MODULE TITLE	**Business Aspects of Digital Forensics and Ethics**				**CREDIT VALUE**	5
MODULE CODE				**MODULE CONVENOR**		
DURATION	**TERM**	**First semester**	**Second semester**		**Number Students Taking Module (anticipated)**	
	WEEKS	16				

DESCRIPTION – summary of the module content (100 words)
This course approaches digital forensics (DF) from the business perspective. It starts by introducing security as a business process with three interacting components: people, technology and process. It discusses cybercrime and its impact on organisations. Students will be introduced to the concept of Incident Response within the context of Contingency Planning which represents the overall plan to manage enterprise security including DF. The Students will explore international related standards with emphasis on both ISO/IEC 27000:2018 ISMS — Overview and vocabulary and ISO/IEC 27037:2012 They will study guidelines for identification, collection, acquisition and preservation of digital evidence. Ethical issues related to DF will be also discussed.
PREREQUISITES – previous courses required to take this course
Foundations of digital forensics
MODULE AIMS – intentions of the module
This course aims to provide students with the knowledge and skills essential for planning and managing digital forensics in business organisations in a professional and ethical way. It will expose the students to principles, frameworks and standards for handling and investigating security incidents considering various ethical and managerial implications.
INTENDED LEARNING OUTCOMES (ILOs) (see assessment section below for how ILOs will be assessed) On successful completion of this module you should be able to:
Module Specific Skills and Knowledge:
1 Understand the impact of cybercrime and the role of digital forensics in today's business organisations.
2 Develop a working knowledge of standards and best practices to plan and manage digital forensics.
Discipline Specific Skills and Knowledge:
3 Recognise security as a business process with various stakeholders and components.
4 Apply the required principles and standards to plan for and perform digital forensics.
Personal and Key Transferable/ Employment Skills and Knowledge:
5 Work in a team to plan and perform digital forensics.
6 Write standard policies and plans for handling and investigating security incidents.
7 Report digital investigation results in a clear and professional way.
8 Demonstrate a high standard of ethics in performing digital forensics.
SYLLABUS PLAN – summary of the structure and academic content of the module
Module Syllabus Part 1: Foundation Ch1: Introduction to Security and Digital Forensics: ▪ Cyberspace and business organisations. ▪ Cybercrimes and threats. ▪ Cybersecurity principles and terminologies. Ch2: Managing security in business organisation: ▪ Security governance, planning and policies. ▪ Security risk management. ▪ Contingency planning. ▪ Incident response. Part 2: Standards, framework and best practices for incident response and digital forensics:

Ch3: NIST Special Publication 800-61 Rev. 2 Computer Security Incident Handling Guide.
Ch4: ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.
Ch5: NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response.

Part 3: Social and Ethical aspect:

Ch6: Ethical and Social issues in digital forensics.

LEARNING AND TEACHING

LEARNING ACTIVITIES AND TEACHING METHODS (given in hours of study time)

Scheduled Learning & Teaching activities	48	Guided independent study	140	Placement/study abroad	0

DETAILS OF LEARNING ACTIVITIES AND TEACHING METHODS

Category	Hours of study time	Description
Scheduled learning and teaching	24	Lectures
Scheduled learning and teaching	24	Case studies and exercises
Guided independent study	36	Assignments
Guided independent study	24	Project
Guided independent study	40	Revision for project presentation and written exams
Guided independent study	40	Preparation for lectures

ASSESSMENT

FORMATIVE ASSESSMENT - for feedback and development purposes; does not count towards module grade

Form of Assessment	Size of the assessment e.g. duration/length	ILOs assessed	Feedback method
Case studies and exercises	12 x 2 hours	1-8	Oral, written

SUMMATIVE ASSESSMENT (% of credit)

Coursework	10%	Written exams	70%	Project	20%

DETAILS OF SUMMATIVE ASSESSMENT

Form of Assessment	% of credit	Size of the assessment e.g. duration/length	ILOs assessed	Feedback method
Assignment	5%	12 weeks	1-4	Online
Project	15%	4 weeks	1-4	Online
Written exams (Mid 30% + Final 50%)	80%	3 hours	4	Online + oral

DETAILS OF RE-ASSESSMENT (where required by referral or deferral)

Original form of assessment	Form of re-assessment	ILOs re-assessed	Time scale for re-assessment

-

RESOURCES

INDICATIVE LEARNING RESOURCES - The following list is offered as an indication of the type & level of

information that you are expected to consult. Further guidance will be provided by the Module Convener.

Basic reading:

1. Business Aspects of Digital Forensics and Ethics (FORC developed textbook)

Web based and electronic resources:

2. NIST Computer Security Resource Centre: https://csrc.nist.gov/publications/sp800
3. IEEE Xplore digital library
4. ACM digital library
5. EBSCO database
6. SpringerLink database
7. ProQuest database

Other resources:

1. Computer Security-related organizations : CERT, SANS, CIS, CASPR, CSI, CIAO, DRII, ISSA, IATFF, I2SF, NIAP, CSRC, OWASP

CREDIT VALUE	5	**ECTS VALUE**	**5**	
PRE-REQUISITE MODULES	None			
CO-REQUISITE MODULES	Foundations of digital forensics			
NQF LEVEL (FHEQ)	6	**AVAILABLE AS DISTANCE LEARNING**		No
ORIGIN DATE		**LAST REVISION DATE**	**08/10/18**	
KEY WORDS SEARCH	Security management, Incident response, business, standards, ethics			