FOCUS UNIVERSITY INSTITUTE

Madrid, Spain

RESPONSIBLE AI, GOVERNANCE, CYBERSECURITY, AND SUSTAINABILITY

Program Developer: Luis Fernando (Lou) Villalba, PhD., EdD.

Course Code:	RAG 505 (Provisional)
Credits:	3 North American Graduate Credits / Proposed 6 ECTS
Academic Level:	Graduate (Master's)
Duration:	14 Weeks
Student Workload:	Approximately 150 Hours (42 Guided + 108 Independent)
Delivery Mode:	Madrid-Based, Online, or Blended
Program/Stage:	Master of Business Administration with a Concentration in Business and Sustainability / Common Trunk
Professor:	_____
Office Hours:	[To be determined]
Contact:	[To be determined]

1. Course Description

This common-trunk graduate course forms part of the Master of Business Administration with a Concentration in Business and Sustainability. It contributes responsible management, operations and value-chain governance, enterprise risk, cybersecurity, accountability, and sustainability assurance to a full-function MBA spanning the principal areas of business administration. The concentration strengthens the program through explicit sustainability outcomes and applications without replacing its broad MBA identity or creating complete course-for-course equivalence with another institution's curriculum.

The course uses enterprise-risk, internal-control, assurance, technology-governance, and stakeholder perspectives to connect strategy with implementation. Students build inventories, classify uses and exposures, evaluate impacts, establish ownership, select proportionate controls, define evidence and escalation requirements, and design monitoring and improvement cycles. NIST, European Union, OECD, UNESCO, cybersecurity, privacy, and sustainability resources are treated as adaptable frameworks rather than mechanical checklists.

Particular attention is given to human-centred and trustworthy AI; data governance; privacy; cybersecurity governance and resilience; third-party and supply-chain risk; incident and crisis response; climate and broader sustainability dependencies, impacts, risks, and opportunities; disclosure quality; greenwashing; and executive communication. The Week 14 signature assessment is an Integrated Governance, Cybersecurity, and Sustainability Assurance Plan for executive or board consideration.

2. Course Learning Outcomes

Upon successful completion of this course, students will be able to:

LO1. **Integrate** enterprise governance, operations, value-chain, risk, ethics, stakeholder, and assurance frameworks to diagnose interdependent AI, data, cybersecurity, social, and environmental exposures. [Bloom's Level 4: Analyze]

LO2. **Evaluate** AI systems and data practices across their lifecycles using inventories, classification, impact assessment, accountability, transparency, human oversight, and proportionate control design. [Bloom's Level 5: Evaluate]

LO3. **Assess** cybersecurity, privacy, third-party, operational, and supply-chain resilience risks using business-impact, threat, vulnerability, control, incident, continuity, recovery, and assurance evidence. [Bloom's Level 5: Evaluate]

LO4. **Analyze** material sustainability dependencies, impacts, risks, opportunities, metrics, targets, transition choices, value-chain implications, and disclosure or claims quality. [Bloom's Level 5: Evaluate]

LO5. **Create** and defend an integrated and measurable governance, operations, cybersecurity, and sustainability assurance and improvement plan for executive or board decision-making. [Bloom's Level 6: Create]

3. Required Materials

3.1 Main Texts and Open Educational Resource (OER)

- Main Text 1: Kshetri, N. (2021). Cybersecurity management: An organizational and strategic approach. University of Toronto Press.
- Main Text 2 (OER Core Resource Set): National Institute of Standards and Technology. (2023-2024). AI Risk Management Framework 1.0, Generative AI Profile, and Cybersecurity Framework 2.0. https://www.nist.gov/itl/ai-risk-management-framework and https://www.nist.gov/cyberframework

3.2 Supplementary Texts (Non-Open Educational Resources)

- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.
- International Sustainability Standards Board. (2023). IFRS S1 and IFRS S2 sustainability disclosure standards, with current official amendments and implementation guidance.
- UNESCO. (2021). Recommendation on the ethics of artificial intelligence; and OECD. (2024). OECD Principles on Artificial Intelligence.
- Selected current incident reports, organizational disclosures, regulatory and standards materials, peer-reviewed articles, professional cases, and lawful non-confidential evidence supplied through the LMS.

3.3 Open Educational Resources (OER)

- NIST AI Risk Management Framework and current profiles: https://www.nist.gov/itl/ai-risk-management-framework
- NIST Trustworthy and Responsible AI Resource Center: https://airc.nist.gov/
- NIST Cybersecurity Framework 2.0 and implementation resources: https://www.nist.gov/cyberframework
- European Union Artificial Intelligence Act: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- European Union NIS 2 Directive: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

- UNESCO Recommendation on the Ethics of Artificial Intelligence: https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence
- IFRS S1 and IFRS S2 official navigator and implementation resources: https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/
- Selected OECD, ENISA, EDPB, EUR-Lex, IFRS Foundation, GHG Protocol, national regulator, company, and standards-body resources.

