COURSE UNIT (MODULE) DESCRIPTION

Course unit (module) title	Code
INFORMATION SECURITY AND RISK MANAGEMENT	

Academic staff	Core academic unit(s)
Coordinating: dr. Renata Danielienė **Other:**	Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics, Muitinės str. 8, LT-44280, Kaunas

Study cycle	Type of the course unit
First (bachelor)	Compulsory

Mode of delivery	Semester or period when it is delivered	Language of instruction
Auditorium	4 semester	English

Requisites	
Prerequisites: The student should have completed: Basics of Information Systems Security, Requirements Analysis and Specification for IS, Information Systems and Databases, Legal Regulation of Cyber Security, English level B1–B2.	**Co-requisites (if relevant):** The student may have completed: Operating Systems and their Security, Data Security and Cryptography, Secure Programming, Electronic Payments and their Security.

Number of ECTS credits allocated	Student’s workload (total)	Contact hours	Individual work
5	**130**	**52**	**78**

Purpose of the course unit
To provide students with skills needed for strategic information security management. This involves learning to identify, assess, monitor, and manage risks based on international professional standards like CISM and CRISC. The module is designed to teach how to identify an organization's critical assets, analyze cyber threats and vulnerabilities, and prepare an incident management plan and risk management strategy to ensure business continuity and resilience.

Learning outcomes of the course unit	Teaching and learning methods	Assessment methods
Identify all IT and critical assets of an organization, assess related risks, and define security requirements.	Problem-based teaching using the Flipped Classroom method (independent study of theory and practical application in class), Case Study analysis, group work, interactive workshops, discussions, situation modeling, and cyber incident simulations.	Cumulative assessment: moderation of interactive workshops (instead of simple theory presentation), defense of practical work (reasoned presentation of results), instant analysis during written work presentations, discussion reports (analysis of real cyber incidents), midterm test, and situation simulation/exam.
Apply modern standards and methods in information security management and risk management processes.		
Formulate an organization's cyber security strategy and apply it systematically to ensure organizational resilience.		

Content	Contact hours							Individual work: time and assignments	
	Lectures	Tutorials	Seminars	Workshop	Laborator y work	Internship	**Contact hours,**	**Individua l work**	**Tasks for individual work**
Introduction to risk management. Key terms and definitions of security risk management.	2			2			**4**	**3**	Independent analysis of video material and literature before each lecture. This is required for successful participation in TK tasks. Consistent analysis of a chosen organization (Modules M2-M8), data collection, application of methods, and report writing. Role distribution in the group, cooperation, and leadership planning. Preparation and rehearsal of interactive tasks for the audience (when the group is leading). Analysis of cyber attack examples, theory, and written work in preparation for the midterm test and final exam (simulation).
Threat Modeling and vulnerability analysis.	2			2			**4**	**3**	
Critical business systems. Asset management and Business Impact Analysis (BIA).	2			2			**4**	**6**	
Cyber risk management, leadership impact, and management responsibility.	2			2			**4**	**6**	
Risk mitigation controls: technical and administrative.	2			2			**4**	**6**	
Compliance, GDPR, and third-party (supplier) risk.	2			2			**4**	**6**	
Incident management and business continuity.	2			2			**4**	**6**	
Forming cyber security culture and cyber strategic management.	2			2			**4**	**6**	
Midterm assessment (test).				8			**8**	**16**	
Case studies of cyber attacks, discussions, and summary.				8			**8**	**4**	
Refining group work, consultations.		4					**4**	**0**	
Exam, consultations.							**0**	**16**	
Total:	**16**	**4**		**32**			**52**	**78**	

