COURSE SYLLABUS

Cybersecurity Supply Chain Risk Management (C-SCRM)

Twelve hours live on cybersecurity supply chain risk management, built on NIST SP 800-161r1 and current to August 2026 on supply chain regulation — criticality, supplier due diligence, procurement, software supply chain, and monitoring.

Group classes (Live Online) and onsite training are available for this course. For more information, email corporate@nobledesktop.com or visit: https://www.nobledesktop.com/classes/cybersecurity-supply-chain-risk-management-c-scrm



hello@nobledesktop.com • (212) 226-4149

Course Outline

Module 1

- Know Your Chain: C-SCRM Foundations
- Defining C-SCRM
- Traditional versus cybersecurity supply chain risk
- Products, services, suppliers, developers, integrators and service providers
- First-party, third-party and downstream relationships
- Dependencies and inherited risk
- Why reduced visibility creates risk

Module 2

- Where Risk Enters: Supply Chain Threats and Vulnerabilities
- Threat sources
- Counterfeit, compromised and malicious components
- Software and firmware tampering
- Vulnerable or malicious third-party software
- Supplier and service-provider compromise
- Insider risk within the supply chain
- Supplier disruption and loss of availability

Module 3

- See What Matters: Criticality and Dependency Analysis
- Identifying critical systems, components, data and services
- Mission and business dependencies
- Critical suppliers

- Single points of failure
- Concentration and systemic risk
- Upstream and downstream dependencies
- Prioritizing resources by criticality

Module 4

- Three Levels, One Risk Picture: Integrating C-SCRM into Risk Management
- C-SCRM within enterprise risk management
- Organization, mission and business-process, and system levels
- Risk appetite and tolerance
- Roles across levels
- Escalation to decision-makers
- Connecting to the Risk Management Framework and to supply chain's place in the Govern function of Cybersecurity Framework 2.0

Module 5

- Build the Program: C-SCRM Strategy, Policy, and Planning
- Developing a strategy
- Policies and procedures
- Implementation planning
- System-level C-SCRM plans
- Governance and accountability
- Coordinating cybersecurity, acquisition, legal, procurement and operations
- Measuring and improving capability

Module 6

- Know Your Supplier: Supplier Risk Assessment
- Identifying and categorizing suppliers
- Determining criticality
- Evaluating supplier cybersecurity practice
- Assessing products and services before acquisition
- Sources of supplier risk information
- Evidence-based assessment across foreign ownership, control or influence, provenance, resilience, foundational cyber practices and supply chain tiers
- Risk scoring
- When additional assurance is required

Module 7

- Security Before the Signature: Acquisition and Supplier Requirements
- Integrating cybersecurity into acquisition
- Defining and communicating security requirements before procurement
- Requirements in agreements and contracts
- Flow-down to subcontractors
- Supplier notification and incident-reporting expectations
- Vulnerability disclosure and remediation
- Authenticity, provenance and integrity
- Acquisition strategies that reduce exposure

Module 8

- Trust but Verify: Supply Chain Controls and Assurance
- The SP 800-53 Supply Chain Risk Management control family
- SR-1 through SR-12
- Supply chain risk management plans
- Supplier assessments and reviews
- Tamper resistance and detection
- Component authenticity
- Supplier notification agreements
- Inspection of systems and components
- Component disposal
- Selecting controls by organizational risk

Module 9

- Software in the Chain: Software Supply Chain Risk
- Software as a dependency
- Commercial, open-source and internally developed software
- Third-party libraries
- Provenance and integrity
- SBOM formats including SPDX and CycloneDX
- VEX and exploitability context
- Build-integrity levels
- Project-health and artifact-signing tooling
- Patch integrity
- Risks in build and development environments

Module 10

- Stay Ahead of the Chain: Monitoring and Response
- Continuous monitoring of suppliers
- Tracking changes in supplier risk
- Vulnerability and threat intelligence
- Supplier security incidents
- Supply chain incident response
- Reassessment triggers
- Changes in ownership, products or services
- Risk acceptance, mitigation, transfer, avoidance and sharing
- Updating the risk register

Module 11

- From Supplier to Sunset: Lifecycle C-SCRM
- C-SCRM across the system development lifecycle
- Planning and acquisition
- Development and integration
- Operations and maintenance
- Supplier changes and replacement

- End-of-life and end-of-support risk
- Secure component disposal
- Data and credential protection during supplier transitions

Module 12

- Put It Together: C-SCRM Scenario Workshop
- Identify assets, suppliers and dependencies in a sample environment, determine which are most critical, build threat scenarios, assess likelihood and impact, evaluate supplier evidence, select risk responses and controls, draft supplier security requirements, document a risk register and justify a C-SCRM decision

Module 13

- The Ground Is Moving: Regulatory Currency and Emerging Domains
- AI and machine learning supply chain risk including model and training-data provenance, malicious models in public repositories, and vendor-disclosure obligations for procured AI
- Post-quantum cryptography as a supply chain domain, cryptographic inventory and agility as due-diligence questions, and the 2030 federal compliance deadline
- And how to verify whether a federal clause, prohibition or deadline is still in force