3.4 Technology Requirements

- Reliable internet connection and Learning Management System access
- Spreadsheet, presentation, collaborative-document, risk-register, process-mapping, dashboard, and data-visualization software
- Instructor-approved artificial-intelligence, cybersecurity, and sustainability-analysis tools; students will not be required to purchase multiple commercial subscriptions
- PDF annotation and video-conferencing capability for source review, scenario exercises, executive briefings, and the final oral defence

4. Assessment Structure

This course combines ongoing governance and assurance laboratories with an individual AI System Inventory and Impact Assessment, an independently completed midterm examination, an integrated Cybersecurity and Sustainability Scenario Assurance Memorandum, and an applied final plan. The final Integrated Governance, Cybersecurity, and Sustainability Assurance Plan replaces a conventional final examination and culminates in Week 14.

Assessment Component	Type	Weight	Due Date
Governance, Risk & Assurance Labs	Ongoing	10%	Continuous
AI System Inventory & Impact Assessment	**Formative**	15%	Week 4
Midterm Examination	**Summative**	20%	Week 7
Cybersecurity & Sustainability Scenario Assurance Memorandum	**Summative**	15%	Week 10
Final Project: Integrated Governance, Cybersecurity & Sustainability Assurance Plan	**Summative**	40%	Week 14
TOTAL		**100%**	

5. Grading Scale

This course uses the American University grading scale:

Letter Grade	Percentage	Description
A	93-100%	Excellent; exceptional achievement
A-	90-92%	Excellent work with minor areas for improvement
B+	87-89%	Very good; above average performance
B	83-86%	Good; solid understanding demonstrated
B-	80-82%	Good work with some areas for improvement
C+	77-79%	Satisfactory; meets basic requirements
C	73-76%	Adequate; acceptable understanding
C-	70-72%	Passing but below average

Letter Grade	Percentage	Description
D	60-69%	Minimum passing; significant improvement needed
F	Below 60%	Failing; does not meet course requirements

6. Course Schedule

Week 1: Integrated Governance, Enterprise Risk, Assurance, and Accountability

Topics: Governance versus management; purpose; value and harm; board and executive accountability; stakeholders; three lines; enterprise risk; internal control; assurance; proportionality; organizational context

Readings: Kshetri, selected governance chapter; NIST AI RMF 1.0, Introduction and Part 1

Synchronous: Governance-system and accountability-mapping workshop

Asynchronous: Select an organization and frame an integrated governance or assurance decision

Week 2: AI, Data, and Technology Lifecycles, Inventories, and Ownership

Topics: AI and data lifecycles; intended purpose and context; asset, system, model, data, vendor, and use-case inventories; roles; ownership; classification; documentation; retirement; shadow AI

Readings: NIST AI RMF 1.0, Core; NIST AI RMF Playbook, selected Govern and Map actions

Synchronous: AI-system inventory, RACI, and lifecycle-evidence laboratory

Asynchronous: Build a preliminary system and evidence inventory for the selected organization

Week 3: Trustworthy AI, Ethics, Rights, Impact Assessment, and Human Oversight

Topics: Validity; safety; security and resilience; accountability; transparency; explainability; privacy; fairness; human rights; affected stakeholders; contestability; impact pathways; human oversight

Readings: UNESCO Recommendation; OECD AI Principles; NIST AI RMF trustworthiness characteristics

Synchronous: Stakeholder-impact, harm-benefit, and human-oversight assessment workshop

Asynchronous: Identify impacts, affected groups, evidence gaps, controls, residual risk, and escalation needs

Week 4: AI Governance Systems, Risk Classification, Regulation, and Assurance

Topics: Governance policies and management systems; risk tiers; prohibited and high-risk uses; provider, deployer, and vendor roles; transparency; documentation; testing; monitoring; audit and assurance

Readings: EU AI Act, selected provisions; NIST AI RMF and current profile resources

Synchronous: AI classification, legal-source verification, and control-design case

Asynchronous: Complete AI System Inventory and Impact Assessment

Assessment Due: AI System Inventory & Impact Assessment (15%)

Week 5: Cybersecurity Governance, Risk Profiles, and Control Architecture

Topics: Cybersecurity as enterprise risk; NIST CSF 2.0 Govern, Identify, Protect, Detect, Respond, and Recover; current and target profiles; risk appetite; control objectives; accountability; metrics