Assessment strategy	Weight %	Deadline	Assessment criteria
Discussions on Cyber Cases (D)	18%	During practical classes at set times.	Tasks must be completed on time and with high quality (during practical classes), supported by reliable sources and well-argued answers (each task is graded from 0 to 10). **Discussion Assessment Strategy.** We assess activity, insights, how well arguments are supported, critical thinking, use of sources, quality of descriptions, and the number of discussion tasks (active participation in 6 discussions). Students must follow the lecturer's instructions. Thoughts must be clear. Answers must be relevant to the case analysis and the question asked. Answers must be specific, not general or unrelated to the situation. Rules for citation and using AI (Artificial Intelligence) generative models are described below the table. The introductory discussion is not graded. Every subsequent discussion has equal weight (3% each). **You do not need to prepare for discussions in advance.** **Work Organization.** Discussions take place during lectures **in temporary groups**. The group members can change each time, depending on how many students attend, ensuring there are at least 4 students in a group. Only the contribution of students physically present in the discussion is assessed. **Preparation and Submission of Discussion Summaries.** Each group prepares one document. In this document, each member answers the questions asked **during the class and presents their summarized insights.** Only the names of students who were physically present and made a real contribution should be listed at the top of the document. If the lecturer notices that a student is obviously not participating (e.g., constantly looking at their phone, being passive), the lecturer has the right to cancel that student's score, even if their name is on the document. Each student must write their name and surname next to their answer. If a student does not submit their written insights from the discussion according to the criteria, their work for that class will not be counted. One group member uploads the discussion summary to the eLearning environment (eMokymai) before the end of the lecture. Work uploaded after the deadline is not graded. Discussions are only for students attending in person. Therefore, a summary (or part of it) is not graded if the student did not attend in person. Written insights must follow the instructions given by the lecturer during each practical class. **Use of Sources.** When answering each discussion question, you must provide at least two reliable external sources (AI tools do not count as sources). To ensure a complete analysis, the group must use a variety of sources. Group members must coordinate their search so that sources do not repeat and complement each other. If it is noticed that all group members use the same 1-2 sources for different answers, ignoring other important information, the grade for the whole group will be reduced. At least two reliable external sources must be provided for each answer**. Links must be active and work at the time of checking.** Non-existent sources generated by AI are considered a violation of academic integrity, and the task will be graded 0. If the

			work lacks sources or uses non-existent sources to support facts, the grade will be reduced.
Theory Application (TK)	10%	During practical classes (throughout the semester)	**Individual short tasks („instant analysis“)** are performed in the Moodle environment during presentations by other groups. The questions check if the student listened to the defense and if they can link the presented practice with the theory provided by the lecturer. It is graded individually on a **“Pass / Fail” basis (1 or 0)**. This grade does not affect the presenting group's grade; it is a personal score for the student for active listening, analysis, and understanding the context of the presented topic. A student who did not attend the group assignment presentations/workshops in person technically cannot complete the task.
Test (T)	30%	Fixed time during the semester	**The Test** is taken by physically arriving at the specified time in the VU Kaunas Faculty classroom indicated by the lecturer. The test questions requires not just the recall of theoretical knowledge, but synthesis: the ability to apply models presented in theoretical videos to practical situations analyzed during group discussions (D). **Test Format.** Various types of questions are presented (multiple choice, matching, sequence ordering, etc.). There is no possibility to go back to a previous question, and the test time is fixed. The test cannot be taken remotely. If a student fails to attend the test without an official valid reason, the exam grade is recorded as 0. **Academic Integrity.** To ensure integrity, students take the test using only the computers in the classroom. During the assessment, student screens may be monitored and recorded. The use of any additional material, smart devices (phones, watches, headphones), or AI tools is strictly prohibited. All personal devices must be turned off and placed in the designated area (not on the table or in pockets) during the assessment. If any violation of academic integrity is noticed, the test is terminated and graded as 0. The administration is informed about the academic integrity violation, and a review by the ethics committee may be initiated.
Exam (E)	20%	During the exam session.	**The Exam** is taken by physically arriving at the designated VU Kaunas Faculty classroom at the scheduled time during the exam session. **The exam** is conducted as a real-time interactive incident management simulation (e.g., based on a cyber incident scenario). This is not a standard theory check, but an assessment of each student's ability to make decisions in a crisis situation. **Grading.** Only individual student decisions submitted in the Moodle system in real-time are assessed. The questions are complex (e.g., situational, priority setting, sequencing), requiring synthesis—the ability to quickly link the entire semester's theoretical knowledge (law, management, technical security) with a specific crisis situation. **Academic Integrity.** During the exam, students use only the classroom computers. During the assessment, student screens may be monitored and recorded. It is strictly forbidden to consult with colleagues while submitting answers, or to use phones or AI tools. Any attempt to cheat or coordinate answers is graded as 0. The administration is informed about the academic integrity violation, and a review by the ethics committee may be initiated.

