QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**		
Course No.	**0133429**		**Course name**		Cybersecurity Governance and Risk Compliance		
Credit Hours	**3**		**Prerequisite Co-requisite**		Data Analytics		
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ Mandatory requirements	☐ ✓ **Elective requirements**	
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓ Traditional learning		
Teaching model	☐ 2Synchronous: 1asynchronous		✓ 2 face to face: 1synchronous		☐ 3 Traditional		

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course focuses on the development and maintenance of effective cybersecurity strategies in *n the modern digital landscape*. Students will examine key governance measures, risk management strategies, and decision-making frameworks that help organizations manage risk and ensure compliance with industry regulations. Emphasizing the importance of threat-informed decisions, the course covers various risk management approaches and provides insights into the regulatory environment and compliance frameworks commonly adopted to enhance organizational cybersecurity posture. Key areas of focus include governance structures, policies, and procedures that ensure ongoing compliance with legal, ethical, and industry-specific standards. Students will also gain a deeper understanding of how organizations can align their cybersecurity strategies with global regulations such as GDPR, HIPAA, and NIST frameworks. Through practical examples from industry and government, students will learn how robust governance and compliance measures can protect organizations from threats while meeting their compliance obligations across different sectors

Learning resources

Course book information (Title, author, date of issue, publisher ... etc.)	• Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices*. Hoboken, Tarantino, A. (2008). NJ: John Wiley & Sons. ISBN-13: 978-0-470-55373-2.
Supportive learning resources	• Enterprise Risk Management: From Incentives to Controls (2nd ed.). Hoboken, Lam, J. (2014). NJ: John Wiley & Sons. ISBN-13:

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

(Books, databases, periodicals, software, applications, others)	978-1118413616ISO 31000:2018 Risk Management – Guidelines, International Organization for Standardization (ISO) • Corporate Governance: Principles, Policies, and Practices (4th ed.). Tricker, B. (2019). Oxford, UK: Oxford University Press. ISBN-13: 978-0198809869. • Society of Corporate Compliance and Ethics (SCCE). (2023). The Complete Compliance and Ethics Manual. Minneapolis, MN: SCCE. ISBN-13: 978-0983375545.			
Supporting websites				
The physical environment for teaching	☐ ✓**Class room**	☐ ✓labs	☐ **Virtual educational platform**	☐ Others
Necessary equipment and software				
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	**Explain** the legal and privacy aspects of cybersecurity (HIPAA).	**MK1**
K2	**Analyze** the differences in governance, risk, and compliance across finance, government, and critical infrastructure verticals.	**MK2**
K3	**Assess** an organization's maturity against industry and regulatory standards.	**MK4**
K4		**MK1**
K5		**MK5**
	Skills	
S1	**Evaluate** and control cybersecurity risks in an organization.	**MK4**
S2	**Develop** cybersecurity program metrics and reporting for effective governance	**MK1**
	Competences	
C1	**Report** on cybersecurity governance and program performance to stakeholders.	
C2	**Apply** industry standards to improve cybersecurity maturity and compliance (e.g., ISO 27001, NIST).	

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation /	0	**0**	0	0

practical applications				
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities include tasks such as projects, assignments, research, and group work performed through the virtual platform without direct teacher interaction.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	Learning Style*	Reference **
1	**Course Overview and Introduction** ○ Introduction to Governance, Risk, and Compliance (GRC) ○ Overview of the course structure, objectives, and assessment ○ Setting expectations and course goals	Lecture	• Tarantino, A. (2008). *Governance, Risk, and Compliance Handbook*. Chapter 1, pp. 1–15 (Introduction to GRC). • ISO/IEC 27001 Overview: Entire standard summary is available online: https://www.iso.org/isoiec-27001-information-security.html • Article: "Why GRC is Critical for Modern Cybersecurity," Harvard Business Review
2	**Governance Frameworks** ○ Introduction to governance frameworks (e.g., COBIT, ISO, ITIL, COSO) ○ Key principles of governance: accountability, transparency, ethical decision-making	Lecture, learning through projects, learning through problem solving	• ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. pp. 5–20 (Framework overview). • ISO/IEC. (2013). ISO/IEC 27001: Information Security Management. Sections 4–6 (Governance-related controls). • ITIL Foundation Overview: ITIL website, no page numbers: https://www.axelos.com/certifications/itil-certifications • COSO. (2017). Enterprise Risk Management: Integrating with Strategy and Performance. pp. 19–30 (Framework principles).
3	**Governance Artefacts** ○ Overview of key governance artefacts (e.g., policies, procedures, charters, reports) ○ The role of artefacts in decision-making, accountability, and monitoring	Lecture, learning through projects, learning through problem solving	• ISO/IEC. (2013). ISO/IEC 27002: Code of Practice for Information Security Controls. pp. 22–35 (Policies, processes, and controls). • SANS Institute. (2020). Sample Cybersecurity Policies for Organizations: https://www.sans.org/policies/ • Tarantino, A. (2008). Governance, Risk, and Compliance Handbook. Chapter 2, pp. 16–28 (Governance artefacts).
4	**Risk Management – Principles and Processes** ○ Introduction to risk management concepts and	Lecture, learning through projects, learning through problem solving	• ISO. (2018). ISO 31000: Risk Management – Guidelines. pp. 4–10 (Principles and terminology). • NIST. (2018). Cybersecurity Framework