Readings: Kshetri, selected risk and strategy chapters; NIST CSF 2.0

Synchronous: Current-profile, target-profile, gap, and priority laboratory

Asynchronous: Develop a risk register connecting assets, business services, threats, vulnerabilities, impacts, controls, and evidence

Week 6: Data Protection, Third-Party Risk, Incidents, Continuity, and Resilience

Topics: Privacy and data governance; identity and access; secure configuration; third-party and supply-chain risk; ransomware; incident response; business continuity; recovery; crisis decisions; lessons learned

Readings: Kshetri, selected controls and resilience chapters; NIS 2 Directive; NIST CSF implementation resources

Synchronous: Cyber incident, business-impact, and executive-escalation simulation

Asynchronous: Prepare for the midterm through an integrated AI, data, cybersecurity, and governance case

Week 7: Midterm Examination and Governance Integration

Topics: Integration of governance, enterprise risk, assurance, AI and data lifecycles, ethics, rights, impact assessment, human oversight, cybersecurity governance, control, incident, and resilience foundations

Readings: Review Weeks 1-6 materials

Synchronous: Individual midterm examination; generative AI is not permitted unless expressly authorized

Asynchronous: Post-examination correction and professional-learning plan

Assessment Due: Midterm Examination (20%)

Week 8: Sustainability Governance, Materiality, Stakeholders, and the Value Chain

Topics: Sustainability dependencies, impacts, risks, and opportunities; financial and impact materiality; stakeholders; governance; strategy; value chains; due diligence; social and environmental justice

Readings: IFRS S1, selected requirements; instructor materials on impact materiality and value-chain due diligence

Synchronous: Sustainability issue, stakeholder, value-chain, and materiality workshop

Asynchronous: Build a sustainability-risk and opportunity register with sources, assumptions, and limitations

Week 9: Climate, Greenhouse-Gas Evidence, Transition, Adaptation, and Scenarios

Topics: Physical and transition risk; Scope 1, 2, and 3 emissions; boundaries; estimates; targets; transition plans; adaptation; climate resilience; scenario analysis; uncertainty; financial implications

Readings: IFRS S2 and current implementation guidance; GHG Protocol, selected standards and guidance

Synchronous: Climate evidence, emissions-boundary, and scenario-assurance laboratory

Asynchronous: Develop an integrated cyber and sustainability scenario with controls, signposts, and evidence needs

Week 10: Integrated Scenarios, Interdependencies, Controls, and Residual Risk

Topics: AI-operations-supply-chain-cyber-sustainability interdependencies; systemic and cascading risk; concentration and vendor dependence; control design; control conflicts; resilience; residual risk; options; decision thresholds

Readings: NIST AI RMF, CSF 2.0, IFRS S1/S2, and selected organization-specific evidence

Synchronous: Cross-domain scenario stress test and assurance challenge

Asynchronous: Submit Cybersecurity and Sustainability Scenario Assurance Memorandum

Assessment Due: Cybersecurity & Sustainability Scenario Assurance Memorandum (15%)

Week 11: Measurement, Testing, Monitoring, Audit, and Independent Assurance

Topics: Control design and operating effectiveness; AI testing, evaluation, verification, and validation; cybersecurity testing; sustainability evidence; auditability; indicators; thresholds; incidents; remediation

Readings: NIST AI Resource Center and CSF 2.0 measurement resources; IFRS implementation materials

Synchronous: Control-evidence, indicator, audit-trail, and assurance-design laboratory

Asynchronous: Define metrics, evidence, ownership, testing, escalation, and review cadence for the final plan

Week 12: Disclosure, Claims, Transparency, Crisis Communication, and Trust

Topics: Board reporting; regulatory and stakeholder disclosure; material information; AI transparency; cyber incident communication; sustainability claims; greenwashing; uncertainty; accessibility; assurance statements

Readings: EU AI Act transparency provisions; IFRS S1/S2; selected current consumer-protection and disclosure guidance

Synchronous: Executive dashboard, disclosure, claims, and crisis-communication review

Asynchronous: Complete final-plan priorities, roadmap, measures, governance, resources, communication, and evidence architecture

Project Milestone Due: Final-project scope, risk universe, assurance criteria, and evidence plan

Week 13: Integrated Assurance and Improvement Plan Studio

Topics: Strategic synthesis; prioritization; proportionality; roadmap; ownership; resources; change dependencies; assurance map; board narrative; AI provenance; oral-defence preparation

Readings: Review current authoritative resources relevant to the selected organization and exposures