Group Work (G)	22%	At the appointed time of the semester	During the semester, **8 student groups** are formed. The standard group size is **8 students**. If there are more than 56 students, a group may have 7 students with the lecturer's approval. In order to ensure an even distribution of workload, all 8 groups must be formed, and no group may have fewer than 5 students. At the start of the semester, the lecturer publishes the tasks for all groups for the entire semester and provides a **schedule for presenting work**. Each group presents their work according to the schedule. All group work must be presented by the **second-to-last lecture** of the semester. Submissions late for the very last lecture are not accepted. **Group work consists of several tasks (total 22%):** **(Teor=8%)** Conducting an interactive **workshop** on theoretical material on a specified topic according to the assigned task. **(R=14%)** Preparing a **written assignment** and conducting a **workshop** on a specified topic according to the assigned task. Content (4%) and defense quality (10%) are assessed. **Leadership Rotation.** To develop management skills, we use a **leader rotation principle**. For each different task (theory and written assignment workshops), the group must delegate leaders. The **same student cannot be the main leader for both tasks**. If a student has not been a group leader at least once during the semester, their own group work grade is reduced by **1 point**. The student group must evaluate the situation: if there are fewer students than tasks, students must plan **co-leadership** so there are no excuses regarding this issue at the end of the semester. Considering the size of the written assignment, its defense, and the group size (4–5 students), two **Co-leads** can be assigned for this task. In this case, responsibilities must be shared (e.g., one is responsible for document quality and source control, the other for moderating the defense and uploading the work). Both co-leads accept **equal responsibility** for the final result and meeting deadlines. **Planning Responsibility.** The group must independently plan the leadership rotation at the start of the semester. If the number of group members does not match the number of tasks (e.g., fewer members than tasks), students must apply the **Co-leads** model or rotate repeatedly. Arguments about poor planning will not be accepted on the last day of the semester – if the leadership requirement is not met, the planned grade reduction applies. **Leaders** and group members participating in the presentation **in person** are listed on the title page of the work (failure to follow this instruction results in a **-1 point** reduction). If there is a member who prepared the written assignment but is not participating in the presentation, this must be listed separately and highlighted on the first page (e.g., name and surname written with the note “**Does not participate in defense**”). **Main Leader Responsibilities.** The main leader uploads the work to the **eLearning (eMokymai)** system and introduces the team. The status of Group Leader (or Co-leaders) is only credited if they actually performed leader functions: **Uploading work.** Only work uploaded in the leader's account is graded.

			Moderation. During the defense, the leader must introduce the team, manage the time limit, and distribute audience questions to the appropriate members. If the leader is silent during the defense or allows chaos to arise, the leadership score is cancelled (**-2 points**). **Contribution Declaration.** If group members assign the leader a **lower than average percentage score** in the contribution table, the leadership is considered fictitious, and the leader's score is not awarded. **Presentation Quality and “No-Text Slides” Requirement.** To develop management skills that meet market needs, the following presentation assessment criteria apply: **Visual Content.** Students must prepare **visual slides** (diagrams, schemes, key points with no more than **5-7 words**). Slides dominated by continuous text (paragraphs) are evaluated as poorly prepared handouts, not a presentation. Presentations generated with AI (e.g., “Gamma” style generic texts) are not credited. **Speaking Style.** Top grades are given only to presentations where students maintain contact with the audience and **speak freely** (short notes can be used, but the full text is not read from notes, a phone, or a computer screen). **Reading Assessment.** If a student constantly reads text (from slides, phone, or paper) during the presentation and cannot express thoughts independently, their individual defense grade cannot exceed **50% (i.e., 5 points)**. This is assessed as a lack of preparation or misunderstanding of the topic. **Exceptions.** Students with a fear of public speaking or special needs must inform the lecturer about **this in the beginning of the semester.** **Assessment of Group Member Contribution.** A table with the percentage contribution of each group member is mandatory in every work. The final grade is individualized based on this contribution. If it is indicated that a member did not contribute (0%), they receive a **0** for the task. **Participation in Defense/Workshops.** Only the contribution of students participating **in person** is assessed. During presentations, each group member presents their part and answers questions asked by the audience from their part. If a student does not participate in the defense/workshop, they lose the defense/workshop conduct score; only the content part of the written assignment is counted for them (if they had a contribution there). Group works are defended **only once** according to the schedule. “Repeat” defenses for defense/practical workshop group members are not organized. Also, one group cannot defend the same work multiple times by splitting group members into several parts. **Continuity of Written Assignment Analysis and Data Integrity.** Since several groups analyze the same organization during the semester, the **data inheritance principle** applies. When preparing their part (e.g., M4), the group **must familiarize themselves** with the analysis of the same organization performed by previous groups (e.g., M2, M3). It is unacceptable to ignore the previously established context or contradict it without arguments (e.g., changing the list of critical assets without justification). If the group notices that the previous analysis was superficial or

