Study Course Title	***Security culture***
Study Course Code	VadZM089
Branch of Science	Economics and business
Sub-branch of science	Business management
Credits (ECTS)	**3**
Total Number of Contact Hours	**24**
Number of Lecture Hours	12
Number of Seminar and Practical Assignment Hours	12
Number of Hours for Laboratory Assignments	0
Independent Study Hours	**51**
Language of Instruction	Latvian and English
Course Approval Date	31.10.2025
Responsible Unit	BA School of Business and Finance of the University of Latvia

Study form	Lectures	Seminars and Practical Assignments	Laboratory Assignments	Independent Studies
Full-time Regular Studies	12	12	0	51
Distance learning	2	4	0	69

Course Developer

Mg. oec., doc. Tatjana Mavrenko

Prerequisite Knowledge

Prerequisite knowledge required for the acquisition of the course corresponds to the study programme admission requirements and the general knowledge, skills and competences obtained at the previous level of education.

Study Course Abstract

In this course, students become acquainted with the definition of the concept of safety culture. Students learn the framework structure of the safety awareness training program. They identify quality requirements for the program content and conduct an analysis of success factors, including training levels, their complexity, target audience determination, as well as methods and tools. The aim of the course is to enhance students' understanding of the impact of employee behaviour, habits, and attitudes on ensuring information security.

Course Plan Full-time Regular Studies

1.Security culture (SC). 2L
2.Quality Requirements for the SC program content. 2L
3.Framework of the security awareness training program. 2S 2Pd
4.SC Success factors and their analysis. 4L 2S 2Pd
5.Training levels, their complexity, and target audience identification; SC Content, current topics, methods, and tools. 4L 4Pd
Total 12L 4S 8Pd

Course Plan Distance learning
1.Security culture (SC). 1L
2.Quality Requirements for the SC program content. 1S
3.Framework of the security awareness training program. 1S
4.SC Success factors and their analysis. 1Pd
5.Training levels, their complexity, and target audience identification; SC Content, current topics, methods, and tools. 1L 1Pd
Total 2L 2S 2Pd

Characterization of students' independent work organization and tasks

Students prepare for discussions, participate in seminars and case analysis discussions, develop and present individual and group practical assignments, and prepare for the examination

Learning Outcomes
Knowledge:
1. Understands the concepts, definitions, and objectives of safety culture.

Skills:
2.Is able to independently identify and critically analyse cybersecurity-related risks, as well as determine, plan, and monitor the outcomes aimed at risk mitigation;
3.Is capable of developing and implementing innovations and improvements at the operational, tactical, and strategic levels of cybersecurity management, providing consultation, explaining, and justifying information security management objectives and outcomes to stakeholders (both specialists and non-specialists).

Competence:

4.Is able to identify and anticipate learning needs, integrate knowledge from various fields, and contribute to the creation of new knowledge;
5.Is capable of advancing their own and others’ cybersecurity competencies, taking responsibility for the work outcomes of personnel groups, and conducting research and continuous learning in complex and unpredictable business environments;
6.Is able to develop, plan, and monitor information protection measures at the levels of processes, technologies, and human behaviour, ensuring the effectiveness of these measures.

Requirements for Awarding Credits
Interim Assessments:
1. Discussions and practical work in the classroom — Weight in the overall grade: 20%
2. Group work in the classroom — Weight in the overall grade: 25%
3. Development and presentation of independent work — Weight in the overall grade: 40%

Final Examination:
Examination: The exam is graded on a 10-point scale. It accounts for 15% of the overall grade.

The interim assessments are graded on a 10-point scale

Criteria for Evaluating Learning Outcomes

In accordance with Regulations of the Cabinet of Ministers of the Republic of Latvia, at the end of the course, students' knowledge is evaluated according to the following criteria: the amount and the quality of the obtained knowledge, acquired skills and competence in compliance with the planned learning outcomes.

Type of Assessment	Learning Outcomes					
	1	2	3	4	5	6
1. Discussions	+	+	+	-	-	+
2. Practical work in the classroom	-	+	+	-	+	+

3. Independent work and presentation	-	+	+	+	-	+
4. Written exam	+	+	+	+	+	+

Compulsory Reading List

1.Roer.K. "Build a security culture?" ITG, 2015

Further Reading List

1.Privacy and Cybersecurity resources by ISACA:
http://www.symantec.com/products-solutions/training/theme.jsp?themeid=ssap
2. Computer Security Resource Centre https://csrc.nist.gov/publications/draft-pubs

Plagiarism and other academic misconducts are not permitted within the course please refer to the Regulations for Academic Integrity at the University of Latvia. Within this course, the use of generative artificial intelligence (AI) tools is allowed in exceptional cases, if it has been specified and authorised in writing by the instructor of this course. In all other cases, submission of materials generated by the AI (text, images, audio, video, etc.) in independent and group assignments, test, examination or any other assessment is not permitted, submission of this type of material will be considered an unauthorised use of aids.