

Professional Master's degree program "Cybersecurity Management"

<b>Study Course Title</b>	<b>Organizational theory</b>
<b>Study Course Code</b>	VadZM096
<b>Branch of Science</b>	Economics and business
<b>Sub-branch of science</b>	Business management
<b>Credits (ECTS)</b>	<b>6</b>
<b>Total Number of Contact Hours</b>	<b>48</b>
<b>Number of Lecture Hours</b>	10
<b>Number of Seminar and Practical Assignment Hours</b>	38
<b>Number of Hours for Laboratory Assignments</b>	0
<b>Independent Study Hours</b>	<b>102</b>
<b>Language of Instruction</b>	Latvian and English
<b>Course Approval Date</b>	22.09.2025
<b>Responsible Unit</b>	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	10	38	0	102
Distance learning	6	6	0	138

**Course Developer**

Dr. oec., prof. Tatjana Volkova

**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**

Study course promotes understanding of business continuity planning, as well as actions during business restructuring and reorganization situations. Understands decision-making algorithms. The aim of this course is to provide a theoretical foundation and knowledge about the competencies of an information security incident response team and team leadership. It also promotes understanding of business continuity planning within an organization.

**Course Plan Full-time Regular Studies**

- 1.Organizational performance criteria. Linking information security incident response plans with the company's business continuity planning. 2L
- 2.Formation of crisis and emergency response teams 4Pd
- 3.Ensuring information security requirements in outsourcing, information security culture 2L
- 4.Corporate governance. Stakeholders and business performance. Stakeholder impact analysis matrix. Governance mechanisms 2L
- 5.Agency theory. The role of the supervisory board in ensuring cybersecurity. Cyber ethics 2L 2S

6. Business planning and influencing factors. Integration of information security incident response plans with the company's disaster recovery planning (DRP) and business continuity planning (BCP) 4Pd
  - 7.Groups and teams. Fundamentals of individual behaviour. Group and team leadership. Organizing, training, and equipping groups to respond to information security incidents 2S 4Pd
  - 8.Business structure design. Aligning structure with business objectives. Basic structural forms. Restructuring and reorganization 2S 4Pd
  - 9.Managing resistance to change. Integration of information security controls into employment contracts 2S 6Pd
  - 10.Decision-making regarding the development and implementation of an information security (IS) assurance program. The decision-making process. Decision-making biases and guidelines for effective decision-making 2L 4Pd
  - 11.Development of programs for information security awareness, training, and stakeholder education. 4Pd
- Total 10L 8S 30Pd

**Course Plan Distance learning**

- 1.Organizational performance criteria. Linking information security incident response plans with the company's business continuity planning. 1L
- 2.Formation of crisis and emergency response teams 1Pd
- 3.Ensuring information security requirements in outsourcing, information security culture 1L
- 4.Corporate governance. Stakeholders and business performance. Stakeholder impact analysis matrix. Governance mechanisms 1L
- 5.Agency theory. The role of the supervisory board in ensuring cybersecurity. Cyber ethics 1L 1S
6. Business planning and influencing factors. Integration of information security incident response plans with the company's disaster recovery planning (DRP) and business continuity planning (BCP) 1Pd
- 7.Groups and teams. Fundamentals of individual behaviour. Group and team leadership. Organizing, training, and equipping groups to respond to information security incidents 1S
- 8.Business structure design. Aligning structure with business objectives. Basic structural forms. Restructuring and reorganization 1Pd
- 9.Managing resistance to change. Integration of information security

controls into employment contracts 1Pd  
 10. Decision-making regarding the development and implementation of an information security (IS) assurance program. The decision-making process. Decision-making biases and guidelines for effective decision-making 1L  
 11. Development of programs for information security awareness, training, and stakeholder education. 1L  
 Total 6L 2S 4Pd

**Characterization of students' independent work organization and tasks**

Students prepare for discussions, participate in seminars and situational analysis discussions, develop and present individual and group practical assignments, and prepare for the exam.

**Learning Outcomes**

Knowledge:

1. Knows and understands information security management issues and their impact on a company's/organization's competitiveness, development, stability, and sustainable operations.

Skills:

2. Can develop and implement innovations and improvements at the operational, tactical, and strategic levels of cybersecurity management.

Competence:

3. Can promote the development of their own and others' cybersecurity competencies, take responsibility for the performance of personnel groups, and conduct research and further learning in complex and unpredictable business environments.

**Requirements for Awarding Credits**

Interim Assessments:

1. Classroom discussions and practical assignments – 20% of the final grade
2. Group work in class – 20% of the final grade
3. Individual project development and presentation – 45% of the final grade

Final exam:

4. Exam. Weight in the overall grade: 15%.

The assessment is 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
1. Discussions	+	+	+
2. Practical work in the classroom	-	+	+
3. Independent work and presentation	+	+	+
4. Written exam	+	+	+

**Compulsory Reading List**

## Professional Master's degree program "Cybersecurity Management"

- 1.(2023) Blomberg Jesper Organization Theory: Management and Leadership analysis, Sage publishing.
2. (2014) Touhill, Gregory J. And Joseph Touhill Cybersecurity for Executives: a practical guide. American Institute for Chemical Engineering. (pp. 125-196)
3. (2018) Jalali et al. Decision making and biases in cybersecurity capability development: evidence form a simulation game experiment in Journal of Strategic Information Systems.
4. (2021) Joyce, S. Principles for Board Governance of Cyber risk. Harvard Law School Forum on Corporate Governance, <https://corpgov.law.harvard.edu/2021/06/10/principles-for-board-governance-of-cyber-risk/>
- 5.(2017) Advancing Cyber Resilience Principles and Tools for Boards, WEF.

### **Further Reading List**

- 1.(2015) The Cyberresilient enterprise: What the Board of Directors needs to ask. ISACA, Cybersecurity Nexus. Roam
2. (2019) Cybersecurity: moving from anchor to enabler of innovation. EY
3. (2018) Goosen et al. AI is a threat to CS. It's also a solution. BCG
4. (2014) Reporting CS to the Board. BitSight.
5. (2015) The Cybersecurity literacy confidence gap. Tripwire.
6. Hiscox Cyber Readiness Report (2021).  
<https://www.hiscox.co.uk/sites/default/files/documents/2021-04/21486-Hiscox-Cyber-Readiness-Report-2021-UK.pdf>

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.