



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

**Establishing Modern Master-level Studies in Information Systems**  
**561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP**

**WP2**  
**Curriculum development**  
**IT Security**

**Tabl. 1**

**List of Competences**

<b>Competences Area</b>	<b>Competences</b>
<b>Systems Development and Deployment</b>	1. Managing plan-based, hybrid, and agile development approaches
	2. Specifying and documenting systems requirements
	3. Managing IS development projects
<b>Data, Information and Content Management</b>	4. Selecting appropriate data management technologies based on the needs of the domain
	5. Integrating and preparing data captured from various sources for analytical use
	6. Selecting and using appropriate analytics methods
<b>Innovation, Organizational Change and Entrepreneurship</b>	7. Developing a business plan
	8. Understanding how to apply creative problem solving to technology-related issues
<b>IS Strategy and Governance</b>	9. Engaging in IS strategic planning
	10. Planning and implementing IS governance
<b>Enterprise Architecture</b>	11. Understanding enterprise architecture principles and the value it provides to business
	12. Communicating and deploying an EA
<b>Business Continuity and Information Assurance</b>	13. Implementing and managing quality audit processes
	14. Managing Information Systems risks
<b>IS Management and Operations</b>	15. Managing IS/IT projects and programs
<b>IT Infrastructure</b>	16. Monitoring emerging technologies to understand their potential to support the domain

**Tabl. 2**

**List of Programme learning Outcomes**

No	Professional Learning Outcomes	P
1.	to understand essential concepts, facts, principles, and theories of information system	P1
2.	to understand the diversity and state-of-the-art in area of information system	P2
3.	to be able to analyse, model, and evaluate organization's business processes from the perspective of information systems development	P3
4.	to be able to apply various methods of information systems analysis	P4
5.	to understand problems of users of information systems, to be able to identify, analyse and specify user requirements	P5
6.	to be able to manage information systems development projects and identify, analyse, evaluate, and solve the arising management problems	P6
7.	to be able to identify, analyse, and understand unorthodox problems of information systems development	P7
8.	to be able to apply various methods of information systems design	P8
9.	to be able to apply methods of knowledge, metadata analysis and information safety engineering	P9
10.	to be able to identify, find and evaluate information relevant to information systems by using data bases and other sources of information	P10
11.	to be able to apply various computerized tools for model driven information systems analysis and design	P11
12.	to be able to choose and apply various technologies of information systems' development	P12
13.	to be able to apply various tools for management of information systems projects	P13
14.	to be able to develop innovative decisions for IT business creation and support	P14
<b>Personal and Social Learning Outcomes</b>		
15.	to be able to think systematically when analysing different situations, solving problems and tasks	PS1
16.	to be able to apply the acquired knowledge creatively	PS2
17.	to be able to work individually with minimum guidance, manage one's work and time	PS3
18.	to be able to work efficiently in a group, manage the team, and act collectively	PS4
19.	to be able to understand the impact of information systems solutions on the society and environment and their economic aspects	PS5

## CourseDescriptors

<b>Course title:</b>	<b>IT Security</b>
<b>Course unit code</b>	ITS
<b>Course Program:</b>	MPIS
<b>University delivering the course:</b>	(UDG)
<b>Type of course unit</b>	Core course
<b>Level of course unit</b>	Masters level
<b>Number of ECTS credits allocated</b>	5 Credits (150 hours of student work)
<b>Teaching Methods</b>	lectures, case study,presentations, Independent study.

## ModuleStructure:

No	Type	Course	CP (h)	In class (h)	Independent study (h)
1	Course	IT Security	150	60	90

## RelevantWork:

Number and Type; Connection to Course	Part of final grade in %
Class participation (minimum 5 class presentations and case studies)	20
Project	40
Written exam	40

**Tabl.3**

**Correlation matrix of Competences and Programme learning Outcomes**

Competencies/ Learning Outcomes	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	PS1	PS2	PS3	PS4	PS5
1. Managing plan-based, hybrid, and agile development approaches	X	X						X		X	X	X	X	X	X	X	X	X	X
2. Specifying and documenting systems requirements	X	X			X					X					X	X	X	X	X
3. Managing IS development projects					X			X		X	X	X	X		X	X	X	X	X
4. Selecting appropriate data management technologies based on the needs of the domain	X	X							X	X	X	X			X	X	X	X	X
5. Integrating and preparing data captured from various sources for analytical use	X	X							X	X	X	X			X	X	X	X	X
6. Selecting and using appropriate analytics methods	X	X	X				X		X	X	X				X	X	X	X	X
7. Developing a business plan	X	X					X			X	X			X	X	X	X	X	X
8. Understanding how to apply creative problem solving to technology-related issues	X	X					X			X	X			X	X	X	X	X	X
9. Engaging in IS strategic planning	X	X	X			X				X	X			X	X	X	X	X	X

