Risk & Compliance Lab

26HS

Programme	MSc in Business Information Systems
Degree	Master
ECTS	6
Module type	elective module
Module coordinator	Prof. Dr. Petra Asprion
Compulsory attendance	Compulsory 2 dates presentation, lab results
Leading principle / Short description	Modern organizations operate in complex regulatory and technological environments, requiring an integrated approach to governance, risk, and compliance (**GRC**). This module offers a structured, practice-oriented introduction to key frameworks, standards, and best practices for effective decision-making, risk control, and regulatory alignment in a digital context. Designed as an interactive **Audit Lab**, the course immerses students in real-world scenarios through case-based exercises and simulated audits. Students actively apply concepts and gain practical insight into how governance, risk, and compliance are implemented and monitored. The module is structured around four interconnected pillars: ◦ **Governance** – designing and evaluating decision structures ◦ **Risk Management** – identifying and mitigating organizational risks ◦ **Compliance** – operationalizing legal and regulatory requirements ◦ **Audit** – performing assurance and monitoring activities A dedicated focus is placed on **cybersecurity**, **AI security, data privacy and GDPR**, addressing its impact on business processes and responsible data governance.
Module content	In this module, we explore how organizations translate regulatory requirements into effective entrepreneurial and operational practices. We develop a structured understanding of how governance, risk, and compliance (**GRC**) support decision-making and enable resilient and effective operations in modern, data-driven and digital environments. We examine audit and assurance approaches, including regulatory audits and quality assessments, and apply established frameworks such as COBIT, ISO standards, ITIL, and NIST, while critically assessing their relevance in data-centric and AI-enabled contexts. In the **Audit Lab**, we emphasize learning by doing. Students: ◦ apply and combine frameworks using a dedicated software solution ◦ select their own company, use case, or industry context ◦ choose and apply an appropriate audit framework ◦ assume the role of an auditor, conducting assessments, documenting findings, and developing recommendations ◦ evaluate internal controls and derive actionable improvements We further explore data governance, AI-related risks, and emerging regulatory expectations. Experienced practitioners enrich the module through guest lectures, providing first-hand insights into current industry challenges and practices.

Competencies to be achieved

Knowledge & Understanding (Remembering / Understanding / Analyzing)

- Students explain and differentiate key concepts of **governance, risk management, compliance, and audit** in date-driven organizations. They analyze the interaction of GRC components and interpret relevant frameworks and regulations, with a focus on cybersecurity, AI regulations, **data privacy and GDPR**.

Application (Applying / Analyzing)

- Students apply GRC frameworks and standards to real or simulated cases within the **Audit Lab**. They conduct structured analyses (e.g., gap analyses/audits), evaluate and assess controls, and document findings in a professional manner using a professional audit application.

Evaluation & Judgement (Evaluating)

- Students assess risks and control effectiveness, and formulate justified recommendations to improve governance, compliance, and risk mitigation based on audit results.

Communication (Applying / Evaluating)

- Students present audit results clearly in written and oral form, communicating key insights, risks, and recommendations in a structured and professional way.

Learning Skills (Analyzing / Evaluating / Creating)

- Students work independently, identify knowledge gaps, and develop solutions in dynamic contexts. They reflect critically on their analyses and decisions, strengthening their ability to adapt and continuously improve.

Prerequisites

Knowledge based no the core module "Business Process Management" is an advantage

Teaching and learning methods

Contact Hours:
Lecture, Discussion, Presentation, Assignment, Group work, Review of Literature, Software Usage
Guided Self-Study:
Individual work, group work

Literature

Required Reading: all material will be provided on Moodle or hints/links to "add-on" literature will be provided

Remarks

The module 'Cyber Security and Resilience' is a perfect complement to the contents of this course.
Links to other modules: Business Process Management

Grading

Grades 1 - 6 (half grades)

Assessment

Assignment: Group Assessment with individual contributions 50%	
Oral / Written	Written (Report) & Verbal (Presentation)
Timeframe	During Semester
Grading Scale	Grade 1-6 (half grades)
Remarks	The results of the assignment are documented in an audit report and subsequently presented in a small group in a discursive format. The assignment consists of one individual component per team member and is graded individually.

Exam: Individual Assessment 50%	
Oral / Written	Written
Duration (min)	60
Timeframe	Examination Period
Grading Scale	Grade 1-6 (half grades)
Remarks	The theoretical component is assessed through a written assessment.

Module details

26HS.Risk & Compliance Lab - Thu - Olten	
Time	1:15 PM - 5:00 PM
Language	Englisch
Periodicity	Weekly
Number	3-26HS.W-M-BIS-E-RCL.EN