			incorrect, they must correct it in their work, clearly stating the arguments for the correction (“**opposing”**). **Duplication.** Information must not be blindly copied; it must be **expanded and deepened** according to the topic of the new module. **When presenting theoretical material**, students must use **examples of the latest cyber incidents** (using examples older than 5 years reduces the grade by **2 points**). All subtopics of the topic specified by the lecturer must be presented and explained in detail. **The text of the written assignment** must be consistent and specific, specifically answering the questions asked, not using generalizing sentences, achieving the minimum word count specified in the tasks, etc. **Quality, Source, and AI Requirements.** **Content.** The text must be consistent, specific, and answer the questions. General sentences (e.g., generated by AI) are not graded. **AI Use.** You cannot submit AI-generated text without authorial analysis and adaptation. If obvious AI signs are noticed (hallucinations, terminology not typical for the course, non-existent sources), the work is graded **0**. **Sources.** It is mandatory to indicate **exact sources** (with pages or chapters). At least **two reliable sources** must be provided for each answer. A list of sources without links in the text is considered invalid. **Hallucinations.** Non-existent sources generated by AI are an academic integrity violation (**grade 0**). To ensure academic integrity, **oral presentations of the theoretical part and written assignment are recorded** and stored during the semester and session. **The duration of one presentation** must be no less than **30 minutes**; together with answers to questions, it must be no less than **40 minutes**. Presenting for less than 30 minutes is considered as not examining and presenting the topic in enough detail, and this accordingly affects the entire presentation score. **Lateness.** If a group does not present work according to the schedule, the score is reduced for **all group members** for each week of delay (**-2 points** for each missed week). All written assignment and theory presentations must be completed by the **second-to-last lecture inclusive**. Written assignments and theory presentations are not credited during the last lecture of the semester (or after the last lecture). **We assess** the quality and completeness of presentations and written assignments, whether the presented text is logical and clearly laid out, whether students are able to think critically, rely on theoretical material, draw conclusions, make suggestions, and answer the questions presented. The volume of the written assignment is also assessed (according to requirements specified in the task). **Text in written assignments cannot be copied from the internet and from AI.** **Descriptions must include sources** (indicating not only the source but also the page, if it is a report, or part of an internet article (e.g., a section)). Work is not accepted if it does not rely on sources or if sources are provided without indicating the location of that source (e.g., page, section). **Links must be active and work at the time of checking.**

			Sources must be indicated next to the relevant part where the source or multiple sources are used (if the list of sources is provided at the end of the document or presentation and sources are not used in the document or presentation, it is considered that the student did not rely on sources properly). If the work lacks sufficient sources to support the presented facts, the work evaluation is reduced accordingly. **Written assignments are mandatory** (all tasks must be graded with a mark of at least 5). Reports are prepared and assessed according to the lecturer's instructions, which are provided together with the written assignment. **Detailed features of using AI (Artificial Intelligence) generative models** are described below the table. **A detailed group work assessment strategy** is provided in the task descriptions.
A student's knowledge and skills are assessed during the exam session only if they have met the requirements and completed the tasks for intermediate assessment during the semester. Student knowledge and skills across all intermediate assessments and the exam are graded on a scale from 1 to 10. The course is passed if: The results of all intermediate assessments are not lower than 5; The exam grade is not lower than 5. **For full-time students**, the cumulative score formula applies: **0.18*D* + *0.30*T + 0.20*E* + *0.22*G** (where D = discussions, TK = theory application in class, T = test, E = exam, G = group work). **For students taking the exam as an EXTERNAL STUDENT** (officially coordinated with the faculty administration). Only students who have completed the written assignments scheduled for the semester and presented them can take the exam externally (at least 50% of all written assignments and presentations must be done during the semester on the days scheduled for the whole group). They must also have completed at least 50% of the discussion tasks (during the semester on the days scheduled for the whole group) and passed the theory test on the date and time assigned to the whole group during the semester. The final score is calculated using the cumulative score formula principle (**0.20*D* + *0.30*T + 0.2*E* + *0.30*G**, where D = participation in discussions, T = theory test during the semester, E = exam test/scenario, and G = group work). Retaking the test is not possible. The assessment schedule for students is published in the eLearning (eMokymai) environment during the first lecture. **Non-attendance and valid reasons.** A student who misses an assessment due to an important, documented reason (e.g., illness) must inform the lecturer in advance. A student who does not attend a group defense, discussion, or theory application assessment (ITK) without a valid reason receives a grade of 0 for the missed part of the assessment.			