Establishing Modern Master-level Studies in Information Systems  
561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

Competencies/ Learning Outcomes	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	PS1	PS2	PS3	PS4	PS5
10. Planning and implementing IS governance	X	X				X				X	X		X	X	X	X	X	X	X
11. Understanding enterprise architecture principles and the value it provides to business	X		X	X						X					X	X	X	X	X
12. Communicating and deploying an EA	X		X							X	X				X	X	X	X	X
13. Implementing and managing quality audit processes	X		X	X			X		X	X					X	X	X	X	X
14. Managing Information Systems risks	X		X	X		X	X		X	X	X				X	X	X	X	X
15. Managing IS/IT projects and programs	X				X	X				X	X	X	X		X	X	X	X	X
16. Monitoring emerging technologies to understand their potential to support the domain	X			X			X			X					X	X	X	X	X

**Tabl.4**

**Correlation matrix of Programme Learning Outcomes and Courses**

Programme Learning Outcomes	Courses
	IT Security
1	10
to understand essential concepts, facts, principles, and theories of information system	X
to understand the diversity and state-of-the-art in area of information system	
to be able to analyse, model, and evaluate organization's business processes from the perspective of information systems development	X
to be able to apply various methods of information systems analysis	
to understand problems of users of information systems, to be able to identify, analyse and specify user requirements	X
to be able to manage information systems development projects and identify, analyse, evaluate, and solve the arising management problems	
to be able to identify, analyse, and understand unorthodox problems of information systems development	
to be able to apply various methods of information systems design	
to be able to apply methods of knowledge, metadata analysis and information safety engineering	X
to be able to identify, find and evaluate information relevant to information systems by using data bases and other sources of information	
to be able to apply various computerized tools for model driven information systems analysis and design	
to be able to choose and apply various technologies of information systems' development	
to be able to apply various tools for management of information systems projects	
to be able to develop innovative decisions for IT business creation and support	

Establishing Modern Master-level Studies in Information Systems

561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

to be able to think systematically when analysing different situations, solving problems and tasks	X
to be able to apply the acquired knowledge creatively	
to be able to work individually with minimum guidance, manage one's work and time	X
to be able to work efficiently in a group, manage the team, and act collectively	
to be able to understand the impact of information systems solutions on the society and environment and their economic aspects	X



**Tabl.5**

**List of Course Learning Outcome (IT Security (ITS))**

<b>Code of Learning Outcomes</b>	<b>Course Learning Outcomes</b>
ITS1	To be able to identify appropriate strategies to assure confidentiality, integrity, and availability of information
ITS2	To be able to identify the role of information systems security (ISS) policy framework
ITS3	To be able to apply current/common cryptographic technologies and controls for authentication and encryption
ITS4	To be able to apply and operationalize network security technologies and techniques
ITS5	To be able to evaluate and justify security technology selections and designs
ITS6	To be able to provide contingency operations including administrative planning processes for incident response, disaster recovery, and business continuity within information security
ITS7	To be able to analyze social, legal and ethical issues represented by information technology environments
ITS8	To be able to argue, justify and present their decision and plans
ITS9	To be able to make decision and take responsibility for them

**Tabl.6**

**Correlation matrix of Programme Learning Outcomes and Fundamentals of IT Security (FITS)  
 Course Learning Outcomes**

<b>Programme Learning Outcomes</b>	<b>Course Learning Outcomes</b>	<b>Code</b>
<b>1</b>	<b>2</b>	<b>3</b>
<b>P1. To understand essential concepts, facts, principles, and theories of information system</b>	To be able to identify appropriate strategies to assure confidentiality, integrity, and availability of information	ITS1
<b>P3. To be able to analyse, model, and evaluate organization's business processes from the perspective of information systems development</b>	To be able to identify the role of information systems security (ISS) policy framework	ITS2
	To be able to provide contingency operations including administrative planning process for incident response, disaster recovery, and business continuity planning within information security	ITS6
<b>P5. To understand problems of users of information systems, to be able to identify, analyse and specify user requirements</b>	To be able to identify the role of an information systems security (ISS) policy framework	ITS2
	To be able to provide contingency operations that include administrative planning process for incident response, disaster recovery, and business	ITS6