Synchronous: Assurance-plan studio, peer challenge, instructor consultation, and defence rehearsal

Asynchronous: Complete board paper, assurance portfolio, AI Usage Statement, presentation, and reflection

Week 14: Board Assurance Presentations, Oral Defence, and Integration

Topics: Integration of AI, data, cybersecurity, governance, ethics, sustainability, enterprise risk, assurance, implementation, communication, and professional judgment

Readings: No new readings; review project evidence and course and certificate-cluster outcomes

Synchronous: Integrated Governance, Operations, Cybersecurity and Sustainability Assurance Plan presentations, oral defence, peer learning, and course synthesis

Asynchronous: Submit final board paper, assurance portfolio, presentation, AI Usage Statement, and individual reflection

Assessment Due: Final Project: Integrated Governance, Cybersecurity & Sustainability Assurance Plan (40%)

7. Detailed Assignment Descriptions

7.1 Governance, Risk & Assurance Labs - 10%

Learning Outcomes Addressed: All course learning outcomes

Description

Graduate governance competence develops through disciplined preparation, classification, evidence review, risk assessment, control design, scenario analysis, professional challenge, and reflection. Students complete applied laboratories and explain how organizational context affects accountability, proportionality, residual risk, and assurance.

Requirements

- Attend a minimum of 12 of 14 synchronous sessions and participate actively
- Complete governance, inventory, impact, risk-profile, control, incident, materiality, scenario, metric, disclosure, and assurance laboratories
- Explain criteria, sources, assumptions, uncertainty, limitations, residual risk, and accountability in accessible executive language
- Provide respectful, specific, evidence-based, and useful challenge during peer, incident, and board-assurance reviews
- Follow confidentiality, privacy, security, lawful-access, source-verification, professional-ethics, and AI-use disclosure requirements

Participation Rubric

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Preparation & Engagement (25%)	Consistently prepared; contributions materially advance governance and assurance analysis	Regular preparation and useful contribution	Basic preparation and participation	Unprepared, absent, or minimal contribution
Applied Assurance Labs (35%)	Rigorous, traceable work with excellent proportionality and contextual judgment	Strong work with minor gaps	Basic work with limited integration	Incomplete, unsafe, unsupported, or formulaic work
Peer Contribution (20%)	Challenge materially improves peers' criteria, evidence, controls, priorities, and safeguards	Constructive and relevant feedback	Basic feedback with limited detail	Little or unprofessional engagement
Professional & Responsible Conduct (20%)	Exemplary privacy, security, confidentiality, safe disclosure, attribution, and transparency	Responsible conduct with minor lapses	Meets minimum requirements	Repeated or serious professional concerns

7.2 AI System Inventory & Impact Assessment (Formative Assessment 1) - 15%

Learning Outcomes Addressed: CLO1, CLO2, CLO3

Due Date: Week 4

Description

Students document and evaluate an approved AI-enabled organizational use or portfolio. The work establishes purpose, context, lifecycle, data, actors, stakeholders, impacts, risk classification, controls, evidence, ownership, and escalation needs without presenting the assessment as legal certification.

Requirements

1. Define the organization, decision context, intended purpose, affected processes, lifecycle stage, scope, exclusions, and assessment criteria
2. Create an AI-system, model, data, vendor, integration, stakeholder, decision, and accountability inventory
3. Evaluate benefits, harms, rights, validity, safety, security, resilience, privacy, fairness, transparency, explainability, accessibility, and sustainability
4. Classify inherent risk and obligations using current authoritative sources; identify controls, evidence, gaps, residual risk, owners, and escalation
5. Recommend immediate actions, monitoring, review triggers, limitations, and an AI Usage Statement

Total Length: 1,800-2,200 words plus inventory, lifecycle map, impact register, responsibility map, and evidence record

Format: APA 7 analytical report and assurance exhibits; submit via LMS as PDF and editable source files

AI System Inventory & Impact Assessment Rubric

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Purpose, Scope & Context (15%)	Precise purpose, lifecycle, boundaries, actors, criteria, and intended use	Clear scope with minor gaps	Adequate scope and context	Purpose or boundaries unclear
Inventory & Accountability (20%)	Complete, usable inventory connects systems, data, vendors, stakeholders, roles, and decisions	Strong inventory with minor gaps	Basic inventory and ownership	Material elements or owners missing
Impact & Trustworthiness Assessment (30%)	Benefits, harms, rights, reliability, safety, privacy, fairness, transparency, accessibility, and sustainability are critically evaluated	Strong assessment with minor gaps	Basic assessment with limited depth	Material impacts omitted or unsupported
Classification, Controls & Residual Risk (25%)	Authoritative criteria support proportionate controls, evidence, ownership, escalation, and calibrated residual risk	Sound design with minor gaps	Basic controls and risk treatment	Classification or controls unreliable
Recommendations, Communication & AI Transparency (10%)	Priorities are executive-ready, cited, auditable, limited, and transparently disclosed	Professional synthesis with minor issues	Adequate but uneven	Unclear, unsafe, poorly cited, or opaque

