Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	**ANALISI E GESTIONE DEL RISCHIO**
Corso di studio	Magistrale sicurezza informatica Taranto
Anno Accademico	2023/2024
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	6 CFU
Settore Scientifico Disciplinare	SECS/S01
Lingua di erogazione	Italiano
Anno di corso	Primo
Periodo di erogazione	2° semestre
Obbligo di frequenza	No, ma la frequenza è fortemente raccomandata
Sito web del corso di studio	https://www.uniba.it/it/corsi/cdl-sicurezza-informatica-taranto

Docente/i

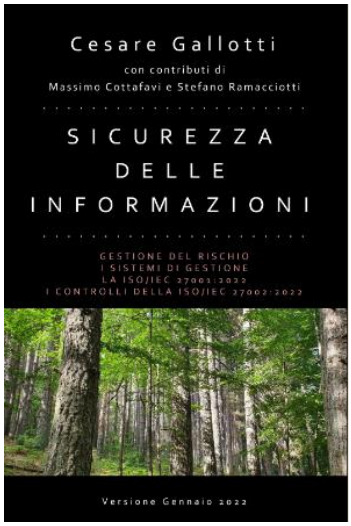
Nome e cognome	Angelo Leogrande
Indirizzo mail	Angelo.leogrande@uniba.it; angelo.economics@gmail.com
Telefono	370.1087760
Sede	Dipartimento di Informatica, Via Alcide de Gasperi
Sede virtuale	Piattaforma e-learning UNIBA - https://elearning.uniba.it/
Sito web del docente	
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Appuntamento per mail

Syllabus

<table>
<tr><td>Obiettivi formativi</td><td>L'insegnamento comprende l'identificazione del rischio e l'analisi del contesto, che comportano la valutazione degli asset, delle minacce e delle vulnerabilità all'interno di un'organizzazione. Inoltre, l'analisi del rischio viene affrontata sviluppando metodi sia quantitativi che qualitativi, includendo lo studio della variabilità, le analisi descrittive, di correlazione e inferenziali, nonché l'uso di test statistici per determinare il livello di rischio. Il trattamento del rischio si concentra sulla ponderazione e mitigazione dei rischi, attraverso l'implementazione di politiche di sicurezza e controlli adeguati. Infine, il corso esamina la governance e il management della sicurezza, analizzando l'organizzazione interna, le figure professionali coinvolte e i ruoli all'interno della struttura organizzativa per garantire una gestione efficace della sicurezza delle informazioni.</td></tr>
<tr><td>Prerequisiti</td><td>Buona comprensione della lingua inglese. Comprensione delle sfide per la sicurezza informatica poste dall’industria 4.0 e dall’attività di digitalizzazione. Riflessioni circa le condizioni di fragilità e sempre più frequenti black swan diffusi a livello locale ed internazionale come per esempio: crisi economiche, pandemie, guerre. Intuizione circa la differenza tra rischio oggettivo e rischio individuale nell’ambito della percezione dei rischi sia su fatti noti che su fatti ignoti.</td></tr>
<tr><td>Contenuti di insegnamento (Programma)</td><td>
<table>
<tr><th>Mod</th><th>Argomenti</th><th>Ore</th></tr>
<tr><td>Asset, Minacce e Vulnerabilità</td><td>Riconoscere e valutare gli asset, identificare le minacce e analizzare le vulnerabilità nel contesto della sicurezza delle informazioni.</td><td>5</td></tr>
<tr><td>Contesto Normativo</td><td>Comprendere gli standard rilevanti come l'ISO IEC 27001-213 e le normative connesse relative all'innovation management ed al risk management.</td><td>8</td></tr>
<tr><td>Metodi di Analisi</td><td>Utilizzo di metodi quantitativi e qualitativi per valutare i rischi, analizzare la loro variabilità e correlazione.</td><td>8</td></tr>
<tr><td>Analisi Inferenziali</td><td>Applicazione di test statistici per la determinazione e la previsione dei rischi.</td><td>8</td></tr>
<tr><td>Ponderazione e Mitigazione</td><td>Sviluppo di strategie per la ponderazione e mitigazione dei rischi identificati.</td><td>8</td></tr>
</table>
</td></tr>
</table>

Controlli di Sicurezza	Implementazione e monitoraggio dei controlli di sicurezza in linea con la politica di sicurezza dell'organizzazione.	6
Organizzazione e Ruoli	Definizione della struttura organizzativa, con specifici ruoli e responsabilità per la gestione della sicurezza delle informazioni.	5

Testi di riferimento



Gallotti, C. (2019). Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione per la sicurezza delle informazioni; la norma ISO/IEC 27001. Lulu. com.

