COURSE SYLLABUS

Cyber GRC Certificate Program

A four-course federal GRC path: risk assessment and quantification, cybersecurity supply chain risk management, security and privacy program management, and CMMC 2.0 readiness.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/certificates/cyber-grc-certificate-program

support@graduateschool.edu •
(888) 744-4723

Course Outline

This package includes these courses

- Understanding CMMC 2.0 for Federal Contractors (3 hours)
- Cyber Risk Management & GRC: From Risk to Assurance Course (12 Hours)
- Cybersecurity Supply Chain Risk Management (C-SCRM) Course (12 Hours)
- Security & Privacy Program Management: From Governance to Assurance Course (12 Hours)

Understanding CMMC 2.0 for Federal Contractors

A plain-language overview of CMMC 2.0 for federal contractors - what it is, who must comply, the maturity levels, and the rollout timeline you need to plan around.

- Explain what CMMC 2.0 is and why it exists.
- Identify who must comply.
- Describe the maturity levels and what they require.
- Understand the assessment and certification path.
- Know the rollout timeline and key deadlines.
- Plan your organization's next steps.

Cyber Risk Management & GRC: From Risk to Assurance Course

An intermediate pass through cyber governance, risk and compliance, from governance and assessment through quantification, registers, controls, assurance, third-party risk, and board-level reporting.

- Governance, risk and compliance defined, and cybersecurity risk distinguished from enterprise risk
- Governance structures, risk appetite and tolerance, and decision authority
- Scoping and conducting a cyber risk assessment
- Prioritizing risk by organizational impact and selecting a defensible response
- Qualitative ratings versus quantification, and the FAIR model applied

- A materiality determination under the SEC disclosure criteria
- A cybersecurity risk register structured to NIST IR 8286A
- Mapping risks to controls, and implementation versus effectiveness
- Third-party and supply-chain risk at the enterprise-governance level
- Key risk indicators, thresholds, and communicating risk to nontechnical stakeholders

Cybersecurity Supply Chain Risk Management (C-SCRM) Course

Intermediate cybersecurity supply chain risk management on the NIST SP 800-161r1 structure, from criticality and supplier assessment through acquisition, controls, software supply chain and lifecycle monitoring.

- C-SCRM defined and separated from traditional supply chain risk
- Threat sources: counterfeit and compromised components, firmware tampering, supplier compromise
- Criticality and dependency analysis, single points of failure, concentration risk
- The three C-SCRM levels and escalating risk to the right decision-maker
- Strategy, policy and system-level plans coordinated across security, acquisition, legal and procurement
- Evidence-based supplier due diligence and risk scoring
- Security requirements in agreements, including flow-down to subcontractors
- The SP 800-53 SR control family, SR-1 through SR-12
- SBOM, VEX, build-integrity levels and project-health tooling
- AI and machine learning supplier assessment and provenance
- Cryptographic inventory and agility in due diligence
- Continuous monitoring, supplier incidents, end-of-life and transitions

Security & Privacy Program Management: From Governance to Assurance Course

An organization-wide course on running security and privacy as a single program: governance and accountability, strategy, risk, controls, assurance, monitoring, and leadership reporting.

- Program management distinguished from system operations, and cybersecurity risk from privacy risk
- Governance structures, decision rights, escalation paths, and who may accept risk
- CISO and Senior Agency Official for Privacy statutory responsibilities, separated from CIO and agency head
- Program strategy, multi-year roadmap, and resource estimates tied to mission outcomes
- FIPS 199 categorization and how it drives baseline selection
- Information flow mapping, data minimization, and when a Privacy Impact Assessment is required
- Control baseline selection and tailoring justified in risk terms that survive oversight
- Evaluating assessment evidence, documenting findings, and tracking POA&Ms
- Security and privacy integrated into each SDLC phase
- Monitoring strategy, and actionable metrics distinguished from activity-only measures
- Determining when an incident is a PII breach and what reporting follows
- Delivering and defending a leadership risk briefing framed around a decision