QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1941

Cybersecurity Controls, Policies & Security Frameworks Training Course

CYBERSECURITY & INFORMATION SECURITY
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cybersecurity Controls, Policies & Security Frameworks Training Course provides a comprehensive and practical understanding of how organizations can establish, implement, govern, and continuously improve cybersecurity controls, policies, standards, and security frameworks. The course focuses on translating cybersecurity requirements into structured controls that protect information assets, technology environments, business operations, and critical services.

Participants will explore the relationship between cybersecurity governance, risk management, security policies, control frameworks, compliance requirements, and operational security. The program examines how organizations can select and tailor appropriate security frameworks, establish control objectives, define responsibilities, document security requirements, and create measurable mechanisms for assessing control effectiveness.

The course covers the development and implementation of cybersecurity policies across areas such as access control, identity security, data protection, incident management, vulnerability management, network security, endpoint security, cloud security, third-party risk, business continuity, and security awareness. Participants will also learn how to align policies and controls with organizational risk appetite, business priorities, regulatory expectations, and technology environments.

Through practical exercises, control assessments, policy-development workshops, framework mapping, gap analysis, and implementation planning, participants will develop the capabilities required to build a coherent cybersecurity control environment, identify weaknesses, prioritize remediation, support audit readiness, and establish a sustainable cybersecurity governance model.

Objectives

- By the end of the course, participants will be able to:
- Analyze the role of cybersecurity controls and security frameworks in organizational resilience.
- Identify the key components of an effective cybersecurity governance structure.
- Evaluate cybersecurity risks and translate them into appropriate security controls.
- Develop and maintain cybersecurity policies, standards, procedures, and guidelines.
- Map security controls against organizational risks, regulatory requirements, and business

objectives.

- Apply recognized cybersecurity framework principles to enterprise security programs.
- Assess the design and operating effectiveness of cybersecurity controls.
- Conduct structured cybersecurity control gap assessments.
- Prioritize security-control improvements according to risk and business impact.
- Establish ownership, accountability, and governance mechanisms for cybersecurity controls.
- Develop security metrics and key performance indicators for control effectiveness.
- Improve cybersecurity audit readiness and evidence management.
- Align cybersecurity policies and controls across cloud, hybrid, and on-premises environments.
- Strengthen third-party and supply-chain cybersecurity controls.
- Develop a practical cybersecurity controls and governance improvement roadmap.

Who Should Attend

This course is designed for cybersecurity professionals, information security managers, security architects, IT managers, governance specialists, risk professionals, compliance officers, internal auditors, and technology professionals responsible for implementing or overseeing cybersecurity controls.

It is also suitable for professionals involved in cybersecurity governance, enterprise risk management, regulatory compliance, audit, business continuity, technology assurance, cloud security, infrastructure security, and information protection.

The course is particularly valuable for managers and decision-makers responsible for establishing cybersecurity governance structures, improving control maturity, preparing organizations for audits and assessments, and aligning cybersecurity programs with organizational risk and strategic priorities.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the purpose and structure of cybersecurity controls and security frameworks.
- Distinguish between cybersecurity policies, standards, procedures, guidelines, and controls.

- Develop a structured cybersecurity policy hierarchy.
- Identify and document cybersecurity control objectives.
- Map cybersecurity risks to appropriate preventive, detective, and corrective controls.
- Assess the effectiveness and maturity of existing cybersecurity controls.
- Conduct cybersecurity framework and control gap assessments.
- Build control matrices and maintain traceability between risks, controls, and requirements.
- Establish control ownership and accountability across business and technology functions.
- Develop cybersecurity metrics, risk indicators, and management reporting.
- Prepare appropriate evidence for cybersecurity audits and assessments.
- Align cybersecurity controls across cloud, hybrid, and traditional technology environments.
- Identify weaknesses in third-party and supply-chain security controls.
- Establish continuous monitoring and improvement mechanisms.
- Develop a prioritized cybersecurity controls implementation roadmap.