Autore: Cesare Gallotti

Titolo: Sicurezza delle informazioni. Gestione del Rischio. I sistemi di Gestione. La ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022.

Disponibile in e-book sul sito dell'autore al link seguente: https://www.cesaregallotti.it/libro.html

Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.

Note ai testi di riferimento

Nel corso delle lezioni il docente utilizzerà delle slide che ripercorrono i contenuti del libro, pertanto non verranno fornite. Il testo di riferimento contiene tutti gli argomenti del corso, pertanto si consiglia di studiare dal testo e di svolgere in autonomia e costantemente tutti gli esercizi inseriti alla fine di ogni capitolo trattato a lezione.

Sulla piattaforma e-learning di Uniba (v. sopra 'sede virtuale') sono disponibili:
- materiale video di supporto utilizzato a lezione;
- alcune tracce di prove scritte di esami, con esempi di tracce svolte.

Molto rilevanti sono anche i riferimenti alle ISO che saranno resi disponibili dal docente.

Organizzazione della didattica

Ore

Totali	Didattica frontale	Laboratorio/esercitazione	Progetto	Studio individuale
150 ore	48 ore			102 ore
CFU/ETCS				
6 CFU	6 CFU			

Metodi didattici	
	Lezioni frontali, esercitazioni ed attività autonome e di gruppo in aula e a casa. Gli studenti non frequentanti possono lavorare singolarmente prendendo accordi con il docente.

Risultati di apprendimento previsti	
Conoscenza e capacità di comprensione	In primo luogo, gli studenti acquisiranno conoscenze matematiche, statistiche e informatiche, essenziali per comprendere e applicare gli strumenti tecnologici e computazionali nel contesto della gestione dei dati informatici. Inoltre, acquisiranno una comprensione approfondita degli strumenti di tecnologia dell'innovazione, applicata specificamente alla gestione delle informazioni.
Conoscenza e capacità di comprensione applicate	• Comprensione e applicazione degli strumenti di tecnologia dell'innovazione e computazionali nel contesto della gestione informatica ed informativa dei dati. • Capacità di utilizzare metodi matematici, statistici e informatici per analizzare e gestire i rischi in ambito informatico. • Sviluppo di capacità critiche nell'affrontare problematiche relative alla gestione delle informazioni, inclusa l'identificazione di minacce e vulnerabilità. • Acquisizione di abilità comunicative e rappresentative per descrivere e discutere gli elementi principali dell'analisi e gestione del rischio. • Capacità di apprendere sia i contenuti basilari che quelli complessi della materia, applicando tali conoscenze alla gestione pratica del rischio.
Competenze trasversali	**Autonomia di giudizio** • Valutazione critica del rischio: gli studenti acquisiscono la capacità di valutare criticamente i rischi identificati, comprendendo come questi possano influenzare l'organizzazione e sviluppando giudizi informati su quali rischi necessitano di mitigazione e quali possono essere accettati. • Applicazione delle normative e standard di sicurezza: attraverso lo studio del contesto normativo, gli studenti imparano a interpretare e applicare le