	terminology ○ Key risk management processes: identification, assessment, response, and monitoring		Version 1.1: Identify Function, pp. 8–15. • Aven, T. (2015). Risk Analysis. Chapter 3, pp. 40–56 (Risk management processes).
5	**Risk Quantification** ○ Quantitative risk analysis techniques (e.g., probability-impact matrix, Monte Carlo simulations) ○ Tools for assessing and measuring risks (e.g., risk scoring, heat maps)	Lecture, learning through projects, learning through problem solving	• NIST. (2012). NIST Special Publication 800-30: Guide for Conducting Risk Assessments. Sections 3.4 and 4.2, pp. 18–25 (Quantification methods). • Hubbard, D. W. (2009). The Failure of Risk Management: Why It's Broken and How to Fix It. Chapter 5, pp. 97–112 (Heat maps and probability-impact models). • Article: "Using Risk Heat Maps for Effective Decision-Making," ISACA Journal (online resource; no page numbers).
6	**Compliance – Industry Overview** ○ Overview of key regulatory frameworks (e.g., GDPR, SOX, PCI-DSS, FISMA) ○ The role of compliance in risk management and governance	Lecture, learning through projects, learning through problem solving	• EU GDPR Portal: Articles 5–6 (Principles of GDPR): https://gdpr-info.eu/ • PCI DSS Standards: Overview, pp. 4–10: https://www.pcisecuritystandards.org/ • FISMA Implementation Project: Key requirements overview: https://csrc.nist.gov/projects/risk-management/about-fisma • Calder, A. (2016). EU GDPR: A Pocket Guide. Chapter 2, pp. 20–32 (Compliance overview).
7	**Compliance – Regulatory Frameworks** ○ Overview of key regulatory frameworks (e.g., GDPR, SOX, PCI-DSS, FISMA) ○ The role of compliance in risk management and governance ○	Lecture, learning through projects, learning through problem solving	• SOX Compliance Overview: Key requirements, pp. 15–22: https://www.soxlaw.com/ • Article: "The Role of PCI DSS in Securing Payment Data," Forbes (online resource; no page numbers). • Tarantino, A. (2008). Governance, Risk, and Compliance Handbook. Chapter 8, pp. 78–95 (Overview of regulatory frameworks).
8	**Legal Aspects and Privacy** ○ Overview of legal considerations in GRC: Contracts, liability, intellectual property ○ Privacy laws and regulations (e.g., GDPR, CCPA, HIPAA)	Lecture, learning through projects, learning through problem solving	• GDPR Overview: Articles 12–22 (Privacy rights and compliance): https://gdpr-info.eu/ • California Consumer Privacy Act (CCPA): Key rights under CCPA: https://oag.ca.gov/privacy/ccpa • Moerel, L. (2014). Big Data Protection: Challenges and Opportunities. Chapter 4, pp. 60–75 (Legal implications of data processing). • HIPAA Compliance Guide: Administrative safeguards, Section 164.308: https://www.hhs.gov/hipaa/index.html
9	**GRC in Finance** ○ Role of GRC in the financial services industry	Lecture, learning through projects, learning through	• Basel III Overview: Principles of Basel III, pp. 5–15: https://www.bis.org/bcbs/basel3.htm