7.3 Midterm Examination (Summative Assessment 1) - 20%

Learning Outcomes Addressed: CLO1, CLO2, CLO3

Due Date: Week 7

Description

The individual midterm examination assesses independent mastery of governance, enterprise risk, assurance, AI and data lifecycles, trustworthy-AI characteristics, impact assessment, human oversight, cybersecurity governance, risk profiles, control architecture, privacy, third-party risk, incident response, continuity, recovery, and executive accountability. Unless expressly authorized for a specific accommodation, students may not use generative-AI tools during the examination.

Requirements

1. Explain and connect governance, management, enterprise risk, internal control, assurance, accountability, proportionality, and residual risk
2. Classify and assess AI systems, data practices, stakeholders, impacts, lifecycle evidence, and human-oversight requirements
3. Apply cybersecurity risk, business-impact, control, incident, third-party, continuity, and resilience concepts to unfamiliar cases
4. Interpret authoritative frameworks and legal or regulatory sources without overstating applicability, compliance, certainty, or expertise
5. Recommend and defend a proportionate response while recognizing evidence gaps, trade-offs, ethics, rights, and limitations

Format: 120-minute examination with applied short answers, evidence interpretation, classification, control analysis, and integrated decision cases

Conditions: Individual work; approved reference sheet permitted; generative AI not permitted

Midterm Examination Rubric

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Governance & Assurance Integration (20%)	Concepts are accurately connected and selected for organizational purpose	Strong integration with minor gaps	Basic understanding with some errors	Major concepts missing or inaccurate
AI, Data & Impact Judgment (20%)	Lifecycle, stakeholder, rights, trustworthiness, and oversight reasoning is rigorous	Sound judgment with minor gaps	Basic analysis with limited depth	Material impacts or duties misinterpreted
Cybersecurity & Resilience Analysis (25%)	Risk, control, incident, third-party, continuity, and recovery analysis is coherent and contextual	Strong analysis with minor gaps	Basic analysis with some errors	Risk or controls seriously misapplied
Authoritative Sources & Responsible Reasoning (20%)	Sources, applicability, ethics, trade-offs, evidence gaps, and uncertainty are critically handled	Sound reasoning with minor gaps	Basic treatment with limited integration	Claims overstated or responsibilities omitted

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Recommendation & Communication (15%)	Coherent, proportionate response is concise and convincingly defended	Clear response with minor issues	Understandable but uneven	Recommendation unclear or unsupported

7.4 Cybersecurity & Sustainability Scenario Assurance Memorandum (Summative Assessment 2) - 15%

Learning Outcomes Addressed: CLO1, CLO3, CLO4, CLO5

Due Date: Week 10

Description

Students develop and stress-test a decision-relevant scenario that connects cyber, operational, climate, environmental, social, value-chain, financial, and stakeholder consequences. They compare controls and response options, identify assurance evidence, and recommend proportionate actions under uncertainty.

Assignment Focus

The memorandum must distinguish verified conditions, assumptions, estimates, scenarios, and predictions. It must use lawful, non-confidential information, avoid operational details that materially enable cyber abuse, and avoid claims of legal compliance or sustainability assurance beyond the evidence.

Requirements

1. Organization, critical services, stakeholders, assets, dependencies, value chain, risk appetite, context, and exposure pathways
2. Plausible scenario with cyber or technology trigger, sustainability or climate interaction, causal logic, time horizon, signposts, and uncertainty
3. Business-impact, stakeholder, rights, financial, operational, environmental, social, and reputational analysis
4. Control and response options compared for effectiveness, feasibility, proportionality, side effects, resilience, and residual risk
5. Recommendation with ownership, thresholds, escalation, continuity, recovery, communication, monitoring, and review cadence
6. Criteria, source and evidence register, assumptions, limitations, safe disclosure, and complete AI Usage Statement

Total Length: 1,800-2,200-word executive memorandum plus scenario, control, impact, and assurance-evidence exhibits

Format: Professional executive memorandum, visual appendices, and 5-7 minute assurance defence; submit via LMS

