ÓBUDA UNIVERSITY
JOHN VON NEUMANN FACULTY OF INFORMATICS

Institute of Cyber-physical Systems						
Name of the subject:	Code of the subject:	Credits:	Weekly hours:			
				lec	sem	lab
Information Security and Audit of Financial Institutions	NSTSAVSANK	3	full-time	3	0	0
Responsible person for the subject: Dr. Szenes Katalin			Classification: honorary associate professor			
Subject lecturer(s): Dr. Szenes Katalin, Tureczki Bence						
Prerequisites:	-					
Way of the assessment:	Exam					

Course description	
Goal:	To help our students to be useful employees of the financial institutions or that of other enterprises either in the IT division - development, operations, or in the security, or audit departments, already at starting their career. The most important basics of information security and audit are extended with specialties of financial institutions.
Course description:	Subjects: In order to help our students to begin their work as a useful employee in a financial institution, or in a related enterprise, an overview is given on: • the challenges yielded by the new customers' and legislation requirements in Europe and in Hungary • well-known attacks, advanced persistent threats • requirements to be derived from some of the most important best practice EU and USA methodologies & standards - useful hints in the ISACA (Information Systems Audit and Control Association), NIST (National Institute of Standards and Technology), ISO (International Standards Organization), and other materials • their basic notions - control objectives / measures, their qualifications and use • the 3 pillars of operations • the infrastructure of the information systems, and the security problems of some of the infrastructural elements • secure application development • business continuity planning and IT business continuity planning • special problems, e.g. outsourcing • some of the problems of determining an appropriate structure for the computer network of the institutions

Lecture schedule	
Education week	Topic
1.	the challenges yielded by the new customers' and legislation requirements in Europe (e.g. NIS2 directive, AI proposals), and in Hungary. Issues from the European Central bank, and from the EBF (European Banking Federation), PSD2 (Payment Services Directive)
2.	challenges continued: the US President's Executive Order on Cybersecurity and other NIST requirements
3.	challenges continued: well-known attacks, advanced persistent threats
4.	the strategy-based risk assessment & management
5.	control objectives / preventive – detective - corrective control measures, information criteria, operational and asset handling excellence criteria; practice: CISA exam test questions
6.	control objectives / preventive – detective - corrective control measures, information criteria, operational and asset handling excellence criteria; practice: CISA exam test questions

7.	Business Continuity Management; practice: CISA exam test questions
8.	Hungarian specialities - the changes in the laws on financial institutions. Data privacy - the new EU GDPR (General Data Protection Regulation)
9.	the 3 pillars of the corporate / institution operations: organization, regulation, technics; practice: CISA exam test questions
10.	outsourcing and other current issues
11.	how to build compliant IT structure - organizational, regulational control measures; practice: CISA exam test questions
12.	business continuity planning and management
13.	examples for the relations between the strategic goals – preventive / detective / corrective operational activities – pillars of operations
14.	preparation for the AI challenges in the European Union - Accountability of AI, XAI - Explainable AI

Mid-term requirements	
Conditions for obtaining a mid-term grade/signature	Requirements During Term Attending the lectures, when they are held in the university, is compulsory This, and the completion of every task given by the teacher are necessary conditions for getting a signature Should the fulfillment of any task be omitted, the compensation is to be discussed with the teacher.

Assessment schedule	
Education week	Topic
	Creating an Information Security Procedural Rulebook based on the ISO/IEC 27001
Exam period	Exam: verbal

Method used to calculate the *mid-term grade* (to be filled out only for subjects with mid-term grades)

Type of the replacement	
Type of the replacement of written test/mid-term grade/signature	Replacement Exam

Type of the exam (to be filled out only for subjects with exams)

Verbal

Calculation of the exam mark (to be filled only for subjects with exams)

90-100: points: 5
80-89 points: 4
70-79 points: 3
60-69 points: 2
0-59 points: 1

Final grade calculation methods:

References	
Obligatory:	the presentations International Standard ISO/IEC 27001 Ed. 2013-10-01 Information technology - Security techniques - Information security management systems - Requirements Copyright ISO/IEC 2013 Special Publication 800-53 Revision 4

	(developed by NIST) under the Federal Information Security Management Act (FISMA) Executive Order 13717 signed by President Obama on 2-2-2016 www.NIST.org
Recommended:	COBIT 4.1 Framework, Management Guidelines, Maturity Models Copyright © IT Governance Institute , 2007 editor: Information Systems Audit and Control Association Rolling Meadows, Illinois, USA, © ISACA Enabling Processes - COBIT 5 An ISACA Framework Copyright © 2012 ISACA. All rights reserved. For usage guidelines, see www.isaca.org/COBITuse (As an Expert Reviewer of the Subject Matter Expert Team of ISACA COBIT 5 I had participated in the COBIT 5 effort in 2010 - 2011 Expert Reviewer member of the Subject Matter Expert Team of COBIT 5: Katalin Szenes COBIT 2019 Framework: Introduction and Methodology COBIT 2019 Framework: Governance and Management Objectives member of the Expert Reviewer Working Group of COBIT 2019: Katalin Szenes CISA Review Technical Information Manual published yearly editor: Information Systems Audit and Control Association Rolling Meadows, Illinois, USA, © ISACA from the year of 1999 member of the Quality Assurance Team of the CISA Manual with the exception of CRM 2011: Katalin Szenes (contributes mostly to the chapters Protection of information assets, and Business continuity planning) Szenes, K.: On the Intelligent and Secure Scheduling of Web Services in Service Oriented Architectures - SOAs Procds. of the 7th International Symposium of Hungarian Researchers on Computational Intelligence Budapest, Hungary, 24-25 November, 2006, p. 473-482 Szenes, K.: Serving Strategy by Corporate Governance - Case Study: Outsourcing of Operational Activities Procds. of 17th International Business Information Management Association - IBIMA November 14-15, 2011, Milan, Italy, ed. Khalid S. Soliman, ISBN: 978-0-9821489-6-9, DOI: 10.5171/2011.903755, indexat BDI: Ebsco © 2011 IBIMA, [CD-ROM], p. 2387-2398 OASIS - Organization for the Advancement of Structured Information Standards - www.oasis-open.org e-business guidelines, non-profit OWASP - Open Web Application Security Project - www.owasp.org www.securityfocus.com
Other references:	Moodle