	○ Regulatory requirements in finance (e.g., Basel III, Dodd-Frank, MiFID II)	problem solving	• Dodd-Frank Act Summary: Key compliance mandates, pp. 12–18: https://www.congress.gov/bill/111th-congress/house-bill/4173 • Lam, J. (2014). Enterprise Risk Management: From Incentives to Controls. Chapter 6, pp. 120–135 (GRC in financial institutions).
10	**GRC in Government** ○ GRC frameworks used in government agencies ○ Public sector accountability, transparency, and risk management	Lecture, learning through projects, learning through problem solving	• COSO. (2017). Enterprise Risk Management: Integrating with Strategy and Performance. Public sector applications, pp. 90–104. • Article: "Risk Management in Government Agencies," Public Administration Review (online resource; no page numbers). • FISMA Compliance Guide: Key requirements for government agencies, pp. 20–32: https://www.cisa.gov/federal-information-security-modernization-act
11	**GRC in Critical Infrastructure** ○ The importance of GRC in critical infrastructure sectors (e.g., energy, transportation, utilities) ○ Industry-specific risks and governance challenges	Lecture, learning through projects, learning through problem solving	• NIST. (2018). NIST Special Publication 800-82: Guide to Industrial Control Systems Security. Chapters 2–3, pp. 25–48. • Article: "The Importance of GRC in Critical Infrastructure Sectors," ISACA Journal (online resource; no page numbers). • Tarantino, A. (2008). Governance, Risk, and Compliance Handbook. Chapter 12, pp. 140–155 (Critical infrastructure governance).
12	**Integration of GRC Components** ○ How to integrate governance, risk, and compliance into a cohesive strategy ○ Best practices for alignment across all GRC functions	Lecture, learning through projects, learning through problem solving	• ISACA. (2019). COBIT 2019 Framework: Implementation Guide. pp. 65–80 (Integration best practices). • Article: "Integrating Governance, Risk, and Compliance for Business Success," Gartner Insights (online resource; no page numbers). • Lam, J. (2014). Enterprise Risk Management: From Incentives to Controls. Chapter 10, pp. 160–175 (Integrated frameworks).
13	**Emerging Trends in GRC** ○ The future of GRC: Technology, automation, AI, and data analytics ○ Evolving regulatory landscapes and their impact on GRC	Lecture, learning through projects, learning through problem solving	• Article: "The Future of GRC: AI and Automation," Harvard Business Review (online resource; no page numbers). • Tarantino, A. (2008). Governance, Risk, and Compliance Handbook. Chapter 14, pp. 175–190 (Emerging technologies in GRC). • NIST. (2020). NIST Special Publication 800-207: Zero Trust Architecture. pp. 5–15.
14	**Course Review and Final Exam** ○ Review of all course topics and key takeaways	Lecture, learning through projects, learning through	• Tarantino, A. (2008). Governance, Risk, and Compliance Handbook. Comprehensive review, pp. 1–190 (all

	○ Final Q&A session and student feedback	problem solving	applicable chapters). • ISO. (2018). ISO 31000: Risk Management – Guidelines. Entire document, focus on pp. 4–25. • ISACA. (2019). COBIT 2019 Framework: Implementation Guide. Comprehensive review, pp. 5–80.
15	Discussion	participatory learning	
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

This activities was designed using the **Project-Based Learning (PBL)**

Project 1: GDPR Compliance Gap Analysis & Corrective Action Plan

Task / Activity	Reference	Expected Results
Conduct a compliance audit for a fictional EU-based fintech startup. Use the official GDPR Article Checklist to evaluate their data handling policies. Analyze the Equifax breach case study to identify similar systemic failures.	Official GDPR Text (Articles 5, 15-22, 32-34), ICO PIA Guidelines, Equifax 2017 Breach Report	A gap analysis report detailing policy violations, a prioritized corrective action plan mapped to GDPR articles, and a risk mitigation strategy for identified failures.

Project 2: Privacy Impact Assessment for a Data-Driven E-Commerce Platform

Task / Activity	Reference	Expected Results
Perform a full PIA for "ShopGlobal," a platform using AI for personalized ads. Map data flows, assess risks for California (CCPA) and EU (GDPR) customers, and design a user consent dashboard and data retention policy.	NIST PIA Framework, CCPA Compliance Guide, EDPS PIA Template	A completed PIA document with data flow diagrams, a dual-compliance matrix (GDPR/CCPA), and prototype designs for privacy notices and a user data management portal.