	continuity planning within information security	
<b>P9. To be able to apply methods of knowledge, metadata analysis and information safety engineering</b>	To be able to apply current/common cryptographic technologies and controls for authentication and encryption	ITS3
	To be able to provide contingency operations including administrative planning process for incident response, disaster recovery, and business continuity within information security	ITS6
	To be able to apply and operationalize network security technologies and techniques	ITS4
<b>PS1. To be able to think systematically when analysing different situations, solving problems and tasks</b>	To be able to evaluate and justify security technology selections and designs	ITS5
<b>PS3. To be able to work individually with minimum guidance, manage one's work and time</b>	To be able to identify the role of information systems security (ISS) policy framework	ITS2
	To be able to argue, justify and present their decision and plans	ITS8
<b>PS5. to be able to understand the impact of information systems solutions on the society and environment and their economic aspects</b>	To be able to analyze social, legal and ethical issues represented by information technology environments	ITS7
	To be able to make decision and take responsibility for them	ITS9

**Tabl.7**

**IT Securitycourse Learning Outcomes**

Establishing Modern Master-level Studies in Information Systems  
561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

Themes	<i>Theoretical component</i>	<i>Practical component</i>	<i>Learning Objectives</i>	<i>Learning Outcomes</i>	
				Professional	Transferable Skills
1	2	3	4	5	6
<b>Topic 1.</b>  <b>Identity and Access Management</b>	1.1. Security Principles Identification, Authentication, Authorization and Accountability 1.2. Access Control Models 1.3. Access Control Techniques and Technologies 1.4. Access Control Administration and Monitoring 1.5. Threats to Access Control	Lab work Case studies	To learn: <ul style="list-style-type: none"> <li>- how to use identification methods and technologies;</li> <li>- how to implement authentication methods, models and technologies;</li> <li>- how to manage and monitor with Access Control Administration;</li> <li>- to recognize different threats to Access Control</li> </ul>	ITS1 ITS2	
<b>Topic 2.</b>  <b>Security Frameworks</b>	2.1. Policies, Standards, Baselines, Guidelines and Procedures 2.3. Risk Management 2.4. Threat Modeling 2.5. Risk Management Frameworks	Lab work Case studies	To learn: <ul style="list-style-type: none"> <li>- how to implement security frameworks, models, standards and best practices;</li> <li>- how to model cyber threats;</li> <li>- how to manage with cyber threats;</li> <li>- how to use Risk Management frameworks</li> </ul>	ITS2	ITS8

<p><b>Topic 3. Cryptography definition and concept</b></p>	<p>3.1. Methods of Encryption (Symmetric, Asymmetric) 3.2. Message Integrity 3.3. Public Key Infrastructure 3.4. Attacks on Cryptography</p>	<p>Lab work Case studies Problem based learning</p>	<p>To learn:</p> <ul style="list-style-type: none"> <li>- how to use different types of Encrypting methods;</li> <li>- how to check message integrity using different types of hash algorithms;</li> <li>- and understand structure of Public Key Infrastructure and how to use Digital sign for different purpose;</li> <li>- how to recognize attacks on cryptography</li> </ul>	<p>ITS3</p>	
<p><b>Topic 4. Communication and Network Security</b></p>	<p>4.1. Open system Interconnection 4.2. Reference Model 4.3. TCP/IP Model 4.4. Networking Foundations 4.5. Network devices 4.6. Wireless Networks 4.7. Network Encryption 4.8. Network Attacks</p>	<p>Lab work Problem based learning</p>	<p>To learn:</p> <ul style="list-style-type: none"> <li>- how to identify some of the factors driving the needs for network security;</li> <li>- identify and classify particular examples of network attacks;</li> <li>- how to identify physical points of vulnerability in simple networks;</li> <li>- how to compare and contrast symmetric and asymmetric encryption systems, their vulnerability to attack,</li> </ul>	<p>ITS4</p>	