	normative e gli standard di sicurezza, sviluppando l'autonomia necessaria per giudicare l'adeguatezza delle politiche di sicurezza esistenti all'interno di un'organizzazione. • Sviluppo di soluzioni personalizzate: gli studenti sono in grado di sviluppare e proporre soluzioni personalizzate per la gestione del rischio, basandosi sulle specifiche esigenze dell'organizzazione e sull'analisi dettagliata dei contesti di rischio e delle vulnerabilità. **Abilità comunicative** • Capacità di comunicare in modo chiaro e preciso le problematiche relative alla gestione del rischio e le soluzioni proposte, utilizzando un linguaggio tecnico adeguato sia per esperti che per non specialisti. • Abilità nella rappresentazione visiva dei dati e dei risultati dell'analisi del rischio, attraverso l'uso di strumenti come presentazioni PowerPoint, grafici e diagrammi, per facilitare la comprensione e la discussione dei risultati ottenuti. • Competenza nel presentare e argomentare i principali aspetti dell'analisi del rischio in contesti accademici o professionali, supportando le proprie tesi con evidenze statistiche e normative appropriate. **Capacità di apprendere in modo autonomo** • Ricerca e aggiornamento continuo: gli studenti apprendono come mantenersi aggiornati sulle nuove normative, tecnologie e metodi di analisi del rischio, sviluppando la capacità di ricercare autonomamente risorse e materiali aggiuntivi per approfondire la propria conoscenza. • Applicazione autonoma di metodi analitici: gli studenti acquisiscono la capacità di applicare in modo indipendente metodi quantitativi e qualitativi di analisi del rischio, adattandoli alle specifiche esigenze e contesti che possono emergere nel proprio lavoro o studi futuri. • Sviluppo di soluzioni personalizzate: attraverso l'esperienza acquisita, gli studenti imparano a sviluppare e implementare soluzioni personalizzate per la gestione del rischio, basandosi sulla propria analisi critica e sulla comprensione del contesto organizzativo.

Valutazione	
Modalità di verifica dell'apprendimento	L'esame è scritto con una valutazione di controllo orale volta a verificare la comprensione generale dell'insorgenza dei rischi soprattutto in connessione con l'applicazione delle tecnologie dell'industria 4.0 all'interno delle imprese nell'ambito del processo di digitalizzazione e trasformazione digitale. L'esame scritto è composto da domande a risposta multipla e domande e risposta aperta. L'orale è volto anche a comprendere eventuali lacune emerse durante l'elaborato scritto.
Criteri di valutazione	**Conoscenza e capacità di comprensione:** • Conoscenze matematiche, statistiche e informatiche di base: forniscono la base per comprendere e applicare metodi quantitativi e qualitativi

nell'analisi del rischio, essenziali per valutare correttamente le minacce e le vulnerabilità all'interno di un'organizzazione.

- Capacità di utilizzare strumenti tecnologici e computazionali: gli studenti apprendono come applicare strumenti di tecnologia dell'innovazione nel contesto della gestione dei dati informatici, migliorando la loro capacità di analizzare e gestire informazioni complesse in modo efficiente.
- Sviluppo di capacità critiche nella gestione delle informazioni: il programma aiuta a sviluppare una comprensione critica delle problematiche legate alla gestione delle informazioni, permettendo agli studenti di identificare, analizzare e risolvere problemi complessi legati alla sicurezza informatica

Conoscenza e capacità di comprensione applicate:

- Applicazione di strumenti tecnologici e computazionali: gli studenti imparano ad utilizzare strumenti di Innovetion Technology e soluzioni computazionali per gestire e analizzare dati informatici, particolarmente nel contesto della sicurezza delle informazioni.
- Analisi critica delle problematiche di gestione delle informazioni: vengono sviluppate capacità critiche per identificare, analizzare e risolvere problematiche complesse legate alla gestione delle informazioni, considerando variabili di rischio e vulnerabilità all'interno di un'organizzazione.
- Sviluppo di abilità comunicative: gli studenti acquisiscono la capacità di comunicare e rappresentare efficacemente i risultati dell'analisi e gestione del rischio, utilizzando metodologie appropriate e strumenti di presentazione per condividere le proprie conclusioni in modo chiaro e preciso

Autonomia di giudizio:

- Valutazione critica delle situazioni di rischio: gli studenti imparano a identificare e valutare autonomamente i rischi, utilizzando sia metodi quantitativi che qualitativi. Questo permette loro di formulare giudizi informati sulle minacce e vulnerabilità che possono influenzare un'organizzazione.
- Applicazione indipendente delle normative e degli standard: lo studio delle normative e degli standard internazionali (come ISO/IEC 27001) fornisce agli studenti la capacità di giudicare l'adeguatezza delle politiche di sicurezza esistenti e di sviluppare raccomandazioni per miglioramenti, basandosi su un'analisi autonoma.
- Elaborazione di strategie di mitigazione del rischio: gli studenti acquisiscono la competenza per decidere autonomamente quali strategie di mitigazione siano più appropriate in base al contesto specifico, ponderando diversi fattori come la probabilità e l'impatto dei rischi.

