QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1943

Cybersecurity Threats, Vulnerabilities & Risk Assessment Training Course

CYBERSECURITY & INFORMATION SECURITY
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cybersecurity Threats, Vulnerabilities & Risk Assessment Training Course provides a comprehensive and practical framework for identifying, analyzing, evaluating, and managing cybersecurity threats, vulnerabilities, and risks across modern organizational environments. The course enables participants to understand how cyber threats emerge, how vulnerabilities can be exploited, and how organizations can systematically assess and prioritize cybersecurity risks.

Participants will examine the evolving cybersecurity threat landscape, including malware, ransomware, phishing, social engineering, credential attacks, insider threats, supply-chain risks, exploitation of software vulnerabilities, cloud security risks, and advanced persistent threats. The course focuses on understanding attack surfaces and identifying weaknesses across applications, networks, endpoints, identities, data, cloud platforms, and critical infrastructure.

The program introduces structured approaches to cybersecurity risk assessment, combining asset identification, threat analysis, vulnerability assessment, likelihood evaluation, business impact analysis, and risk prioritization. Participants will learn how to translate technical security findings into business-oriented risk information that supports management decisions, investment priorities, and security improvement initiatives.

Through practical risk assessment exercises, threat scenarios, vulnerability analysis, risk-rating workshops, attack-surface assessments, and mitigation planning, participants will develop the capabilities required to identify high-priority cybersecurity risks, recommend appropriate controls, communicate risk effectively, and establish a continuous cybersecurity risk management process.

Objectives

- By the end of the course, participants will be able to:
- Analyze the modern cybersecurity threat landscape and emerging attack patterns.
- Identify critical information assets, systems, applications, identities, and infrastructure.
- Assess organizational attack surfaces and exposure points.
- Identify common and emerging cybersecurity vulnerabilities.
- Evaluate threats based on likelihood, capability, intent, and potential impact.

- Conduct structured cybersecurity risk assessments.
- Apply qualitative and quantitative approaches to cybersecurity risk analysis.
- Prioritize vulnerabilities and risks according to business impact and exploitability.
- Analyze the relationship between threats, vulnerabilities, assets, and business consequences.
- Develop risk treatment and cybersecurity mitigation strategies.
- Evaluate security controls and their ability to reduce identified risks.
- Establish cybersecurity risk registers and risk ownership mechanisms.
- Communicate cybersecurity risks effectively to technical and executive stakeholders.
- Develop cybersecurity risk indicators and monitoring mechanisms.
- Build a continuous cybersecurity threat and risk assessment program.

Who Should Attend

This course is designed for cybersecurity professionals, information security specialists, security analysts, risk managers, IT managers, security architects, vulnerability management professionals, security operations teams, and technology specialists responsible for identifying or managing cybersecurity risks.

It is also suitable for governance, risk and compliance professionals, internal auditors, business continuity specialists, enterprise risk professionals, infrastructure and cloud security teams, application security professionals, and managers responsible for cybersecurity governance and risk-based decision-making.

The course is particularly valuable for organizations seeking to improve their understanding of cyber threats, strengthen vulnerability management, establish structured risk assessment processes, and prioritize cybersecurity investments based on business impact and organizational risk.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain major cybersecurity threats and attack techniques.
- Identify organizational assets and critical business dependencies.
- Map attack surfaces across networks, applications, endpoints, identities, cloud environments,

and data.

- Identify vulnerabilities and assess their potential for exploitation.
- Analyze threat actors, attack vectors, motivations, and capabilities.
- Evaluate cybersecurity risks using structured assessment methodologies.
- Determine risk likelihood and potential business impact.
- Prioritize cybersecurity risks and vulnerabilities based on severity and organizational context.
- Develop comprehensive cybersecurity risk registers.
- Design appropriate risk treatment and mitigation plans.
- Evaluate existing security controls and identify control gaps.
- Establish risk ownership, accountability, and escalation mechanisms.
- Communicate cybersecurity risk information to executives and decision-makers.
- Develop risk indicators and continuous monitoring mechanisms.
- Establish a repeatable cybersecurity threat, vulnerability, and risk assessment process.

