

IMT4571 IT Governance - 2011-2012

Course code:

IMT4571

Course name:

IT Governance

Course level:

Master (syklus 2)

ECTS Credits:

5

Duration:

Autumn

Duration (additional text):

Second half of autumn semester

Language of instruction:

English

Expected learning outcomes:

Calder and Watkins define IT Governance as "the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization's information systems support and enable the achievement of its strategies and objectives". IT Governance is of crucial importance for organizations owing to the need to best safeguard critical information and, through the increasing requirements from national and international regulations. Central to IT Governance in Europe is the ISO 27001 / ISO 27002 standard.

This course provides an overview of IT Governance and the basic concepts of the ISO 27001 / ISO 27002 standard.

The candidate should after attending the course

- fully understand the main principles of IT Governance.
- fully understand the basic concepts of the ISO 27001 / ISO 27002 standard
- master the principles for designing & implementing an ISO 27001 ISMS
- be fully aware of the difference between security technology and the management of secure systems
- have a thorough understanding of security management as a continuous improvement process.
- possess awareness of security certification schemes (BS7799, ISO 15408, ...)

Topic(s):

- Reasons for IT Governance: Compliance, liability, stability
- Organizing information security
- Information security policy and scope
- The risk assessment and statement of applicability
- Identification of risks related to external parties
- Asset management
- Human resources security
- Physical and environmental security
- Equipment security
- Communications and operations management
- Controls against malicious software (malware) and back-ups
- Network security management and media handling
- Exchanges of information
- Electronic commerce services
- E-mail and internet use
- Access control
- Network access control
- Operating system access control
- Application access control and teleworking
- Systems acquisition, development and maintenance
- Cryptographic controls
- Security in development and support processes
- Monitoring and information security incident management
- Business continuity management
- Compliance
- Principles of auditing

Teaching Methods:

Other

Teaching Methods (additional text):

Lectures, exercises and projects.

Form(s) of Assessment:

Other

Form(s) of Assessment (additional text):

- 1-2 Multiple Choice Tests (weight: 20%)
- 1-2 Group Assignments (weight: 30%)
- Digital Final Exam, 2 hours (weight: 50%)
- All three parts are mandatory and must be passed!

Grading Scale:

Alphabetical Scale, A(best) – F (fail)

External/internal examiner:

Evaluated by the lecturer

Re-sit examination:

For the final exam: Ordinary re-sit examination.

Tillatte hjelpemidler:**Coursework Requirements:**

None.

Academic responsibility:

Faculty of Computer Science and Media Technology

Course responsibility:

Forskningssjef Åsmund Skomedal

Teaching Materials:

Literature:

Alan Calder & Steve Watkins. IT Governance : IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002. Fourth Edition. Kogan Page. 2008.

Anderson, Ross (1999) Why cryptosystems fail, University Computer Laboratory, University of Cambridge, Cambridge, UK, <http://www.cl.cam.ac.uk/~rja14/wcf.html>.

Publish:

Yes