PROFESSIONAL DEVELOPMENT & CONTINUING EDUCATION

SECURITY CENTER of EXCELLENCE

Harrisburg University

Information Security Leader
ISO / ISSO (Officer)

7 Modules (84 Hours)

Attention - IT Security Leaders and Professionals

The Information Security Leader Certificate provides a unique focus on the leadership components expected and required to empower the proper IT Security culture within private businesses and public organizations. This course targets candidates responsible for (or who collaborate with) IT Security, to develop the knowledge & skills necessary to succeed at the executive level.

Module 1: Information Security Leadership Skills

Creating a security culture within your organization by leading people, managing programs, and applying continuous learning:

- Addressing cybersecurity as a Business Function.
- Opportunities to build security leadership skills and 360 communications.
- Communicate infosec operational goals, direction, and business impact to c-suite officers and board of directors.
- Establishing a Collaborative environment with internal / external stakeholders, partners, investors, compliance agencies, legal, etc.
- Examining the Financial and Budgetary skills security leaders require to garner the proper funding support.

Module 2: Information Risk Management and Implementation

Identifying acceptable organizational risk thresholds and developing a risk management program:

- Establishing a Security / Privacy Compliance baseline and a Risk Management program
- Performing a security health assessment to identify gaps & opportunities while evaluating employee behaviors & organizational culture
- Determine required security and awareness training at organization level and certification requirements for security/privacy team(s).
- Defining and Instituting Data Identification, Classification, Loss, and Fraud Prevention (basis for Data Governance).
- Developing a Foundational Security Roadmap and identifying the correlation between the Roles & Responsibilities of the teams surrounding Compliance, Contingency, Incident Response and Disaster Recovery
- Exploring the NIST Risk Management Framework (RMF) / NIST Cybersecurity Framework (CSF)

Module 3: Information Security Governance

Establishing and maturing internal governance processes to ensure all the below initiatives run smoothly and receive the required funding and that corporate leadership understands the importance:

- Creating a Change Management Control Group, Data Governance Board, and a Technical Review Board.
- Establishing security in the Strategic Plan, Budget, Supply Chain and Vendor Management.
- Identifying security and privacy policies, procedures and specifically crafting an Incident Response Plan.
- Aligning the IT Security Roadmap with the Core Business Strategy
- Deploying the methodology of DevSecOps within the organizational culture.

Module 4: Information Security Architecture Management

Discuss a mature organizational posture that mitigates vulnerabilities and risks:

- Expanding the Zero Trust framework beyond the traditional in-network boundaries to include Remote Users, Bring Your Own Devices (BYOD) and Cloud-Based assets.
- Establish and understand the organizational data footprint including data centers.
- Align IT Security with the Core Business Strategy.
- Explore Silo-based Architecture vs Enterprise Architecture
- Understand the differences between Physical, Technical, and Administrative Controls
- Addressing the presence of Cryptography by requirement, measure, and application.

Module 5: End to End Security Operations and Continuous Monitoring

Developing a proactive culture around security operations, ongoing monitoring, and preemptive responsiveness:

- Exploring, managing, and maintaining the types of hardware / software tools used for continuous monitoring & correlated intel.
- Understanding how to implement the defense in-depth model (layered security).
- Utilize a Threat-Hunting team via agile processes to assess emerging risks, trends, and technologies.
- Managed Support Services (MSS) vs. in-house Security Operations Center (SOC).
- Briefing Executive Level Leaders – Frequency, Techniques, and Dashboards.
- Developing, Testing, and Implementing a Business Continuity Plan (BCP), Continuity of Operations Plan (COOP), Disaster Recovery Plan (DRP), Incident Response Plan (IRP) - and conducting corresponding Tabletop Exercises.

Module 6: Ownership, Authorization and Prioritization Process

Establish executive sponsorship to ultimately develop an "Ongoing Authorization" Culture:

- Analyze risk assessment thresholds at the enterprise vs. the program level through regular reviews at defined frequency.
- Risk Based Prioritization and the critical components surrounding cost, resources, impact, probability, etc....
- Defining and Embodying the Authorization to Operate (ATO) process used within public sector organizations
- Ongoing Authorization and Assessments against the Security Privacy Control baseline.

Module 7: Capstone

Course objectives are synthesized into an applied project – for example: the student may develop a comprehensive security centric maturity index for their organization or participate in a community-based project that involves the entire class. This capstone will include an executive summary and formal classroom presentation describing results and an action plan.