

Valid from 2026.HS

Module description: IT Security Management	
Module Code	w.MA.XX.ITSM.26HS
ECTS Credits	6
Language of Instruction/Examination	English
Module Description	This module equips future information-security leaders with the managerial knowledge and skills required to protect organisational assets. During the semester students move from the technical foundations to IT security management practices and the implementation of secure and usable systems. Throughout the semester students will analyse real-world breaches, design elements of an ISO/IEC 27001-aligned Information Security Management System (ISMS), conduct risk assessments, and practise incident-response coordination. Emphasis is placed on aligning security objectives with business strategy, embedding privacy and usability principles early in the systems-development life-cycle, and fostering cybersecurity and privacy awareness among employees. Each semester week begins with individual self-study and a group case preparation and is followed by in class case exercises led by the students.
Organizational Unit	Institut für Wirtschaftsinformatik
Module Coordinator	Nico Ebert
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	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 an advantage but not required.
Contribution to Learning Objectives (by the concerned Module)	• Professional Competence • Methodological Competence • Social Competence • Self-Competence

Module description: IT Security Management

Contribution to 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 • Creativity & Innovation Social Competence • Written Communication • Oral Communication • Teamwork & Conflict Management Self-Competence • Self-Management & Self-Reflection • Ethical & Social Responsibility • Learning & Change
Module Learning Objectives	Students... • will develop foundational knowledge by understanding core concepts, attack vectors, system and cryptographic security, and network/cloud security principles. • will analyse and evaluate contemporary cyber-threats and determine appropriate technical and organisational controls to mitigate them. • will design and govern an information security management system (ISMS) that meets recognised standards and supports continuous improvement. • will apply structured risk-management methodologies to identify, assess, prioritise, and treat information-security risks in diverse organisational contexts. • will plan and coordinate effective incident-response processes, covering preparation, detection, containment, eradication, recovery, and post-incident learning. • will integrate legal, human, and usability considerations - including regulatory compliance, security awareness, and privacy- & security-by-design - into security-management decisions.
Module Content	• Course Overview & Basic Concepts: establishes core terminology, the CIA triad, threat landscape, actors, and foundational controls. • Attack Vectors & Cyber Operations: examines external and internal attack vectors, tactics/techniques/procedures, and breach case studies. • System Security & Cryptography: explores secure system architectures, cryptographic primitives, key-management practices, and common system-level attacks. • Network & Cloud Security: covers defences for on-prem and cloud networks, secure virtualisation, segmentation, and monitoring strategies. • Authentication & Identity-/Access-Management: analyses authentication factors, multi-factor approaches, IAM life-cycle, policies, and Zero-Trust principles. • Information-Security Governance & Culture: studies governance frameworks, leadership roles, metrics, policy development, and cultivating a security-minded culture. • ISMS & Security-Programme Implementation: details ISO/IEC 27001 control families, ISMS life-cycle, programme roadmaps, and continuous-improvement metrics. • Information-Security Risk Management: practises risk identification, qualitative & quantitative assessment, risk treatment options, and reporting to stakeholders. • Information-Security Incident Management: addresses readiness planning, detection & analysis, containment, recovery, and lessons-learned activities. • Security & Privacy Law: reviews Swiss privacy and security law as well as EU law applicable to organisations. • Security & Privacy by Design: integrates security and privacy requirements into SDLC, covers threat modelling and data anonymization. • Security Awareness & Behaviour Change: designs awareness interventions and leverages behavioural-science insights. • Usable Security & Privacy: applies human-centred design to security and privacy mechanisms, balancing usability with protection (e.g., password UX).

Module description: IT Security Management

Links to other modules	Linked Module				
	w.MA.XX.AISM.26HS / Advanced IT Security Management w.MA.XX.ITIS.26HS / IT Infrastructure Security				
Digital Learning Resources	• Reader • Teaching Videos • Teaching Materials • Case Studies (with Key)				
Methods of Instruction	• Lecture • Interactive Instruction • Problem-Oriented Teaching • Exercises • Case Studies		Social Settings Used: • Group Work • Individual Work		
Type of Instruction		Classroom Instruction	Guided Self-Study	Autonomous Self-Study	
	Lecture	-	30 h		
	Excercise	28 h	30 h		
	Project Work	-	-		
	Seminar	-	34 h		
	Total	28 h	94 h	58 h	
Performance Assessment	End-of-module exam		Form	Length (min.)	Weighting
	Written exam		closed book	90	100.00%
	Permitted Resources		Spec. calculator acc. to leaflet "Utilities"	With dictionary	
		Assessment	Format	Length (min.)	Weighting
	-	-	-	-	-
Classroom Attendance Requirement	None				
Compulsory Reading	• Jøsang, A. (2024). Governance and Information Security Management. Springer Cham: Springer. ISBN 978-3-031-68483-8. https://doi.org/10.1007/978-3-031-68483-8.				
Comments	Further details about assignments and attendance are defined in the semester program. Supplementary examinations may not be set, and assessed work may not be resubmitted.				