Establishing Modern Master-level Studies in Information Systems

561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

			and explain the characteristics of hybrid systems		
<b>Topic 5.</b> <b>Software Development Security</b>	5.1. Software Development Models 5.2. Programming Languages and Concepts 5.3. Mobile Code 5.4. Web Security 5.5. Database Management 5.6. Malicious Software	Lab work Case studies	To learn: - security characteristics of different software development models; - security requirements for mobile application; - security requirements for web based application; - security issue of databases; - different malware types, attacks and how to protect IT system from malicious software.	ITS5 ITS6	
<b>Topic 6.</b> <b>Security Operations</b>	6.1. Administrative Management 6.2. Operational Management 6.3. Physical Security 6.4. Preventive Measures 6.5. The Incident Management Process 6.6. Disaster Recovery 6.7. Investigation	Lab work Case studies	- To understand administrative and operational management responsibilities; - To learn how to organize physical security; - To learn how to implement appropriate preventive measures; - To learn how to organize incident management process	ITS6 ITS7	ITS8 ITS9

Establishing Modern Master-level Studies in Information Systems  
561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

			<p>es;</p> <ul style="list-style-type: none"> <li>- To learn how to implement disaster recovery procedures;</li> <li>- To learn how to realize investigation process after cyber-attacks.</li> </ul>		
Topic 7. Asset Security	<p>7.1. Information Life Cycle 7.2. Information Classification 7.3. Layers of Responsibility 7.4. Data Breaches 7.5. Protecting Privacy 7.6. Protecting Assets</p>		<p>To learn:</p> <ul style="list-style-type: none"> <li>- how to manage and protect information according with their classification;</li> <li>- importance of clear definition of layers' responsibilities ;</li> <li>- how to provide privacy and protect assets.</li> </ul>	ITS7	ITS8

**Tabl.8**

**Characteristics of Learning Outcomes for IT Security Course**

Course Learning Outcomes	Code of Learning Outcomes	Knowledge	Skills	Transferable Skills
To be able to identify appropriate strategies to assure confidentiality, integrity, and availability of information.	ITS1	Determine basic principles and objectives of IT security	Analyse principles, methods and concepts of IS Security	
To be able to identify the role of information systems security (ISS) policy framework	ITS2	Define description and requirements of IS Security Management.	Develop requirements for IS security management in accordance with standards and ISS policy framework	
To be able to apply current/common cryptographic technologies and controls for authentication and encryption.	ITS3	Formulate methods of cryptographic technologies for establishing control for encryption and authentication	Contribute to enhancement of research organization's competitiveness using requirements and specifications in strategic planning	
To be able to apply and operationalize network security technologies and techniques.	ITS4	Determine of purpose and tasks for apply and organize enterprise network security	Develop enterprise network security model in accordance with specific security requirements	
To be able to evaluate and justify security technology selections and designs	ITS5	Compare different architectures, methodologies and technologies for IS Security	Use modern technical and software solution to achieve appropriate level of IS security	



Establishing Modern Master-level Studies in Information Systems

561592-EPP-1-2015-1- FR-EPPKA2-CBHE-JP

To be able to provide contingency operations that include administrative planning process for incident response, disaster recovery, and business continuity planning within information security	ITS6	Implement basic operations for incident response and disaster recovery in order to provide business continuity	Analyse principles, methods and concepts of enterprise architecture management in order to provide business continuity	
To be able to Analyze social, legal and ethical issues represented by information technology environments.	ITS7	Define description and requirements of social, legal and ethical issues of IS security.	Develop requirements for enterprise IS security management according to standards including social, legal and ethical issues	
To be able to argue, justify and present their decision and plans	ITS8	Formulate methods of strategic planning enterprise IT Security	Analyse principles, methods and concepts of the strategic planning for enterprise IS security	
To be able to make decision and take responsibility for them	ITS9	Determine of purpose and tasks of stakeholders and impact on enterprise IT Security system	Develop model of decision making architecture for enterprise IT security	

## **Recommended or required reading**

### **Main:**

List of required literature will be provided after consultations with the EU partners

### **Additional:**

CISSP (All in one – Exam guide 7<sup>th</sup> Edition), ISBN-13: 978-0071849272, ISBN-10: 0071849270.

## **Planned learning activities and teaching methods**

- Classes will be integrated with students' direct involvement in teaching activities. Students will be subdivided into groups of 3-5 people and they will be asked to rehearse course content with teaching cases.

- The groups will be also responsible for the development of projects in certain topics

## **Assessment methods, criteria and regime**

- Class participation 20% (participation and presentation of minimum 5 case studies)
- Project 40% (Preparation of the project 70% and its presentation (30%)). The group responsible for the project will get the total grade. Students will distribute the grade among the group members internally.
- Written exam 40%