Security Technology

## Prof. Marika Assogna; Prof. Franco Fantozzi

Module 1: *Safety of IT environments* (Prof. Marika Assogna)

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

Every company has a wealth of electronic data that are exchanged and processed through technological tools and procedures (ICT). This data is essential to all business activities run in the company, thus needs to be adequately protected and its privacy, integrity and availability guaranteed.

Lack of adequate levels of data security can result in negative consequences for the company, also in terms of fines related to violations of current norms on ICT systems and processes (for example GDPR, PSD2, DORA, EBA Guidelines). Therefore, security of ICT processes and information plays a key role in business management; it can be attained by implementing proper security measures to reduce the risks that IT data can be exposed to.

The course aims to provide students with an overview of concepts to better understand how to safeguard and protect ICT data and operative processes for corporate business in the specific field of ICT, both from the point of view of business continuity and of ICT risk and compliance management.

The course aims to provide students with knowledge about to the main regulations and sector standards which define important suggestions on the organisational and technical measures to be adopted to manage ICT data security. The course comprises two parts: the first one explores theoretical concepts, the second one includes workshops on real case studies of companies that have IT security issues.

The course intertwines theory with practical exercises in class with the help of the lecturer.

At the end of the course, students will be able to know the main cyber security threats and will become familiar with ICT processes.

Students will be able to identify risks and vulnerabilities related to ICT systems and define ICT security requirements necessary for the protection of company information.

Students will also be able to examine the main regulatory requirements in ICT security compliance and apply them to concrete cases.

***COURSE CONTENT***

1. *Theoretical concepts*

ICT Risk Management and IT Security.What’s an ICT system and how it is structured: basic notions.

The Plan-Do-.Check-Act cycle.

ITIL –IT Service Management.

The ISO/IEC 27001:2022 standard - *Information security, cybersecurity and privacy protection - Information security management systems – Requirements* (Organisational controls, Policy for ICT security; Organisation for information security (overview), Separation of roles, Controls on Human resources (overview). Management of goods; Access control, Cryptography, controls for physical and environmental security (overview), Technological controls, Operations management; Communication management; Acquisition, development and maintenance of IT systems; Relations with suppliers; Management of accidents in IT security; Aspects of IT security in managing continuity of business; Conformity and Audit.

Internal Control System: control activity and non-conformity risk: focus on risk & compliance ICT.

Specific principles introduced by EU General Data Protection Regulation (GDPR) related to ICT security: privacy by design and by default; *Data* *Protection* *Impact Assessment* (DPIA); data breach (notification and communication to the Guarantor).

The main cyber threats: definition, causes, implementing rules and security countermeasures.

2. *Workshop*

Presentation of concrete case studies of various companies with different issues related to IT security. Group discussion and work to choose the best solution to each case.

***READING LIST***

The reading list will be illustrated by the lecturer at the beginning of the course and will be posted on Blackboard.

***TEACHING METHOD***

Lectures in class, group discussion, group work during workshops, individual and group papers, presentation and discussion of exercise results.

***ASSESSMENT METHOD AND CRITERIA***

The final exam is written and takes place in the IT laboratory. The exam is divided into two parts. In the first one, students will answer 20 multiple choice questions; answers will be automatically corrected by the system and students will know their mark immediately. In the second part, students will answer three open-ended questions; answers will be marked by the lecturer at the end of the exam. Students will be assessed on their correct understanding of the questions, correct use of grammar syntax, and their ability to link concepts studied during the course and practical examples.

The final mark is the sum of the results of both parts.

***NOTES AND PREREQUISITES***

Being an introductory course, there are no content related prerequisites to attend the course. However, students are expected to show interest and curiosity about technologies and sensitivity to risk assessment.

Further information can be found on the lecturer's webpage at http://docenti.unicatt.it/web/searchByName.do?language=ENG, or on the Faculty notice board.

Module II: *Safety of physical environments* (Prof. Franco Fantozzi)

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

The corporate business security process comprises the assessment, management, control and review of the risks and threats and must be managed by security specialists.

The purpose of security activities is to prevent, tackle and solve security issues which may attack a company’s tangible, intangibile, organisational and human assets.

Hence, the security manager must have the knowledge, competences and abilities which are required to carry out his/her role effectively. Consequently, the aim of the course is to provide future corporate security specialists, with the technical, legal and in particular methodological tools to develop the knowledge, abilities and competences they require in order to fulfil their role properly.

The present security model, which has ceased to focus only on protecting corporate assets, has turned its attention to the risks and threats which may negatively affect business and the continuity of production or of services provision.

