Module description: IT Security

Module Code	w.MA.XX.ITSY.24HS
ECTS Credits	6
Language of Instruction/Examination	English
Module Description	This advanced seminar on information system security is designed to equip students with in-depth knowledge of contemporary challenges and innovative solutions in cybersecurity. The course begins with four days of introductory lectures on information security basics to ensure all participants have a sufficient foundational understanding. For each of the following ten days of the seminar, a specific cutting-edge topic will be introduced. Each day will start with an introductory talk on the "topic of the day," providing a comprehensive overview of the subject matter. Students will then engage in preparing and delivering a conference-style presentation focusing on a specific research paper related to the day's topic. These presentations will allow students to delve deeply into current research, critically evaluate findings, and discuss implications. In addition to individual presentations, student groups (assigned to the same topic of the day) will collaborate to prepare an overview paper. This paper will synthesize the state-of-the-art research and highlight current challenges in the specific area of information system security, incorporating additional materials beyond the primary research papers.
Organizational Unit	IWI Ltg.
Module Coordinator	Peter Heinrich
Program and Specialization	• Business Information Technology
Legal Framework	Academic Regulations MSc in Business Information Technology dated 22.08.2019, Appendix to the Academic Regulations for the degree program in Business Information Technology, first adopted on 10.07.2012
Module Category	**Module Type** Compulsory
Prerequisite Knowledge	To successfully engage in this advanced seminar on information system security, students should possess a basic understanding of computer science, networking concepts, and introductory cybersecurity principles. Critical thinking and problem-solving skills are essential, as well as a willingness to learn and adapt to new technologies. Prior hands-on experience in cybersecurity is beneficial but not required. Enthusiasm for learning and a proactive approach will ensure a rewarding seminar experience.
Contribution to Program Learning Objectives (by the concerned Module)	• Professional Competence • Methodological Competence • Social Competence • Self-Competence
Contribution to Program Learning Objectives	**Professional Competence** • Knowing and Understanding Content of Theoretical and Practical Relevance • Apply, Analyze, and Synthesize Content of Theoretical and Practical Relevance • Evaluate Content of Theoretical and Practical Relevance **Methodological Competence** • Problem-Solving & Critical Thinking • Scientific Methodology • Work Methods, Techniques, and Procedures • Information Literacy **Social Competence** • Written Communication • Oral Communication **Self-Competence** • Self-Management & Self-Reflection • Ethical & Social Responsibility • Learning & Change

Module description: IT Security

Module Learning Objectives	Students... • will develop a comprehensive understanding of cutting-edge information system security topics, enabling them to critically evaluate and discuss recent research papers. • will gain experience in academic research and writing, ensuring they can effectively communicate complex information security topics to diverse audiences. • will enhance their presentation skills by delivering a well-organized talk on a selected research paper, clearly articulating key findings and their implications. • will improve their collaborative skills by working in groups to produce a detailed summarizing overview paper that synthesizes insights from multiple sources. • will cultivate the ability to analyze and critique advanced cybersecurity concepts, applying theoretical knowledge to practical scenarios.
Module Content	• Zero Trust Architecture (ZTA) - Focuses on the principle of "never trust, always verify," continuously verifying the identity and context of users and devices. • Ransomware and Advanced Persistent Threats (APTs) - Studies evolving ransomware tactics and APTs, including detection, prevention, and response strategies. • Artificial Intelligence and Machine Learning in Cybersecurity - Utilizes AI/ML for threat and anomaly detection, and predictive analysis in cybersecurity. • Blockchain and Distributed Ledger Technologies for Security - Explores blockchain applications for secure transactions, enhancing privacy, and ensuring data integrity. • Internet of Things (IoT) Security - Addresses the unique security challenges of the proliferation of IoT devices in various domains. • Quantum Computing and Cryptography - Investigates the impact of quantum computing on current cryptographic methods and the development of quantum-resistant algorithms. • Privacy-Preserving Technologies - Focuses on techniques that ensure user privacy while enabling data analysis and sharing. • Cloud Security and Secure Virtualization - Examines security issues in cloud computing environments, including data protection, access control, and secure virtualization. • Human Factors and Social Engineering - Studies the role of human behavior in cybersecurity, focusing on social engineering attacks and human-centric security measures. • Cyber-Physical Systems (CPS) and Critical Infrastructure Protection - Investigates the security of CPS and critical infrastructures like power grids and water systems.
Links to other modules	This module is linked to the following modules: • w.BA.XX.3ITSe-WIN.XX
Digital Learning Resources	• Reader • Teaching Materials
Methods of Instruction	• Lecture • Literature Review • Interactive Instruction • Project Work Social Settings Used: • Group Work • Individual Work

Type of Instruction		Classroom Instruction	Guided Self-Study	Autonomous Self-Study
	Lecture	26 h	-	
	Excercise	-	-	
	Project Work	56 h	-	
	Seminar	30 h	68 h	
	Total	**112 h**	**68 h**	**0 h**

Module description: IT Security

Performance Assessment	End-of-module exam	Form	Length (min.)	Weighting
	-			
	Permitted Resources			

	Others	Assessment	Format	Length (min.)	Weighting
	Talk/oral presentation	Grade	Einzelarbeit	30	80.00
	Written hand-in *In groups of 3-4 you present how the field evolved during the last year in one specific topic (one day of lecturing). You will use the 3-4 papers presented on that day and add further papers from other journals and conferences to complete the picture.*	Grade	Gruppenarbeit	0	20.00

Classroom Attendance Requirement	Other Students must be present for 8 out of 10 seminar blocks starting in week 5. The introductory lectures spanning week 1-4 will be recorded.
Compulsory Reading	• vom Brocke, J. & Simons, A. & Niehaves, B. & Riemer, K. & Plattfaut, R. & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process.. Proceedings of the European Conference on Information Systems (ECIS), • Webster, J. & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, 2002 pp. xiii-xxiii.
Recommended Reading	
Comments	