COURSE SYLLABUS

Cyber GRC Certificate Program (Self-Paced)

Work through federal GRC at your own pace: risk assessment and quantification, 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-self-paced

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

Course Outline

This package includes these courses

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

Understanding CMMC 2.0 for Federal Contractors (Self-Paced)

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 (Self-Paced)

Intermediate cyber governance, risk and compliance covering the full arc from governance and risk assessment through quantification, registers, controls, assurance, third-party risk, and reporting to leadership.

- GRC defined, and cybersecurity risk distinguished from enterprise risk
- Governance structures, risk appetite and tolerance, and who holds decision authority
- Scoping and conducting a cyber risk assessment end to end

- Prioritizing by organizational impact and selecting a defensible response
- Qualitative ratings versus quantification, with the FAIR model applied
- Materiality determinations under the SEC disclosure criteria
- Risk registers structured to NIST IR 8286A and staged for enterprise oversight
- Risk-to-control mapping, and implementation versus effectiveness
- Enterprise-level third-party and supply-chain risk
- Key risk indicators, thresholds, and communicating risk to nontechnical audiences

Cybersecurity Supply Chain Risk Management (C-SCRM) Course (Self-Paced)

An intermediate practitioner course in cybersecurity supply chain risk management built on NIST SP 800-161r1, spanning criticality, supplier assessment, acquisition, controls, software supply chain and lifecycle monitoring.

- Cybersecurity supply chain risk distinguished from traditional supply chain risk
- Supply chain threat sources, including counterfeit components, firmware tampering and supplier compromise
- Criticality and dependency analysis, single points of failure and concentration risk
- Organization, mission and business-process, and system-level C-SCRM, and escalation to the right decision-maker
- C-SCRM strategy, policy and system-level planning across security, acquisition, legal and procurement
- Evidence-based supplier due diligence and risk scoring
- Security requirements written into agreements, with flow-down to subcontractors
- The NIST SP 800-53 SR control family, SR-1 through SR-12
- Software supply chain risk via SBOM, VEX, build-integrity levels and project-health tooling
- AI and machine learning supplier assessment, including model and training-data provenance
- Cryptographic inventory and agility as due-diligence questions
- Continuous supplier monitoring, incident response, end-of-life and supplier transitions

Security & Privacy Program Management: From Governance to Assurance Course (Self-Paced)

Program-level training that runs security and privacy as a single organization-wide program, from governance and strategy through risk, controls, assurance, monitoring, and leadership reporting.

- Program management versus system operations, and cybersecurity risk versus privacy risk
- Governance structure, decision rights, escalation, and risk acceptance authority
- CISO and SAOP statutory responsibilities separated from CIO and agency head
- Program strategy, roadmap, and resourcing tied to mission outcomes
- FIPS 199 categorization driving baseline selection
- Information lifecycle mapping, data minimization, and PIA triggers
- Baseline selection and tailoring defensible under oversight
- Assessment evidence, findings, and POA&M remediation tracking
- Security and privacy across each SDLC phase
- Monitoring strategy and actionable, manipulation-resistant metrics
- Determining when an incident is a PII breach and the reporting that follows
- Delivering and defending a decision-framed leadership risk briefing