MODULE **DESCRIPTOR**

MODULE TITLE	Information Security Management		
MODULE CODE	CO4512 (L7)	**CREDIT VALUE**	20 credits / 10 ECTS
SCHOOL	SCHOOL OF SCIENCE		

MODULE **AIMS**

An increasing level of security threats and the existence of vulnerabilities expose organisations to frequent security risks. Managing those risks is essential not only for protecting organisational and clients' assets but also as a competitive business advantage. This module exposes students to Information Security Management and Information Risk Management concepts and their use in practice to enforce preventive security.

The aims of the module are:

- To introduce information security and risk management standards and methods that students will most likely encounter as a security professional.
- To evaluate the applicability and critically analyse alternatives for information security management and risk assessment.
- To apply techniques and conduct activities involved in the process of information security and risk management.
- To critically evaluate the benefits and pitfalls of compliance-based security.

MODULE **CONTENT**

Information Security Management
ISO/IEC 27K family; ISO/IEC 27001 implementation, certification and auditing; scope of an Information Security Management System (ISMS); the Plan, Do, Check, Act (PDCA) process; selection of clauses and controls; documentation; advantages/disadvantages of an ISMS; maintaining the ISMS.
Other management and governance approaches, such as COBIT, and domain-specific security standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act |(HIPAA).

Information Security Risk Management
Essential concepts; different standards and methods (e.g., ISO/IEC 27005, SP-800-30, CORAS, CRAMM); the risk management process according to ISO 27005; identify assets; identify, analyse and evaluate risks; the Common Vulnerability Scoring System (CVSS) and other approaches for risk level estimation; identify and evaluate risk treatment options; documentation; monitor and review the effectiveness of controls selected; find information relevant to risk management (e.g. databases such as the National Vulnerability and the Open Security Vulnerability Database (OSVDB), security intelligence labs and specialized news media).

Compliance and Security
Factors driving compliance; compliance problems; relation between compliance and security.

INTENDED **LEARNING OUTCOMES**

On successful completion of this module a student will be able to:

1.	Select and use applicable standards and methods for information security and risk management.
2.	Compare and critically evaluate alternatives for information security management and risk assessment.
3.	Conduct and properly document risk assessment based on a given scenario.
4.	Find and evaluate appropriate published information to remain up-to-date about threats, vulnerabilities and patches.
5.	Critically discuss benefits and pitfalls of compliance in respect to security.

TEACHING METHODS

Lectures are used to present new knowledge and concepts illustrated by examples, and to expose students to experiences reported by visiting speakers, whenever possible. While tutorials are used to consolidate, and to build skills by applying presented knowledge and concepts to different situations found in practice. Tutorials take advantage of exercises, analysis of scenarios, and discussion as instruments for learning.

Directed reading will also be used to complement and broaden the content of lectures, and to provide material for in-class discussion.

The assignment will assess students' ability to plan, conduct and report a risk assessment based on a realistic, yet fictitious, scenario. The examination will assess the understanding of concepts and their application to unseen situations, as well as students' critical skills related to topics covered.

Distance learning

The module tutor will deliver live online lectures through Adobe Connect. During the live lectures the participating students will have the opportunity to engage in discussions, present their views and ask questions. The lecture sessions will be recorded and made available to the students through Blackboard. Students who cannot participate in the live lectures will have the opportunity to answer and reflect on guided questions posted by the module tutor asynchronously, through a Blackboard discussion forum. The tutor will provide appropriate feedback to students' comments posted on the discussion board. Students will also be provided with relevant further reading, web links and resources for independent study. Speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.

Tutorials will further enhance student's skills in terms of communication, time management and critical thinking skills as the students will have the opportunity to work in small groups and participate more actively. The module tutor will assign the students in groups and guide them to use collaborative tools such as Skype to interact with their group members and work on an assigned worksheet. The findings of each team will be communicated to the module tutor as indicated by the worksheet instructions, for example by submitting a report through Blackboard or posting a post on the module's discussion forum. Feedback to the students will be provided asynchronously through Blackboard. If the group members would like to discuss their findings with the module tutor prior to submitting them, they can do so by contacting the module tutor to arrange a group live Adobe Connect or Skype session. If the need arises, the tutor will schedule live sessions to provide further feedback to all the students.

ASSESSMENT METHODS

This module is assessed through a Risk assessment report (50%) and an examination (50%).