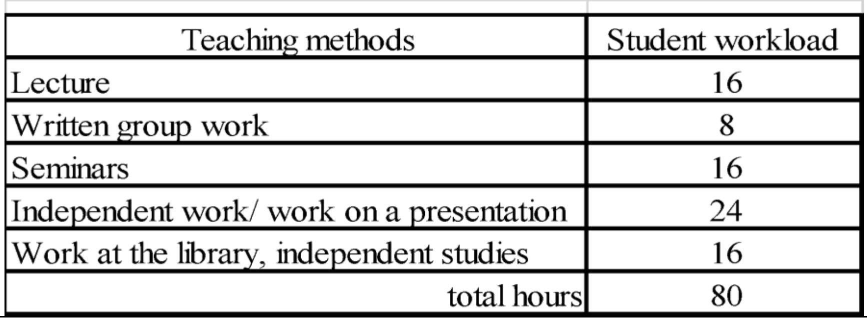
DESCRIPTION OF STUDY COURSE

<table>
<tr><td><b>Course unit title</b></td><td><b>Security Culture</b></td></tr>
<tr><td><b>Programme</b></td><td>MBA in Cybersecurity Management</td></tr>
<tr><td><b>Year of study</b></td><td><b>2</b></td></tr>
<tr><td><b>Academic year</b></td><td>2022/2023</td></tr>
<tr><td><b>Level of course unit (e.g. first, second or third cycle)</b></td><td>2nd cycle</td></tr>
<tr><td><b>Course unit code</b></td><td>MKP001</td></tr>
<tr><td><b>Name of lecturer(s)</b></td><td>Sintija Deruma</td></tr>
<tr><td><b>Number of ECTS credits allocated</b></td><td>3 ECTS
2 Latvian credit points are multiplied by 1,5 to get ECTS credit points</td></tr>
<tr><td><b>Credit points</b></td><td>2 CP</td></tr>
<tr><td><b>Module</b></td><td>Management</td></tr>
<tr><td><b>Language of instruction</b></td><td>English and Latvian</td></tr>
<tr><td><b>Type of course unit (compulsory, optional)</b></td><td>optional</td></tr>
<tr><td><b>Mode of delivery</b></td><td>In person or online</td></tr>
<tr><td><b>Aim of Course</b></td><td>The aim of the course is to increase students' understanding of the impact of employee behavior, habits and attitudes in ensuring information security</td></tr>
<tr><td><b>Preliminary knowledge (prerequisites and co-requisites)</b></td><td>HR management</td></tr>
<tr><td><b>Course contents</b></td><td>~ security culture;
~ security awareness curriculum framework
~ quality requirements for the content of the program
~ success factor analysis:
~ training levels, their complexity, targeting
~ current topics, methods and tools</td></tr>
<tr><td><b>Planned learning activities and teaching methods</b></td><td>The student attends lectures, completes practical work, presents group and individual work.
The total evaluation of the course consists of: 30% group work in classroom setting; 20% practical work in classroom setting;20% group work completion and presentation; 30% individual work completion and presentation.

<table>
<tr><th>Teaching methods</th><th>Student workload</th></tr>
<tr><td>Lecture</td><td>16</td></tr>
<tr><td>Written group work</td><td>8</td></tr>
<tr><td>Seminars</td><td>16</td></tr>
<tr><td>Independent work/ work on a presentation</td><td>24</td></tr>
<tr><td>Work at the library, independent studies</td><td>16</td></tr>
<tr><td>total hours</td><td>80</td></tr>
</table></td></tr>
<tr><td><b>Learning outcomes of the course unit</b></td><td>Knowledge of human resource management functions and theoretical foundations; understanding of operational human resource management processes: planning, selection, performance management, motivation and</td></tr>
</table>

<table>
<tr><td></td><td colspan="4">rewarding, employee training and development, analytical ability to apply human resource management skills in various organizations.

(s3) Is able to independently identify and critically analyze the risks related to cyber security, identify, plan and monitor the results to be achieved to reduce the risks;
(s4) Is able to develop and implement innovations, improvements at the operational, tactical and strategic levels of cybersecurity management;
(s5) Is able to cooperate, communicate, consult, explain and argue information security management objectives and results to stakeholders (professionals and non-specialists);
(c6) Is able to identify and anticipate learning needs, integrate knowledge from different fields, contribute to the creation of new knowledge;
(c7) Is able to direct the development of one's own and other cyber security competencies, take responsibility for the results of the work of personnel groups, carry out research and further learning in complex and unpredictable conditions in the business environment;
(c8) Able to develop, plan, monitor information security measures, at the levels of processes, technologies and human behavior, ensuring the effectiveness of measures.</td></tr>
<tr><td rowspan="5">**Assessment methods and criteria**</td><td>**Learning outcomes**
The form of assessment</td><td>1.</td><td>2.</td><td>3.</td></tr>
<tr><td>Written work in a classroom</td><td>●</td><td>●</td><td></td></tr>
<tr><td>Group work in a classroom</td><td></td><td>●</td><td>●</td></tr>
<tr><td>Independent work and its presentation</td><td></td><td>●</td><td>●</td></tr>
<tr><td>Written examination</td><td>●</td><td>●</td><td>●</td></tr>
<tr><td>**Study course calendar plan**</td><td>Lesson 1</td><td colspan="3">security culture (SC); quality requirements for the content of the SC program</td></tr>
<tr><td></td><td>Lesson 2</td><td colspan="3">security awareness curriculum framework</td></tr>
<tr><td></td><td>Lesson 3</td><td colspan="3">SC success factors, their analysis
training levels, their complexity, targeting;</td></tr>
<tr><td></td><td>Lesson 4</td><td colspan="3">SC content, current topics, methods and tools.</td></tr>
<tr><td>**Recommended or required reading**</td><td colspan="4">https://securitycultureframework.net/
http://www.securementem.com/wp-content/uploads/2013/07/Habits_white_paper.pdf
http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
http://www.isaca.org/Knowledge-Center/Research/Pages/Cybersecurity.aspx
http://www.isaca.org/Knowledge-Center/Research/Pages/Privacy.aspx
http://predragtasevski.com/wp-content/uploads/Tasevski_ICSAP.pdf Interactive Cybersecurity Awareness program</td></tr>
<tr><td>**Recommended optional programme components**</td><td colspan="4">To be agreed at the start of the course.</td></tr>
</table>