Abilità comunicative:

- Capacità di esprimere concetti complessi in modo chiaro e comprensibile: gli studenti imparano a comunicare in modo efficace i risultati dell'analisi del rischio, sia a esperti del settore che a persone non specializzate, adattando il linguaggio e la presentazione alle diverse esigenze del pubblico.
- Competenza nell'uso di strumenti visivi per la rappresentazione dei dati: il programma insegna agli studenti come utilizzare strumenti di presentazione come PowerPoint per creare grafici, tabelle e diagrammi che rappresentano visualmente i dati e le conclusioni delle loro analisi, facilitando la comprensione e l'impatto della loro comunicazione.
- Sviluppo di abilità di presentazione orale: attraverso l'uso di presentazioni e discussioni durante le lezioni, gli studenti migliorano le loro capacità di

presentazione orale, imparando a esporre in modo strutturato e persuasivo i loro risultati e le loro proposte di gestione del rischio

Capacità di apprendere:

- Capacità di apprendere autonomamente nuovi concetti: Gli studenti sviluppano la competenza di apprendere sia contenuti basilari che complessi della materia in modo indipendente, sfruttando le risorse disponibili per approfondire le conoscenze acquisite durante il corso.
- Adattamento e applicazione di nuove conoscenze: Il programma incoraggia gli studenti a integrare e applicare in modo flessibile le nuove conoscenze acquisite, utilizzando metodi analitici avanzati e strumenti tecnologici per risolvere problemi concreti nel contesto della gestione del rischio.
- Capacità di aggiornarsi continuamente: Gli studenti imparano a rimanere aggiornati su nuove normative, standard di sicurezza e tecnologie emergenti, sviluppando una mentalità di apprendimento continuo che è essenziale in un campo in rapida evoluzione come la sicurezza informatica.

Criteri di misurazione dell'apprendimento e di attribuzione del voto finale

Voto	Descrittori
< 18 insufficiente	Conoscenze frammentarie e superficiali dei contenuti, errori nell'applicare i concetti, descrizione carente.
18 - 20	Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell'applicazione di concetti teorici.
21 - 23	Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice.
24 - 25	Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato.
26 - 27	Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta.
28 - 29	Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta.
30 30 e lode	Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione.

Altro

Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea
- https://www.uniba.it/it/ricerca/dipartimenti/informatica
- https://elearning.uniba.it/

I programmi di tutti gli insegnamenti sono disponibili al seguente link:

- https://elearning.uniba.it/

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei regolamenti didattici dei Corsi di Studi disponibili nel sito:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

Main information on the course

Course name	Risk Analysis and Management
Degree	Cybersecurity, Taranto
Academic year	2024/25
European Credit Transfer and Accumulation System (ECTS), in Italian Crediti Formativi Universitari (CFU)	6
Settore Scientifico Disciplinare	SECS/S01
Course language	Italian
Course year	First
Course period	Second Semester
Course attendance requirement	It is highly recommended to attend classes
Website of the Degree	https://www.uniba.it/it/corsi/cdl-sicurezza-informatica-taranto

Teacher(s)

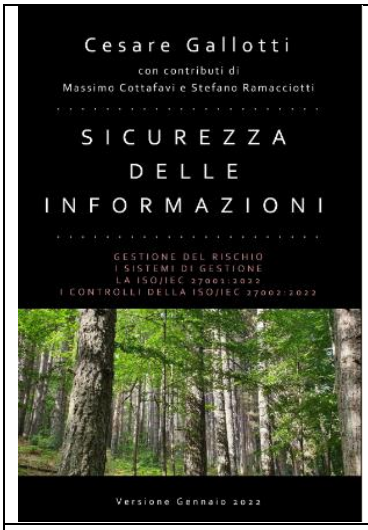
Name and Surname	Angelo Leogrande
email	Angelo.leogrande@uniba.it; angelo.economics@gmail.com
phone	370.1087760
office	Dipartimento di Informatica, Via Alcide de Gasperi, Taranto
e-learning platform	https://elearning.uniba.it/
Teacher's homepage	
Office hours	Appointment by email

