COURSE SYLLABUS

Security & Privacy Program Management: From Governance to Assurance Course

Twelve hours live on running security and privacy as one program — governance, strategy, risk, controls, assurance, and a defended leadership briefing.

> Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/security-and-privacy-program-management



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

Course Outline

Module 1

- Two Missions, One Program: Security & Privacy Foundations
- Program management versus system operations
- Cybersecurity risk versus privacy risk including risk from authorized processing
- Shared and distinct objectives
- Confidentiality, integrity and availability related to predictability, manageability and disassociability
- The federal program authorities

Module 2

- Who Owns the Risk? Governance, Roles & Accountability
- Centralized, federated and hybrid governance
- Responsibilities at executive, program, system and control levels
- Authorizing official, risk executive, system owner, control owner and program manager
- CISO and SAOP statutory responsibilities
- Decision rights and escalation
- Risk appetite versus tolerance

Module 3

- Build the Program: Strategy, Policy & Planning
- Linking activities to mission outcomes
- Translating drivers into traceable requirements
- Policy, standard, procedure and guideline
- Multi-year roadmap

- Measurable objectives with owners
- Staffing, skills, funding and tooling estimates
- Role-based training
- Records evidencing governance decisions

Module 4

- Know the Risk: Security & Privacy Risk Management
- Framing risk context
- Threats, vulnerabilities, predisposing conditions and problematic data actions
- Assessing security risk and privacy impact on individuals
- Inherent versus residual risk
- FIPS 199 categorization
- Prioritizing against mission
- Selecting and approving responses
- The risk register

Module 5

- Follow the Data: Privacy Risk & Information Lifecycle
- PII versus sensitive PII and how aggregation changes sensitivity
- Mapping flows from collection to disposal
- Data minimization and data held without a current purpose
- Documented purpose and legal authority
- Notice, access, amendment and consent including SORNs
- When a Privacy Impact Assessment is required
- Retention and sanitization

Module 6

- Controls Make It Real: Security & Privacy Controls
- Controls as operationalized risk decisions
- Navigating the SP 800-53 catalog including privacy controls
- Organization-level versus system-level
- Common, system-specific and hybrid
- Baseline selection and tailoring through scoping, compensating controls and parameters
- Documenting in a system security and privacy plan

Module 7

- Prove It Works: Assessment, Compliance & Assurance
- Implementation versus effectiveness, compliance versus assurance
- Assessment scope, procedures and determination statements
- Examine, interview and test
- Judging evidence sufficiency
- Findings stating condition, criteria, cause and risk
- POA&Ms
- How results inform authorization and ongoing authorization

Module 8

- Privacy by Design, Security by Design
- Integrating into each SDLC phase
- Testable design-phase requirements
- Least privilege, least functionality, separation of duties and defense in depth in design review
- Minimization and purpose limitation in architecture
- Assessing privacy risk before implementation
- Change management
- Influencing engineering and acquisition early

Module 9

- Keep Watch: Monitoring, Metrics & Program Improvement
- Monitoring strategy and frequencies driven by volatility, impact level and risk
- KPIs versus KRIs
- Testing whether a metric is actionable and manipulation-resistant
- Tracking vulnerabilities, incidents, findings and corrective actions
- Reporting in mission language framed around a decision

Module 10

- When Things Change: Incidents, Third Parties & Emerging Risk
- Security and privacy roles across the incident lifecycle
- Determining when an incident is a PII breach and the reporting obligations
- Third-party and supply chain risk across the acquisition lifecycle
- Contract terms for security, privacy, incident reporting and assessment rights
- Evaluating emerging technology including AI
- When change requires reassessment, reauthorization or an updated PIA

Module 11

- From Program Manager to Advisor: Security & Privacy Workshop
- Evaluate a fictional federal organization, diagnose governance and accountability gaps separating root causes from symptoms, rank risks with rationale, locate ineffective control coverage, prioritize corrective actions by risk reduction against cost, and deliver and defend a leadership briefing