Course Outline

DAY 01

Cybersecurity Governance, Controls, and Security Frameworks

- Understanding cybersecurity governance and its organizational role.
- Cybersecurity risk, governance, compliance, and control relationships.
- Cybersecurity control concepts and control objectives.
- Preventive, detective, corrective, and compensating controls.
- Cybersecurity policies, standards, procedures, and guidelines.
- Security frameworks and their role in enterprise cybersecurity.
- Framework selection and organizational alignment.
- Security governance structures and accountability.
- Control ownership and responsibility models.
- Cybersecurity maturity and control environment assessment.

DAY 01 — CONTINUED

PRACTICAL APPLICATION

Assess a representative organization's cybersecurity governance structure and identify key control and accountability gaps.

DAY 02

Cybersecurity Policies, Standards, and Control Design

- Principles of effective cybersecurity policy development.
- Building a cybersecurity policy hierarchy.
- Defining policy scope, ownership, responsibilities, and enforcement.
- Information security and acceptable-use policies.
- Identity, access control, and authentication policies.
- Data protection and information classification policies.
- Network, endpoint, and infrastructure security policies.
- Vulnerability and patch management policies.
- Incident response and security event management policies.
- Cloud security and remote-access policies.
- Third-party and supplier cybersecurity requirements.
- Policy exceptions, approvals, reviews, and lifecycle management.

PRACTICAL APPLICATION

Develop a cybersecurity policy framework and draft selected policy requirements for a representative enterprise.

DAY 03

Security Framework Mapping, Risk, and Control Assessment

- Understanding cybersecurity framework structures.
- Mapping business and cybersecurity risks to security controls.
- Control identification and classification.
- Developing cybersecurity control matrices.

DAY 03 — CONTINUED

- Framework-to-framework control mapping.
- Identifying overlapping and redundant controls.
- Control design assessment.
- Operating effectiveness assessment.
- Control testing methodologies.
- Evidence collection and documentation.
- Cybersecurity gap analysis.
- Risk-based prioritization of control weaknesses.

PRACTICAL APPLICATION

Build a cybersecurity control matrix, map identified risks to controls, and perform a structured control gap assessment.

DAY 04

Control Implementation, Compliance, and Security Operations

- Implementing cybersecurity controls across enterprise environments.
- Identity and access security controls.
- Privileged access and authentication controls.
- Network and infrastructure security controls.
- Endpoint protection and vulnerability management controls.
- Data protection and encryption controls.
- Security monitoring and logging controls.
- Incident detection and response controls.
- Cloud and hybrid security controls.
- Third-party and supply-chain security controls.
- Business continuity and disaster recovery controls.
- Compliance monitoring and audit readiness.
- Managing control deficiencies and remediation plans.

DAY 04 — CONTINUED

PRACTICAL APPLICATION

Evaluate a simulated cybersecurity control environment and develop a risk-based remediation plan for identified weaknesses.

DAY 05

Cybersecurity Control Governance, Measurement, and Continuous Improvement

- Establishing a sustainable cybersecurity control governance model.
- Control lifecycle management.
- Periodic control reviews and reassessments.
- Continuous control monitoring.
- Cybersecurity performance indicators and risk indicators.
- Measuring control effectiveness and maturity.
- Management dashboards and executive reporting.
- Cybersecurity audit preparation and evidence management.
- Tracking remediation and corrective actions.
- Managing cybersecurity policy and control exceptions.
- Integrating controls with enterprise risk management.
- Building a cybersecurity improvement and transformation roadmap.
- Establishing continuous improvement mechanisms.

FINAL WORKSHOP

Develop an integrated Cybersecurity Controls, Policies & Security Frameworks Program covering governance, policy architecture, control objectives, framework alignment, risk assessment, control testing, gap analysis, compliance, measurement, remediation, continuous monitoring, and a prioritized implementation roadmap.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/cybersecurity-controls-policies-security-frameworks-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440