Syllabus

Course goals	The course includes risk identification and context analysis, which involve assessing assets, threats, and vulnerabilities within an organization. Additionally, risk analysis is addressed by developing both quantitative and qualitative methods, including the study of variability, descriptive analyses, correlation and inferential analyses, as well as the use of statistical tests to determine the level of risk. Risk management focuses on the weighting and mitigation of risks through the implementation of appropriate security policies and controls. Finally, the course examines security governance and management, analyzing the internal organization, the involved professional roles, and the positions within the organizational structure to ensure effective information security management.
Prerequisites/requirements	Good understanding of the English language. Understanding of the cybersecurity challenges posed by Industry 4.0 and digitalization activities. Reflections on the conditions of fragility and increasingly frequent black swan events on both local and international levels, such as economic crises, pandemics, and wars. Insight into the difference between objective risk and individual risk in the context of risk perception, both for known and unknown events.
Course program	

Mod	**Argomenti**	**Ore**

	Asset, Minacce e Vulnerabilità	Riconoscere e valutare gli asset, identificare le minacce e analizzare le vulnerabilità nel contesto della sicurezza delle informazioni.	5	
	Contesto Normativo	Comprendere gli standard rilevanti come l'ISO IEC 27001-213 e le normative connesse relative all'innovation management ed al risk management.	8	
	Metodi di Analisi	Utilizzo di metodi quantitativi e qualitativi per valutare i rischi, analizzare la loro variabilità e correlazione.	8	
	Analisi Inferenziali	Applicazione di test statistici per la determinazione e la previsione dei rischi.	8	
	Ponderazione e Mitigazione	Sviluppo di strategie per la ponderazione e mitigazione dei rischi identificati.	8	
	Controlli di Sicurezza	Implementazione e monitoraggio dei controlli di sicurezza in linea con la politica di sicurezza dell'organizzazione.	6	
	Organizzazione e Ruoli	Definizione della struttura organizzativa, con specifici ruoli e responsabilità per la gestione della sicurezza delle informazioni.	5	
Books of reference	Autore: Cesare Gallotti Titolo: Sicurezza delle informazioni. Gestione del Rischio. I sistemi di Gestione. La ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022. Link: https://www.cesaregallotti.it/			

	
Notes to the books	During the lectures, the instructor will use slides that follow the content of the book, so they will not be provided. The reference text covers all the topics of the course; therefore, it is recommended to study from the text and to independently and consistently complete all the exercises included at the end of each chapter discussed in class. On the Uniba e-learning platform (see above 'virtual location'), the following are available: • video materials used during the lectures; • some examples of written exam questions, with samples of completed exam questions. References to the ISO standards, which are also highly relevant, will be made available by the instructor.

Organization of the didactic activities

Hours				
Total	Lectures	Practice sessions	Project work	Individual study
150 hours	48 hours			102 hours
CFU/ETCS				
6 CFU	6 CFU			

Teaching methods

Lectures, exercises, and independent and group activities both in the classroom and at home. Non-attending students can work individually by making arrangements with the instructor.

Expected learning outcomes

Knowledge and understanding	**Autonomy of Judgment** • Critical Risk Evaluation: Students acquire the ability to critically evaluate identified risks, understanding how they can influence the organization and developing informed judgments on which risks need mitigation and which can be accepted. • Application of Regulations and Security Standards: Through the study of the regulatory context, students learn to interpret and apply regulations and security standards, developing the autonomy needed to judge the adequacy of existing security policies within an organization. • Development of Customized Solutions: Students are capable of developing and proposing customized solutions for risk management, based on the specific needs of the organization and a detailed analysis of risk contexts and vulnerabilities. **Communication Skills** • Ability to Communicate Clearly and Precisely: Students develop the skill to communicate clearly and precisely the issues related to risk management and the proposed solutions, using appropriate technical language for both experts and non-specialists. • Proficiency in Visual Data Representation: Students acquire the ability to visually represent data and the results of risk analysis through the use of tools like PowerPoint presentations, charts, and diagrams, facilitating the understanding and discussion of the results obtained. • Competence in Presenting and Arguing: Students gain competence in presenting and arguing the main aspects of risk analysis in academic or professional contexts, supporting their arguments with appropriate statistical and regulatory evidence. **Ability to Learn Autonomously** • Continuous Research and Updating: Students learn how to stay updated on new regulations, technologies, and risk analysis methods, developing the ability to independently research additional resources and materials to deepen their knowledge. • Independent Application of Analytical Methods: Students acquire the ability to independently apply quantitative and qualitative risk analysis methods, adapting them to the specific needs and contexts that may arise in their work or future studies. • Development of Customized Solutions: Through the experience gained, students learn to develop and implement customized solutions for risk management, based on their critical analysis and understanding of the organizational context.
Applying knowledge and understanding	• Understanding and application of innovative technology and computational tools in the context of IT and data management. • Ability to use mathematical, statistical, and IT methods to analyze and manage risks in the field of information technology. • Development of critical skills in addressing issues related to information management, including the identification of threats and vulnerabilities. • Acquisition of communicative and representational skills to describe and discuss the key elements of risk analysis and management. • Ability to learn both basic and complex aspects of the subject, applying this knowledge to the practical management of risk.

