Certified Third Party Security Manager

Course Duration: 32 Hours **Course code: CTPSM**

1. Course Overview

This certification course equips participants with the knowledge and skills to manage, assess, and secure third-party relationships in organizations. It focuses on identifying risks, implementing security frameworks, ensuring compliance, and managing vendor contracts to protect organizational data and systems.

2. What you'll learn?

- Understand third-party and supply chain risk management concepts.
- Assess vendor risks and security postures.
- Implement third-party security policies and frameworks.
- Manage compliance requirements (GDPR, ISO 27001, NIST, etc.).
- Monitor, audit, and enforce third-party security controls.
- Build and manage vendor risk management (VRM) programs.
- Handle incident response and business continuity planning with third parties.

3. Target Audience

- Security Managers and IT Risk Managers.
- Compliance Officers and Governance Professionals.
- Vendor Risk Managers and Procurement Managers.
- IT Auditors, Consultants, and Cybersecurity Professionals.
- Professionals seeking certification in third-party risk/security management.

4. Pre-Requisites

- Basic knowledge of information security and risk management.

- Familiarity with compliance frameworks (ISO, GDPR, NIST, etc.) preferred.
- Experience in vendor management or IT governance is beneficial.

5. Course content

Module 1: Introduction to Third Party Security Management

- Definition of third-party/vendor risks
- Common threats in supply chain security
- Regulatory drivers for third-party risk management (TPRM)
- Case studies of third-party breaches

Module 2: Third Party Risk Assessment

- Risk identification and classification
- Due diligence and vendor onboarding process
- Risk scoring models and frameworks
- Practical: Conducting a vendor risk assessment

Module 3: Security Policies and Frameworks

- Building third-party security policies
- Integration with ISO 27001, NIST, and COBIT frameworks
- Service Level Agreements (SLAs) and security addendums
- Practical: Drafting a vendor security policy

Module 4: Compliance and Legal Considerations

- GDPR, HIPAA, PCI-DSS, SOX compliance requirements
- Contract management and legal obligations
- Cross-border data transfer and privacy considerations
- Practical: Compliance checklist for third-party contracts

Module 5: Vendor Risk Management (VRM) Programs

- Establishing a VRM governance structure

- Vendor tiering and classification models
- Ongoing monitoring and periodic assessments
- Tools for VRM (e.g., Archer, OneTrust, Prevalent)

Module 6: Security Monitoring and Auditing

- Continuous monitoring strategies
- Vendor audits and reporting mechanisms
- Security questionnaires and evidence gathering
- Practical: Creating a vendor monitoring dashboard

Module 7: Incident Management with Third Parties

- Coordinating incident response with vendors
- Communication protocols and escalation paths
- Business continuity and disaster recovery planning
- Lessons learned from real-world third-party breaches

Module 8: Emerging Trends in Third Party Security

- Cloud vendor security management
- Fourth-party and subcontractor risks
- AI/ML in vendor risk assessment
- Cyber insurance and third-party liabilities

Module 9: Capstone Project & Certification Exam Prep

- Design a third-party security management plan for a sample organization
- Conduct vendor risk assessment and propose mitigation strategies
- Exam practice questions and review session