INTENDED LEARNING OUTCOMES OF THE MASTER OF SCIENCE IN CYBER RISK STRATEGY AND GOVERNANCE

CORE AREA OF STUDY

Knowledge and Understanding

Graduates will acquire advanced knowledge related to:	Knowledge and Understanding will be achieved through the following courses:
1. Computer science and data analysis, to set the base for a solid professional development in cyber risks; in particular: 1.1. Main concepts of ICT architectures, computer network infrastructures and software methodologies of firms and institutions and their security vulnerabilities 1.2 Models and technologies for identifying, preventing, working with and recovering from situations of information technology, data protection and web-based risks 1.3 Technology risks assessments and identification of potential exploitable vulnerabilities as a driver for the definition of security requirements 1.4 Key concepts of artificial intelligence and their application to security problems	1.1 Software methodologies and architectures for security (module 1 and 2) 1.2 Cybersecurity technologies, procedures and policies 1.3 Technology risk governance 1.4 Artificial intelligence for security
2. Multi-disciplinary tool kits to frame cyber risks, set the appropriate strategies and govern their complexity in organizational environments; in particular: 2.1 Enterprise - wide models for identifying, detecting, responding and recovering from cyber risks 2.2 Mathematical methods of decision analysis and modelling 2.3 Scenarios for understanding macro risks for industries, infrastructures and locations 2.4 Legal issues regarding vulnerability, anonymity, privacy, data protection	2.1 Strategy and governance for cyber risk 2.2 Methods and data analytics for risk assessment 2.3 Institutional scenarios for cyber risk 2.4 Cyber risk and data protection law

Applying Knowledge and Understanding

Graduates will be able to:	Ability to Apply Knowledge and Understanding will be achieved through the following courses:
1. Manage technological issues related to cyber risk and security; in particular: 1.1 design the requirements of an appropriate security architecture and organization 1.2 define, assess, audit cybersecurity policies and procedures in organizations in the framework of national and international regulations 1.3 apply risk management models to enterprise-wide IT systems 1.4 apply artificial intelligence and machine learning techniques to cyber risk and security problems	1.1 Software methodologies and architectures for security (module 1 and 2) 1.2 Cybersecurity technologies, procedures and policies 1.3 Technology risk governance 1.4 Artificial intelligence for security
2. Govern and manage strategic and main organizational issues related to cyber risk and security of firms, institutions and critical infrastructures; in particular: 2.1 Apply methodologies and technique to assess the most valuable assets of organizations 2.2 Apply mathematical advanced models (including game theory models) to properly and effectively assess cyber risk 2.3 Map and analyze risks at macro and micro level for organizations and industries 2.4 Interpret relevant rules and regulations for effective operations in cyber environments	2.1 strategy and governance for cyber risk 2.2 methods and data analytics for risk assessment 2.3 institutional scenarios for cyber risk 2.4 Cyber risk and data protection law

CUSTOMIZED AND LINGUISTIC AREA OF STUDY

Knowledge and Understanding

Regarding the “personalized” part of the study plan, graduates will acquire wide-ranging and in-depth knowledge related to specific topics of their choice, identified on the basis of individual interests and in line with the educational program. In particular:

- knowledge related to strategic risk assessment, governance and management and relative impact on the organization’s functioning and overall performance;
- knowledge related to data and privacy protection and relative assessments and operations.

Regarding languages, besides English (which is an entry requirement), graduates will acquire knowledge of another EU language (Italian: at least level A2; other EU language among those listed in the University Guide: at least level B1 business; Italian is compulsory for non-Italian native speakers).

Applying Knowledge and Understanding

Graduates will be able to apply the methodologies acquired during the study program and use related practical tools; over time, they will be able to analyze and interpret the context of reference for issues related to the subjects of the study program and apply the logical methods acquired for tackling any new problems that may arise during their professional activity.

All graduates will be able- at different levels according to the personalization of their study plan - to :

- Contribute to setting and implementing cyber policies in organizations to reduce risks of vulnerability and take advantage of opportunities in the cyber world
- Contribute in designing, advising, managing and maintaining procedure compliance with data protection laws and policies

Regarding languages, besides English (language of the program) graduates will demonstrate abilities (written and oral comprehension and expression) in another EU language (at least elementary level; the exit level depends on the language – Italian or other EU language – and on the student’s entry level).

Making Judgements	Graduates will acquire the ability to integrate knowledge, manage complexity and make judgements even with partial information, including considerations and assessments regarding decision process related to “cyber risk”.
ommunication	Graduates will acquire skills and tools appropriate for the management and transfer of information, both to specialists and non-specialists of the topic. In particular, they will be able to express themselves clearly and effectively in any setting. They will be able to make a presentation in public using the most modern IT tools.
Lifelong Learning Skills	Graduates will acquire learning skills that allow them to be autonomous in updating and developing their knowledge and competences related to “cyber risk” analysis and management.