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results

QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Week	Task / activity	Reference	Expected results
1	Cybersecurity Governance Case Study Discussion • **Objective:** Introduce students to the real-world importance of GRC in cybersecurity. • **Task:** • Provide a short case study (e.g., a recent cybersecurity breach involving governance failures). • Students work in groups to identify governance, risk management, and compliance failures in the scenario. • Discuss as a class how better GRC practices could have mitigated the issue.	• Tarantino, A. (2008). *Governance, Risk, and Compliance Handbook*. Chapter 1: Introduction to GRC. • Article: "Target's 2013 Data Breach: The Failure of Governance and Risk Management." • ISO 27001 overview: https://www.iso.org/isoiec-27001-information-security.html	**Deliverable:** Group insights presented verbally during class
2	Governance Framework Analysis • **Objective:** Compare and evaluate governance frameworks for cybersecurity. • **Task:** • Groups analyze governance frameworks (e.g., COBIT, ISO 27001, ITIL). • Highlight differences in principles, scope, and applicability.	• ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. • ISO/IEC. (2013). ISO/IEC 27001: Information Security Management. • ITIL Foundation: Overview of ITIL Principles and Practices: https://www.axelos.com/certifications/itil-certifications	**Deliverable:** A comparative table and a brief group presentation.
3	Drafting a Cybersecurity Policy • **Objective:** Learn to create governance artefacts. • **Task:** • Provide a scenario (e.g., drafting a password policy). • Students draft a policy document, including purpose, scope, roles, and enforcement.	• SANS Institute. (2020). Sample Cybersecurity Policies for Organizations: https://www.sans.org/policies/ • ISO/IEC. (2013). ISO/IEC 27002: Code of Practice for Information Security Controls.	**Deliverable:** A completed cybersecurity policy for instructor feedback
4	Risk Identification Workshop • **Objective:** Identify and categorize risks in an organizational context. • **Task:** • Analyze a case study (e.g., a hospital's IT system vulnerable to ransomware). • Students list risks, categorize	• ISO. (2018). ISO 31000: Risk Management – Guidelines. • NIST. (2018). Cybersecurity Framework Version 1.1: Identify Function.	**Deliverable:** A risk categorization and prioritization report.

Week	Task / activity	Reference	Expected results
	them, and prioritize based on likelihood and impact.		
5	Creating a Risk Heat Map • **Objective:** Quantify risks and represent them visually. • **Task:** • Students calculate risk scores and create a heat map.	• NIST. (2018). NIST Special Publication 800-30: Guide for Conducting Risk Assessments. • Book: Hubbard, D. W. (2009). The Failure of Risk Management: Why It's Broken and How to Fix It.	**Deliverable:** A completed heat map with an explanation of findings.
6	Compliance Checklist Analysis • **Objective:** Evaluate compliance with industry standards. • **Task:** • Provide a checklist (e.g., GDPR requirements). • Students assess a fictional company's policies against the checklist and identify gaps.	• EU GDPR Portal: https://gdpr-info.eu/ • PCI DSS Standards: https://www.pcisecuritystandards.org/ • Book: Calder, A. (2016). *EU GDPR: A Pocket Guide*.	**Deliverable:** A compliance gap analysis report with recommendations
7	Regulatory Failure Case Study • **Objective:** Analyze a real-world compliance failure to extract lessons learned. • **Task:** • Provide a detailed case study (e.g., Equifax's 2017 data breach). • Students analyze causes, consequences, and propose corrective actions.	• Case Study: "The Equifax Data Breach: What Went Wrong?" Harvard Business Review. • SOX Compliance Overview: https://www.soxlaw.com/ • Book: Lam, J. (2014). *Enterprise Risk Management: From Incentives to Controls*	**Deliverable:** A report summarizing findings and recommendations.
8	Privacy Impact Assessment (PIA) • **Objective:** Assess the impact of data collection practices on privacy. • **Task:** • Students complete a Privacy Impact Assessment (PIA) for a fictional e-commerce platform. • Propose strategies for ensuring compliance with privacy regulations (e.g., GDPR, CCPA).	• GDPR Overview: https://gdpr-info.eu/ • California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa • Book: Moerel, L. (2014). *Big Data Protection: Challenges and Opportunities*.	**Deliverable:** A completed PIA template and recommendations.