Other skills	*Making judgements* • Basic Mathematical, Statistical, and IT Knowledge: Provides the foundation for understanding and applying quantitative and qualitative methods in risk analysis, which are essential for correctly assessing threats and vulnerabilities within an organization. • Ability to Use Technological and Computational Tools: Students learn how to apply innovative technology tools in the context of IT data management, enhancing their ability to efficiently analyze and manage complex information. • Development of Critical Information Management Skills: The program helps develop a critical understanding of issues related to information management, enabling students to identify, analyze, and solve complex problems related to cybersecurity. *Communication* • Application of Technological and Computational Tools: Students learn to use Innovation Technology tools and computational solutions to manage and analyze IT data, particularly in the context of information security. • Critical Analysis of Information Management Issues: Critical skills are developed to identify, analyze, and resolve complex issues related to information management, considering risk variables and vulnerabilities within an organization. • Development of Communication Skills: Students acquire the ability to effectively communicate and represent the results of risk analysis and management, using appropriate methodologies and presentation tools to clearly and precisely share their conclusions. *Learning skills* • Critical Evaluation of Risk Situations**:** Students learn to independently identify and assess risks using both quantitative and qualitative methods. This enables them to formulate informed judgments about the threats and vulnerabilities that may impact an organization. • Independent Application of Regulations and Standards**:** The study of international regulations and standards (such as ISO/IEC 27001) equips students with the ability to judge the adequacy of existing security policies and to develop recommendations for improvements based on autonomous analysis. • Development of Risk Mitigation Strategies**:** Students acquire the competence to independently decide which mitigation strategies are most appropriate based on the specific context, weighing various factors such as the probability and impact of risks.

Assessment	
Assessment methods	The exam is written, with an oral assessment aimed at verifying the overall understanding of risk emergence, particularly in connection with the application of Industry 4.0 technologies within companies in the context of digitalization and digital transformation processes. The written exam consists of multiple-choice questions and open-ended questions. The oral examination also serves to address any gaps identified during the written test.

Evaluation criteria	
Measurements and final grade	

Mark	descriptors
< 18 insufficiente	Fragmentary and superficial knowledge of the contents, errors in applying the concepts, deficient description.
18 - 20	Sufficient but general content knowledge, simple description, uncertainties in the application of theoretical concepts.
21 - 23	Appropriate but not in-depth knowledge of content, ability to apply theoretical concepts, ability to present content in a simple way.
24 - 25	Appropriate and extensive knowledge of the contents, good ability to apply knowledge, ability to present the contents in an articulated way.
26 - 27	Precise and complete content knowledge, good ability to apply knowledge, analytical skills, clear and correct description.
28 - 29	Wide, complete and in-depth knowledge of the contents, good application of the contents, good capacity for analysis and synthesis, safe and correct description.
30 30 e lode	Very broad, complete and in-depth knowledge of the contents, well-established ability to apply the contents, excellent capacity for analysis, synthesis and interdisciplinary connections, mastery of description.

Further information

Students are advised to rely exclusively on the information/communications provided on the official websites of the Computer Science Department, or on social groups only if set up and administered exclusively by the teachers of the related courses:

• https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea
• https://www.uniba.it/it/ricerca/dipartimenti/informatica
• https://elearning.di.uniba.it/

Course schedules are available here:
• https://programmi.di.uniba.it/

The information that all students should know is written in the Teaching regulations and study posters available on the site:
• https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea

Students are advised to be wary of information circulating on unofficial sites or social groups, as they are often found to be unreliable, incorrect or incomplete.

Link to the course on the department e-learning platform:
https://elearning.di.uniba.it/