution
Evaluation of module:	The evaluation of module is based on overall performance in each assessment task. Student is able to secure and manage IT solutions in an enterprise (workstations, servers, cloud computing solutions, network infrastructure) as well as implement and protect IT disaster recovery solutions. Grading of this module is non-distinctive, student will pass the module if all assessment criteria are fulfilled the minimum required level.			
Teaching materials:				

Comparison of occupational standard competences and modules of curriculum

Modules/competences	B.2.1 **ICT Solution Design**	B.2.2 **Technology Trend Monitoring**	B.2.3 **Component Integration**	B.2.4 **Testing**	B.2.5 **Solution Deployment**	B.2.6 **Documentation Production**	B.2.7 **User Support**	B.2.8 **Change Support**	B.2.9 **Service Delivery**	B.2.10 **Problem Management**	B.2.11 **Information Security Strategy Development**	B.2.12 **Personnel Development**	B.2.13 **Risk Management**	B.2.14 **Relationship Management**	B.2.15 **Information Security Management**
Information Security Management (1)		X				X		X			X	X	X	X	X
Business Continuity Management (2)		X				X		X	X	X				X	X
Customer Service / Service Delivery (3)		X				X	X							X	
Securing IT Solutions (4)	X	X	X	X	X	X	X		X			X	X	X	