Cybersecurity & Sustainability Scenario Assurance Memorandum Rubric

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Context, Dependencies & Scenario (15%)	Material services, stakeholders, dependencies, exposure pathways, causal logic, and uncertainty are precise	Strong scenario with minor gaps	Basic scenario and context	Scenario arbitrary or incoherent
Impact & Evidence Analysis (25%)	Cyber, operational, financial, environmental, social, rights, and stakeholder consequences are rigorously evidenced	Strong analysis with minor gaps	Basic analysis with limited integration	Material impacts or evidence missing
Controls, Options & Residual Risk (25%)	Options are critically compared for effectiveness, feasibility, side effects, resilience, and residual risk	Sound comparison with minor gaps	Basic comparison and controls	Options or controls unsupported
Responsibility, Continuity & Communication (15%)	Ethics, legal context, continuity, recovery, safe disclosure, and affected stakeholders are integrated	Responsible treatment with minor gaps	Basic safeguards	Material responsibilities omitted
Recommendation, Triggers & Assurance (15%)	Actions, ownership, thresholds, evidence, escalation, monitoring, and review are compelling	Practical recommendation with minor gaps	Basic recommendation and monitoring	Recommendation unclear or impractical
Professional Quality & AI Transparency (5%)	Concise, fully cited, auditable, safely disclosed, and transparently documented	Professional with minor issues	Adequate but uneven	Unsafe, unclear, poorly sourced, or opaque

8. Final Project: Integrated Governance, Cybersecurity & Sustainability Assurance Plan (Summative Assessment 3) - 40%

Learning Outcomes Addressed: All course learning outcomes (CLO1-CLO5)

8.1 Project Overview

The final project is the signature assessment of Course 5 and a primary-evidence assessment in the MBA common trunk. Students assess an organization's AI, data, cybersecurity, governance, ethical, and sustainability exposures and design a proportionate assurance and improvement plan for executive or board consideration.

8.2 Project Scope

Each student selects an approved organization, business unit, program, or bounded portfolio for which lawful, non-confidential, and sufficiently reliable information is available. Suitable contexts include AI adoption, data-intensive operations, digital transformation, third-party concentration, cyber resilience, sustainability transition, governance redesign, or an integrated risk and assurance challenge.

8.3 Deliverables

Board Assurance Paper and Evidence Portfolio (3,500-4,500 words, excluding appendices)

1. Executive Assurance Summary: Scope, criteria, material exposures, current assurance, priorities, residual risk, and decisions requested
2. Context and Governance: Purpose, strategy, stakeholders, obligations, risk appetite, roles, committees, three lines, accountability, and decision rights
3. AI and Data Assurance: Inventory, lifecycle, classification, impacts, trustworthy-AI characteristics, privacy, human oversight, controls, monitoring, and evidence
4. Cybersecurity and Resilience Assurance: Critical services, assets, threats, vulnerabilities, profiles, controls, third parties, incidents, continuity, recovery, and testing
5. Sustainability Assurance: Dependencies, impacts, risks, opportunities, materiality, value chain, climate, metrics, targets, transition, disclosure, claims, and evidence quality
6. Integrated Risk and Control Evaluation: Interdependencies, scenarios, control effectiveness, gaps, conflicts, residual risk, opportunities, and proportionate priorities
7. Improvement and Assurance Roadmap: Actions, owners, resources, sequencing, capabilities, measures, thresholds, audit trail, escalation, review, and adaptation
8. Evidence and AI Record: Dated authoritative sources, criteria, inventories, registers, reproducible analysis, limitations, independent judgment, reflection, and full disclosure

Executive or Board Presentation and Oral Defence (12-15 minutes plus 5-10 minutes for questions)

- Present during the Week 14 synchronous session
- 10-12 slides or equivalent board-ready visual narrative supported by integrated risk, control, scenario, metric, and assurance evidence
- Respond to questions about scope, criteria, sources, classifications, impacts, threat and control reasoning, materiality, evidence, trade-offs, priorities, and implementation
- Professional, accessible, and interculturally responsive communication with safe disclosure, clear attribution, and independent graduate mastery expected

8.4 Project Timeline & Milestones

Week	Milestone	Deliverable	Weight
Week 9	Assurance Scope & Criteria	Organization, portfolio, boundaries, criteria, stakeholders, evidence access, and approval	Formative feedback

Week	Milestone	Deliverable	Weight
Week 12	Integrated Risk & Control Review	Inventories, profiles, materiality, scenarios, controls, residual risk, and priorities	Peer/instructor review
Week 13	Complete Draft & Challenge	Board paper, assurance portfolio, roadmap, presentation, and AI record	Instructor feedback
Week 14	Final Presentation & Defence	Final assurance package, presentation, and individual defence	40% of final grade

