Die Modulbeschreibung sollte direkt über diesen Link in HISinOne eingepflegt werden.

Module code	Module title		Category
MAIE3020	Information Security Management for Software Engineering		MA
	Degree program	MA Software Engineering	
	Faculty	Building Services Engineering and Computer Science	

Module coordinator	Prof. Dr. Volker Herwig
Module type	Mandatory module
Frequency	1x annually in SuSe
Recommended semester	1. semester
Credit (ECTS-Points)	5
Academic Assessment Method	Exam PZ = Examination requirement (N: graded) PZ (N), K90)
Teaching language	English
Admission requirements for this Module	none
Module duration	1 Semester
Required Registration	Students enrolled in the above-mentioned degree program/standard semester will be registered automatically upon re-enrollment; all other participants, please refer to the information below. none

	Course	Lecturer	Type	Group Size (max.)	Number of Groups	Contact hours per week (SWS)	Workload (in h)	
							Face-to-face	Self-study
1	Information Security Management for Software Engineering	Extern	Seminar	30	1	4	60	65
2	Titel der Lehrveranstaltung.	Dozent*in	Wählen Sie ein Element aus.		Wählen Sie ein Element aus.			
3	Titel der Lehrveranstaltung.	Dozent*in	Wählen Sie ein Element aus.		Wählen Sie ein Element aus.			
4			Wählen Sie ein Element aus.					

Zuletzt bearbeitet: 08.02.2026

5	Titel der Lehrveranstaltung.	Dozent*in	Wählen Sie ein Element aus.		Wählen Sie ein Element aus.			
						Sum	**4,0**	**60**	**65**
						Total Workload for Module		**125**	

Learning Objectives / Learning outcomes	1. Explain the purpose and principles of an Information Security Management System (ISMS), including context, interested parties, scope, governance, roles, and the Plan-Do-Check-Act (PDCA) cycle. 2. Define and justify an ISMS scope for a software organization/product (including cloud services), and establish an asset inventory with ownership and classification. 3. Perform a risk assessment per ISO/IEC 27005: identify assets, threats, vulnerabilities; estimate likelihood and impact; set risk acceptance criteria; and produce a risk treatment plan. 4. Select and justify security controls from ISO/IEC 27001:2022 Annex A (with guidance from ISO/IEC 27002:2022) and compile a defensible Statement of Applicability (SoA). 5. Integrate control requirements into a secure Software Development Life Cycle (SDLC) and DevOps workflows (requirements, design, coding, testing, deployment, change management, segregation of duties, least privilege). 6. Implement and evidence key controls in Continuous Integration / Continuous Delivery (CI/CD) pipelines: secrets management, access control, vulnerability management, logging/monitoring, backups/restore tests, and software supply-chain integrity (e.g., artifact signing, provenance). 7. Set information-security objectives and metrics, monitor effectiveness, and execute corrective actions through internal audits, management review, and continual improvement. 8. Develop ISMS documentation: policies and procedures, risk register, asset register, SoA, incident response plan, supplier security requirements, and interfaces to business continuity. 9. Assess third-party and cloud risk (due diligence, contractual controls, data processing agreements), applying guidance from ISO/IEC 27017 (cloud security) and ISO/IEC 27018 (protection of personally identifiable information in cloud). 10. Plan and conduct an internal ISMS audit: define scope/criteria, gather evidence, identify nonconformities, and propose corrective and preventive actions.
Contents	• ISMS foundations: purpose, principles, governance model, roles, and PDCA cycle • ISMS scope definition for software products and organizations (incl. cloud services) • Asset management: inventory, ownership, classification, and handling rules • Risk management per ISO/IEC 27005: threat/vulnerability identification and risk estimation • Risk treatment planning: acceptance criteria, treatment options, residual risk, approvals • Control selection and tailoring using ISO/IEC 27001:2022 Annex A and ISO/IEC 27002 guidance • Statement of Applicability (SoA): structure, rationale, and evidence expectations • Secure SDLC integration: embedding controls into requirements, design, implementation, and testing

	• Security requirements engineering: misuse/abuse cases, security acceptance criteria, traceability • Threat modeling practice (e.g., STRIDE): attack surfaces, trust boundaries, mitigations • DevSecOps in CI/CD: quality gates, secrets management, access control, and segregation of duties • Vulnerability management: SAST/DAST, dependency scanning, triage, remediation, and retesting • Software supply-chain security: SBOM creation, artifact signing, provenance, and integrity checks • Incident management aligned with ISO/IEC 27035: detection, classification, escalation, postmortems • Internal audits and continual improvement: audit planning, evidence collection, metrics/KPIs, management review, certification readiness
Literature	• ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO. • ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls. ISO. • ISO/IEC 27005:2022 — Information security risk management. ISO. • ISO/IEC 27035 (Series) — Information security incident management. ISO. • NIST (2022). Secure Software Development Framework (SSDF), SP 800-218. National Institute of Standards and Technology. (frei verfügbar) • OWASP (ongoing). OWASP Application Security Verification Standard (ASVS). OWASP Foundation. (frei verfügbar) • Shostack, Adam (2014). Threat Modeling: Designing for Security. Wiley. • Anderson, Ross (2020, 3rd ed.). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley. • Kim, Gene; Humble, Jez; Debois, Patrick; Willis, John; Forsgren, Nicole (2021, 2nd ed.). The DevOps Handbook. IT Revolution.