

Óbudai Egyetem Neumann János Informatikai Kar			Kiberfizikai Rendszerek Intézet		
Tantárgy neve és kódja: NAIS1EVNM Information System Audit			Kreditérték: 2		
Mérnök informatikus MSc szak			Nappali tagozat, 2020-21. tanév, II. félév		
Tantárgyfelelős oktató: Dr. Szenes Katalin					
Előtanulmányi feltételek: (kóddal)		-			
Heti óraszámok:	Előadás: 2	Tantermi gyak.:	Laborgyakorlat:	Konzultáció:	
Számonkérés módja (s,v,f):	v				
The Material					
Goal of Education: IT is regularly audited both in the government and in the business sector. Such critical infrastructures, as e.g. the financial and the energy sector have especially to be compliant to the laws, government decrees and European Union directives. From the viewpoint of the owners / mother companies an emphasized viewpoint is the quality of strategy support. Every member of the IT staff, even the developers of either data processing applications or those of the embedded systems have to be prepared to participate in audit interviews, exploring, if their results support corporate governance, and such information quality criteria as e.g. the availability, confidentiality and integrity of the resource handling, the business continuity planning, and other aspects of IT security. The goal of subject Information System Audit is to support compliance to the most frequently required audit aspects.					
Subjects: Professional audits are usually based on the COBIT (Control Objectives for IT) methodology of ISACA (Information Systems Audit and Control Association, on ISO (International Standards Organization) security standards and NIST (USA National Institute of Standards and Technology) recommendations. Besides these, we take EU (European Union) directives also into consideration, together with other internationally acknowledged materials, too. The lecture gives, among other important issues, an overview of the professional best practice dealing with risk management, organizational, regulational and technical problems, together with their resolving, the development / acquisition of application systems, the business continuity plans, recommendations on outsourcing. We deal with the methods of auditing these issues, too.					
Scheduling:					
week	subject				
1.	Threats in the cyberspace (APT - Advanced Persistent Threats, and other current security issues)				
2.	Governments' defense efforts: laws, directives - Hungarian, EU, USA - SEC (Security Exchange Committee). SOX: Sarbanes - Oxley. CERT: Computer Emergency Response Team.				
3. – 4.	The basics of institutional audit & security: control objectives, preventive, detective, corrective control measures; the basic pillars of corporate operations; practice: CISA exam test questions; pillars of operations (organization, regulation, technics)				
5.	The strategy-based risk assessment & management				
6.-7.	Information criteria according to the ISACA and ISO materials and their ancestors				
8.	Application security. Operational excellence: strategy and security				
9.	Auditing physical security				
10.	Auditing outsourcing				
11.	Auditing institutional network topology				
12.	Data privacy requirements				
13.	Business continuity planning and management				
14.	Written test				
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.

Exam: verbal

**Compulsory literature:**

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](http://www.nist.org)

**Recommended literature:**

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](http://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](http://www.oasis-open.org)

e-business guidelines, non-profit

OWASP - Open Web Application Security Project - [www.owasp.org](http://www.owasp.org)

[www.securityfocus.com](http://www.securityfocus.com)