Course Outline

DAY 01

Cybersecurity Threat Landscape and Attack Surface

- Understanding the modern cybersecurity threat landscape.
- Cyber threats, threat actors, and attack motivations.
- Common cyberattack techniques and attack vectors.
- Malware, ransomware, phishing, and social engineering.
- Credential theft and identity-based attacks.
- Insider threats and malicious or negligent users.
- Supply-chain and third-party cybersecurity threats.
- Advanced persistent threats and targeted attacks.
- Cloud, mobile, remote-work, and hybrid environment threats.
- Identifying organizational attack surfaces.
- Critical assets, business services, and technology dependencies.

DAY 01 — CONTINUED

> **PRACTICAL APPLICATION**
>
> Develop an organizational attack-surface map and identify major threat sources, exposed assets, and critical security dependencies.

DAY 02

Vulnerability Identification and Security Weakness Assessment

- Understanding cybersecurity vulnerabilities and weaknesses.
- Vulnerability types across applications, systems, networks, and endpoints.
- Common configuration and security weaknesses.
- Software vulnerabilities and patch management.
- Application and web security vulnerabilities.
- Network and infrastructure vulnerabilities.
- Identity and access vulnerabilities.
- Cloud security weaknesses.
- Data protection and information security weaknesses.
- Vulnerability discovery and assessment processes.
- Vulnerability severity and exploitability.
- Distinguishing technical vulnerabilities from business risks.

> **PRACTICAL APPLICATION**
>
> Conduct a vulnerability assessment of a simulated technology environment and identify, classify, and prioritize critical weaknesses.

DAY 03

Cybersecurity Risk Assessment and Analysis

- Principles of cybersecurity risk management.
- Asset, threat, vulnerability, and consequence relationships.
- Establishing cybersecurity risk assessment criteria.
- Qualitative risk assessment methodologies.

DAY 03 — CONTINUED

- Quantitative cybersecurity risk assessment concepts.
- Likelihood and impact evaluation.
- Business impact and operational consequences.
- Risk scoring and risk-rating models.
- Threat-based and vulnerability-based risk analysis.
- Identifying systemic and interconnected cybersecurity risks.
- Developing cybersecurity risk scenarios.
- Creating and maintaining cybersecurity risk registers.

PRACTICAL APPLICATION

Perform a complete cybersecurity risk assessment for a representative organization and develop a prioritized risk register.

DAY 04

Risk Treatment, Mitigation, and Security Controls

- Cybersecurity risk treatment strategies.
- Risk avoidance, reduction, transfer, and acceptance.
- Selecting appropriate security controls.
- Preventive, detective, corrective, and compensating controls.
- Identity and access security controls.
- Network and endpoint security controls.
- Vulnerability and patch management controls.
- Data protection and encryption controls.
- Security monitoring and incident response controls.
- Cloud and third-party security controls.
- Developing risk mitigation plans.
- Tracking remediation and residual risk.

DAY 04 — CONTINUED

PRACTICAL APPLICATION

Develop a risk treatment plan for high-priority cybersecurity risks and select appropriate controls to reduce likelihood, impact, and residual exposure.

DAY 05

Cybersecurity Risk Governance, Monitoring, and Continuous Assessment

- Establishing cybersecurity risk governance.
- Defining risk ownership and accountability.
- Risk reporting and escalation mechanisms.
- Cybersecurity risk appetite and tolerance.
- Key risk indicators and security performance measures.
- Continuous threat and vulnerability monitoring.
- Tracking changes in the cybersecurity threat landscape.
- Reassessing risks following major technology or business changes.
- Executive communication and cybersecurity risk reporting.
- Integrating cybersecurity risk with enterprise risk management.
- Building a sustainable vulnerability and risk management program.
- Continual improvement of cybersecurity risk assessment processes.

FINAL WORKSHOP

Develop an integrated Cybersecurity Threats, Vulnerabilities & Risk Assessment Framework covering asset identification, threat analysis, attack-surface assessment, vulnerability identification, risk scoring, prioritization, mitigation, security controls, residual risk, governance, reporting, continuous monitoring, and improvement.

Register or Request More Information

Course page: https://quest-training.com/courses/cybersecurity-threats-vulnerabilities-risk-assessment-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440