COURSE SYLLABUS

Cyber Risk Management & GRC: From Risk to Assurance

A full pass through governance, risk and compliance — including FAIR quantification and an applied SEC materiality determination — for the person who has to turn technical findings into a defensible risk decision.

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/cyber-risk-management-and-grc



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

Course Outline

Module 1

- Risk Is the Business: Cyber Risk & GRC Foundations
- Defining GRC
- Cybersecurity risk versus enterprise risk via COSO and ISO 31000
- Assets, threats, vulnerabilities, likelihood and impact
- Emerging and AI-specific risk
- Inherent versus residual risk
- Risk and control owners

Module 2

- Set the Rules: Governance, Strategy & Accountability
- Policies, standards, procedures and guidelines
- Roles and responsibilities
- Risk appetite and tolerance
- Governance committees and decision authorities
- NIST CSF 2.0 Govern including the GV.SC supply-chain category
- Federal authorizing officials compared to commercial boards and audit committees

Module 3

- Find the Risk: Cyber Risk Assessment
- Scope and context
- Critical assets and business dependencies
- Threat sources and threat-event scenarios
- Vulnerabilities and predisposing conditions

- Likelihood and impact
- NIST SP 800-30 compared with ISO/IEC 27005:2022

Module 4

- Make the Call: Risk Analysis, Quantification & Response
- Interpreting results
- Prioritization
- Acceptance, avoidance, mitigation, transfer and sharing
- Qualitative ratings versus quantification
- The FAIR model and FAIR-MAM
- Escalation
- SEC materiality determination

Module 5

- From Findings to Action: Risk Registers & Treatment Plans
- The risk register per NIST IR 8286A Rev. 1
- Writing risk statements
- Causes, events and consequences
- Risk owners
- Staging risks for enterprise risk management per IR 8286C Rev. 1
- POA&Ms and their basis in OMB Circular A-130

Module 6

- Controls Change Risk: Security Controls & Frameworks
- Purpose of controls
- Administrative, technical and physical
- Preventive, detective, corrective and recovery
- Selection and tailoring
- Common, system-specific and hybrid
- Implementation versus effectiveness
- The NIST SP 800-53 Rev. 5 Release 5.2.0 families

Module 7

- Trust but Verify: Compliance, Assessment & Assurance
- Risk management versus compliance
- Control objectives
- Internal versus independent assessment
- Objective evidence
- Examine, interview and test methods per SP 800-53A
- Deficiencies and findings
- Compensating controls and exceptions

Module 8

- Risk Beyond Your Walls: Third-Party & Supply Chain Risk
- Enterprise-level third-party oversight distinguished from acquisition-level C-SCRM
- Supplier criticality

- Supply-chain threats
- Security requirements in acquisitions
- Flow-down to subcontractors
- DORA as a regulator-mandated example

Module 9

- Risk Never Stands Still: Monitoring, Metrics & Reporting
- Continuous monitoring as a risk activity
- Control effectiveness per SP 800-137A
- Key risk indicators versus key performance indicators
- Thresholds and escalation triggers
- Dashboards including quantified loss exposure
- Board communication per the NACD handbook

Module 10

- From Analyst to Advisor: GRC Risk Workshop
- Applied exercise on a fictional organization covering scenarios, quantification, register entries, control gaps, third-party risk, a materiality call, and a defended treatment recommendation