As a result, aspects related to the methodology for correct risk detection, analysis and mitigation and for drawing up a security plan will be elaborated. Subsequently, there will be an in-depth presentation of the elements of corporate crisis management and of the security manager’s role inside the crisis team.

Finally, the module will focus on the content of investigative activities, of the safety of staff during business trips and on the safety of the logistics chain, without neglecting privacy and international legal aspects.

At the end of the course, students will be able to autonomously carry out the detection, analysis and management of security risks and to identify related mitigation measures, both in terms of physical safety and of safety of the supply chain.

The students, also through scenario simulation, will be aware about the steps, the process and methodology for dealing with crisis management and will be holistically exposed to the management of travel risk management, acquiring basic knowledge for proper planning and management of risks associated with business trips.

***COURSE CONTENT***

1. Corporate business security.

Evolution of the security manager’s role, UNI 10459 certification, Professional profiles, knowledge and competences.

1. Risk management and security risk management. Risk analysis in accordance with ISO 31000:2018 guidelines and drawing-up of a security plan.
2. Crisis management and elements of Business Continuity management.

Crisis analysis. Review of best and worst practices in crisis management, the Crisis team and crisis management. Guidelines for the implementation of a business continuity plan; Exercises on crisis and emergency management. Scenario simulation;

1. Protection of privacy and security.

Video surveillance and use of IT systems to monitor employee activities. The EU Regulation on data protection (GDPR). The Organisational Model 231/2001. Tools for the control of workers and respect for privacy;

1. Supply chain security.

Cargo crime. Security in the transport and supply chain. Security programmes and TAPA, CT-PAT, AEO standards. Security in retail and last mile. ISO 28000:2007 guidelines. Site security assessment;

1. Travel risk management.

Safeguard and operational management of human resources during travel abroad. Occasional business trips and EXPATS on overseas contracts, Corporate Criminal Liability; duty of care, ISO 31030:2021 guidelines on travel risk management, travel risk policy and personal safety on the road.

Case studies.

Review of course teaching and preparation for the exam.

***READING LIST***

Slides and presentations provided by the lecturer;

Hypertext searches on websites recommended by the lecturer and consultation of official documents

“Security risk management”, author: Stefano BONACINA, IPSOA editore, 2010;

“La perfetta comunicazione d’emergenza, author: Mauro de Vincentis, Editori di comunicazione-Lupetti, 2001;

“Crisis therapy” author: Andrea Polo, edizioni Il Sole 24 ore;

“Manuale di Business continuity e crisis management”, author: Anthoiny Cecil Wright, Franco Angeli editore;

“Governare il rischio. Un modello di security risk management”, author: Umberto Saccone, edizioni ARACNE, 2014;

“Gè-Politikè”, Manuale di introduzione alla analisi geopolitica, author: Stefano Cont, Laurus Robuffo;

GDPR e Decreto Legislativo 101/2018, edited by Marco Martorana, Wolters Kluver;

Risk Managenent, la norma ISO 31000: 2018, by Ioannis Tsiouras, edizioni Youcanprint;

***TEACHING METHOD***

The course is characterised by frontal lectures with extensive interaction with students and their active participation in the examination and assessment of case studies and practical examples. During crisis management simulation, documents will be prepared and there will be a group examination of test results. Further exercises will focus on drawing up a security plan.

***ASSESSMENT METHOD AND CRITERIA***

The final exam is written and is divided into two parts. In the first one, students will answer 20 multiple choice questions set at random and taken from 100 questions suggested by the lecturer. The answers to the multiple choice questions will be automatically corrected by the system and students will know their mark immediately. In the second part, students will answer 3 open-ended questions, set at random and taken from 20 questions suggested by the lecturer. Subsequently, the answers will be marked by the lecturer who will mark open-ended questions out of 4.

During the written exam, students will be assessed on their correct understanding of the questions, on their ability to create links with other topics studied during the course, contextualising them within the question and demonstrating a correct use of grammar syntax when replying.

Students will also be able to include in their written dissertation practical examples and links with real-world cases developed during lectures.

 The final mark is the sum of the results of both parts.

***NOTES AND PREREQUISITES***

Attendance to the course, although not mandatory, is strongly recommended.

The slides and additional material, useful for exam preparation, will be made available online. Although there are no content-related prerequisites to attend the course, for an effective and successful interaction, students who are taught security, understood as an activity aiming to prevent, tackle and solve security issues which may expose the human resources and assets (tangible and intangible) of an Organisation to harmful and/or damaging effects, are expected to show interest in the study of law and a strong intellectual curiosity about the growing complexity of economic-production and geopolitical scenarios.

Further information can be found on the lecturer's webpage at http://docenti.unicatt.it/web/searchByName.do?language=ENG, or on the Faculty notice board.