8.5 Final Project Grading Rubric

Board Assurance Paper and Evidence Portfolio (70% of Final Project Grade)

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Scope, Governance & Assurance Criteria (15%)	Decision-ready scope and criteria connect strategy, stakeholders, accountability, appetite, and assurance	Strong foundation with minor gaps	Basic foundation with limited integration	Scope or criteria unreliable
AI & Data Assurance (15%)	Lifecycle, inventory, impacts, rights, trustworthiness, oversight, controls, monitoring, and evidence are critically integrated	Strong assurance with minor gaps	Basic assurance with limited depth	Material AI or data exposures omitted
Cybersecurity & Resilience Assurance (15%)	Services, assets, risks, controls, third parties, incidents, continuity, recovery, and testing are coherently assessed	Strong assurance with minor gaps	Basic assurance with limited depth	Material cyber or resilience gaps
Sustainability Assurance (15%)	Dependencies, impacts, risks, opportunities, materiality, climate, value chain, metrics, claims, and evidence are critically assessed	Strong assurance with minor gaps	Basic assurance with limited depth	Material sustainability issues omitted
Integrated Risk, Controls & Priorities (15%)	Interdependencies, scenarios, effectiveness, conflicts, residual risk, and proportionality support compelling priorities	Strong integration with minor gaps	Basic integration and priorities	Priorities unsupported or siloed

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Roadmap, Governance, Metrics & Adaptation (15%)	Actions, ownership, resources, sequencing, measures, thresholds, assurance, escalation, and review are actionable	Practical roadmap with minor gaps	Basic roadmap and measures	Roadmap vague or impractical
Evidence, Limitations, AI Transparency & Professional Quality (10%)	Board-ready, fully cited, auditable, safe, current, calibrated, and transparently disclosed	Professional with minor issues	Adequate but uneven	Unsafe, unprofessional, unreliable, or opaque

Executive or Board Presentation and Oral Defence (30% of Final Project Grade)

Criteria	Excellent (4)	Good (3)	Satisfactory (2)	Needs Improvement (1)
Board Assurance Narrative (30%)	Compelling narrative connects exposures, evidence, controls, residual risk, priorities, and decisions	Clear narrative with sound prioritization	Adequate narrative with gaps	Unclear or unsupported narrative
Risk, Control & Assurance Visuals (25%)	Accurate, accessible visuals make interdependencies, evidence, gaps, roadmap, and trade-offs immediately understandable	Professional visuals support the decision	Basic visuals with limited analytical value	Visuals inaccurate, unsafe, inaccessible, or absent
Executive & Intercultural Presence (20%)	Confident, concise, accessible, and responsive to diverse board and stakeholder perspectives	Professional delivery and engagement	Adequate delivery with limited adaptation	Unprofessional or ineffective delivery
Oral Defence (25%)	Responses demonstrate independent mastery of criteria, evidence, risk, controls, residual risk, ethics, limits, and implementation	Sound responses demonstrate strong understanding	Basic responses with some uncertainty	Unable to explain evidence or defend judgment

9. Course Learning Outcomes, Program Outcomes, and Assessment Alignment

Course Learning Outcome	Assurance Labs	AI Assessment	Midterm	Scenario Memo	Final Plan
CLO1	✓	✓✓	✓✓	✓✓	✓✓

Course Learning Outcome	Assurance Labs	AI Assessment	Midterm	Scenario Memo	Final Plan
CLO2	✓	✓✓	✓✓	✓	✓✓
CLO3	✓	✓	✓✓	✓✓	✓✓
CLO4	✓	✓	✓	✓✓	✓✓
CLO5	✓	✓	✓	✓✓	✓✓

Key: ✓ = Addressed | ✓✓ = Primary Focus

10. Course Policies

10.1 Attendance & Participation

Regular attendance and active participation in synchronous sessions are essential for success in this course. Students are expected to attend all scheduled synchronous sessions with cameras enabled. If you must miss a session, please notify the instructor in advance. More than two unexcused absences may result in a reduced participation grade.

10.2 Late Submission Policy

- Assignments submitted within 24 hours of deadline: 10% penalty
- Assignments submitted 24-48 hours late: 20% penalty
- Assignments submitted more than 48 hours late: not accepted without prior approval
- Extensions may be granted for documented emergencies with advance notice

10.3 Academic Integrity

All work submitted must be your own original work. Plagiarism, including the use of AI-generated content without proper disclosure, is a serious academic offense. All sources must be properly cited. Violations of academic integrity will result in a zero for the assignment and may lead to further disciplinary action.