When preparing assignments, the student may use external help: teaching material, reliable internet sources, and AI generative models, ensuring that the student adheres to the principles of academic integrity (the Copy-Paste principle is considered plagiarism, or citation must be used; see more below).

Examples of using AI generative models: it is best to use such tools for:

- generating ideas,
- creating structure,
- explaining concepts,
- searching for specific cases,
- generating summaries (for further work),
- processing large texts (for further work),
- text analysis.

However, all generated information must be verified, and sources linking to external sources must be provided in the work to ensure proper citation (in any case, the Copy-Paste principle is considered plagiarism if not cited). It is also important to understand that AI generative models are not co-authors of the work.

More about VU academic integrity (especially pay attention to point 19): https://www.vu.lt/site_files/Akademines_etikos_kodeksas_suvestine_redakcija.pdf

When can AI generative models not be used in this course? These tools cannot be used:

- in written assignments and presentations (using the Copy-Paste principle) to present text without proper citation.
- to “beautify” text (this does not apply to machine translation tools like DeepL).

- while taking assessment tests during the semester and the exam.

If AI generative models were used when preparing work? If AI generative models were used to generate ideas when preparing a written assignment, the following must be described at the beginning of the written assignment:

- the strategy for using AI tools,
- what questions were asked,
- what result was obtained and what percentage of the obtained result was modified and adapted when preparing the work.

In the appendices, the queries (e.g., ChatGPT query: "...") and results (e.g., ChatGPT generated answer "...") must be provided, indicating the name, version, and date of use of the generative model.

More about citation: https://apastyle.apa.org/blog/how-to-cite-chatgpt, https://guides.library.uq.edu.au/referencing/chatgpt-and-generative-ai-tools

Also, the written assignment must describe the volume of text generated by AI tools used in the work.

If text is copied from generative model systems, it must be cited like any other source (more at https://plagiarismcheck.org/blog/what-is-the-acceptable-percentage-of-plagiarism/).

When using AI generative models, it is important that students critically evaluate the answers provided, adhere to the principle of ethics, ensure the information is accurate, and each student must ensure transparency towards other group members.

Important. In the case of academic dishonesty: if the lecturer notices signs of plagiarism or determines that the presented work contains blocks of text generated by artificial intelligence tools (i.e., suspected academic dishonesty), they inform the administration. In this case, a process is initiated in the faculty ethics committee to evaluate academic integrity.

Author (-s)	**Publishing year**	**Title**	**Issue of a periodical or volume of a publication**	**Publishing house or web link**
Required reading				
R. Danielienė	2026	Moodle aplinka		https://emokymai.vu.lt
Adarsh Nair and Greeshma M. R.	2023	Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance	9781803243160	Packt Publishing, Limited https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&query=risk%20management
Shobhit Mehta	2023	ISACA Certified in Risk and Information Systems Control (CRISC®) Exam Guide	9781803236902	Packt Publishing, Limited https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management
Gregory J. Falco, Eric Rosenbach	2021	Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity	9780197526545	Oxford university press, eBook
Peter H. Gregory	2021	CISM Certified Information Security Manager All-in-One Exam Guide	ISBN-10: 1264268319 ISBN-13: 9781264268313	McGraw-Hill
ISACA	2021	CRISC Review Manual 7th edition	ISBN-10 1604208503 ISBN-13 978-1604208504	ISACA

Dawn Dunkerley, Bobby E. Rogers	2015	CRISC Certified in Risk and Information Systems Control	9780071847 148	McGraw-Hill
Recommended reading				
Kristina Narvaez, Betty Simkins, John Fraser	2014	Implementing Enterprise Risk Management: Case Studies and Best Practices	9781118691 960	John Wiley & Sons
R.Vageris	2005	Rizikos analizės vadovas	ISBN 5-415- 01827-1	Vaga https://www.nksc.lt/doc/rizikos_analize.pdf
Egidijus Kazanavičius, Algimantas Venčkauskas, Agnius Liutkevičius, Arūnas Vrubliauskas	2008	Informacijos saugos vadyba	e. ISBN 978- 609-02- 0359-0	

Description updated – 14 November 2025