10.4 AI Usage Policy

Artificial intelligence may support selected discovery, comparison, inventory, risk, control, scenario, measurement, and communication activities in this course, but students remain accountable for every source, classification, data element, risk judgment, control, assurance conclusion, and recommendation.

1. Assessment Conditions: The Week 7 midterm examination is completed without generative AI unless the instructor expressly authorizes a specific tool or accommodation.
2. Transparency and Provenance: Every AI-assisted submission must include an AI Usage Statement identifying tools, purposes, material prompts, outputs used, information supplied, verification steps, limitations, and substantive human revisions.
3. Verification, Current Authority, and Professional Limits: AI output is not evidence. Laws, standards, threats, incidents, climate information, disclosures, and organizational conditions change. Students must use dated authoritative sources, distinguish mandatory requirements from voluntary guidance, identify jurisdiction and applicability, and avoid presenting course work as legal, audit, certification, engineering, or professional-security assurance.

4. Privacy, Security, Confidentiality, and Safe Disclosure: Personal, sensitive, confidential, client, proprietary, security-restricted, or operationally dangerous information must not be entered into public AI systems or unnecessarily reproduced. Course work must use lawful access, data minimization, responsible disclosure, safe simulation, and institutionally approved storage; it must never facilitate unauthorized access, evasion, harm, or deceptive sustainability claims.

10.5 Communication Expectations

The instructor will respond to emails within 48 hours during the work week. For urgent matters, please indicate 'URGENT' in the subject line. Course announcements will be posted on the LMS. Students are expected to check the LMS and their university email daily.

10.6 Accessibility & Accommodations

Focus University Institute is committed to providing equal access to all students. Students requiring accommodations should contact the Disability Services Office and the instructor at the beginning of the term. Reasonable accommodations will be made to ensure full participation in all course activities.

10.7 Netiquette Guidelines

Online learning requires respectful, professional communication. When participating in synchronous and asynchronous discussions, please use professional language, be respectful of diverse perspectives, avoid all-caps (which reads as shouting), and provide constructive feedback. Remember that cultural differences may affect communication styles.

11. Additional Resources

11.1 Library & Research Support

- Focus University Institute Library: Governance, enterprise risk, AI, cybersecurity, privacy, law, ethics, sustainability, accounting, climate, management, and interdisciplinary research databases
- Research Librarian consultations available for authoritative legal, regulatory, standards, company, incident, sustainability, and methodological evidence

11.2 Writing & Academic Support

- Writing and Learning Support: Graduate risk analysis, evidence evaluation, board writing, quantitative reasoning, visualization, presentation, and study consultations
- APA Citation Guide: Purdue OWL (owl.purdue.edu)

11.3 Technical Support

- IT Help Desk: LMS, account, spreadsheet, secure-storage, visualization, presentation, accessibility, and approved-tool support

- Risk-register, framework-crosswalk, source-verification, safe-disclosure, privacy, accessibility, incident-simulation, and AI Usage Statement tutorials in the course 'Getting Started' module

11.4 Professional Development

- NIST AI RMF, AI Resource Center, and CSF 2.0: Open governance, risk, testing, control, profile, and implementation resources
- EUR-Lex, ENISA, EDPB, OECD, and UNESCO: Current European and international AI, cybersecurity, privacy, ethics, rights, and governance sources
- IFRS Foundation, GHG Protocol, company disclosures, and relevant regulators: Sustainability, climate, value-chain, metrics, claims, and disclosure evidence

11.5 Suggested Bibliography (APA 7)

European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj
European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
International Sustainability Standards Board. (2023a). IFRS S1: General requirements for disclosure of sustainability-related financial information. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s1-general-requirements/
International Sustainability Standards Board. (2023b). IFRS S2: Climate-related disclosures. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2-climate-related-disclosures/
Kshetri, N. (2021). Cybersecurity management: An organizational and strategic approach. University of Toronto Press.
National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1
Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
Tabassi, E. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1
United Nations Educational, Scientific and Cultural Organization. (2021). Recommendation on the ethics of artificial intelligence. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence
Organisation for Economic Co-operation and Development. (2024). OECD Principles on Artificial Intelligence. https://oecd.ai/en/ai-principles

12. Syllabus Disclaimer

This syllabus represents a plan for the course and may be modified at the instructor's discretion based on pedagogical needs, material changes in technologies, threats, incidents, laws, regulations, standards, sustainability evidence, organizational conditions, source availability, or unforeseen circumstances. Students will be notified of significant changes

through the LMS and email. Continued enrollment constitutes acceptance of such modifications.

Focus University Institute

Madrid, Spain