Security Quality Assurance Training Course

Professional Development Training Course Outline

Category	Aviation and Airport Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Security Quality Assurance (SQA) is a critical component of modern cybersecurity, risk management, and organizational resilience strategies. Security Quality Assurance Training Course is designed to equip professionals with advanced knowledge and practical skills in security testing, quality assurance frameworks, vulnerability assessment, compliance management, and continuous security improvement. With increasing cyber threats, regulatory requirements, and digital transformation initiatives, organizations require skilled professionals who can integrate security assurance practices into business operations, software development, and information technology environments.

This course focuses on developing expertise in security quality processes, security governance, penetration testing principles, secure software development lifecycle (SSDLC), audit readiness, and security performance measurement. Participants will explore global best practices, industry standards, and real-world case studies to strengthen their ability to identify security gaps, improve controls, and establish proactive security assurance programs that support business continuity and cyber resilience.

Programme Curriculum

Security Quality Assurance Training Course

Introduction

Security Quality Assurance (SQA) is a critical component of modern cybersecurity, risk management, and organizational resilience strategies. Security Quality Assurance Training Course is designed to equip professionals with advanced knowledge and practical skills in security testing, quality assurance frameworks, vulnerability assessment, compliance management, and continuous security improvement. With increasing cyber threats, regulatory requirements, and digital transformation initiatives, organizations require skilled professionals who can integrate security assurance practices into business operations, software development,

and information technology environments.

This course focuses on developing expertise in security quality processes, security governance, penetration testing principles, secure software development lifecycle (SSDLC), audit readiness, and security performance measurement. Participants will explore global best practices, industry standards, and real-world case studies to strengthen their ability to identify security gaps, improve controls, and establish proactive security assurance programs that support business continuity and cyber resilience.

Course Objectives

By the end of this Security Quality Assurance Training Course, participants will be able to:

1. Understand modern Security Quality Assurance frameworks and cybersecurity quality management principles.
2. Apply advanced security testing methodologies for identifying vulnerabilities and risks.
3. Develop effective security assurance strategies aligned with organizational objectives.
4. Implement secure software development lifecycle (SSDLC) practices.
5. Conduct security audits, assessments, and compliance reviews.
6. Evaluate cybersecurity controls using industry standards and frameworks.
7. Apply risk-based approaches to security quality management.
8. Improve vulnerability management and threat detection capabilities.
9. Integrate security automation and continuous monitoring practices.
10. Enhance incident prevention through proactive security assurance.
11. Manage security governance, policies, and regulatory compliance requirements.
12. Apply global cybersecurity standards and best practices.
13. Build organizational cyber resilience through quality-driven security practices.

Organizational Benefits

- Strengthened cybersecurity posture through improved security assurance practices.
- Reduced exposure to cyber threats, vulnerabilities, and operational risks.
- Improved compliance with international security standards and regulations.
- Enhanced quality control within information security processes.
- Increased ability to detect and prevent security weaknesses.
- Improved decision-making through security performance analytics.
- Stronger integration between IT, security, and business operations.
- Enhanced customer trust and organizational reputation.
- Improved incident response and business continuity readiness.
- Development of skilled security quality assurance professionals.

Target Audiences

1. Cybersecurity professionals and security analysts.
2. Quality assurance engineers and software testers.
3. Information technology managers and administrators.
4. Risk management and compliance officers.
5. Software developers and DevSecOps teams.

6. Internal auditors and security consultants.
7. Business leaders responsible for digital security.
8. Professionals seeking careers in cybersecurity and information assurance.

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of Security Quality Assurance

- Introduction to Security Quality Assurance concepts, principles, and cybersecurity quality frameworks.
- Understanding the role of SQA in modern information security environments.
- Exploring security assurance lifecycle processes and quality management approaches.
- Identifying security risks, vulnerabilities, and control weaknesses.
- Global case study: Security assurance practices implemented by Microsoft cybersecurity teams.

Module 2: Security Testing and Assessment Methodologies

- Understanding security testing approaches including vulnerability assessment and penetration testing.
- Applying security verification techniques throughout technology development processes.
- Evaluating applications, networks, and infrastructure security controls.
- Developing effective security testing plans and assessment reports.
- Global case study: Security testing strategies used by financial institutions such as JPMorgan Chase.

Module 3: Secure Software Development Quality Assurance

- Understanding Secure Software Development Lifecycle (SSDLC) principles.
- Integrating security practices into software design, development, and deployment.
- Applying code review, security testing, and vulnerability scanning methods.
- Managing security requirements within software development projects.
- Global case study: DevSecOps implementation practices at Google.

Module 4: Security Governance, Risk, and Compliance

- Understanding cybersecurity governance structures and security quality policies.
- Applying risk management frameworks for security assurance improvement.
- Evaluating compliance requirements using international standards.
- Developing security metrics and performance indicators.
- Global case study: ISO 27001 security governance implementation in global organizations.

Module 5: Vulnerability Management and Continuous Improvement

- Developing vulnerability identification and remediation strategies.
- Implementing continuous security monitoring processes.
- Prioritizing security risks using risk-based approaches.
- Improving security quality through performance evaluation.
- Global case study: Continuous vulnerability management practices at Cisco.

Module 6: Security Auditing and Quality Control

- Understanding security audit methodologies and assessment procedures.
- Conducting security reviews to evaluate control effectiveness.
- Preparing security documentation and audit evidence.
- Improving organizational security quality assurance processes.
- Global case study: Security audit programs used by multinational enterprises.

Module 7: Security Automation and Emerging Technologies

- Exploring automation tools for security testing and quality assurance.
- Understanding artificial intelligence applications in cybersecurity assurance.
- Applying machine learning techniques for threat detection improvement.
- Integrating automation into security monitoring processes.
- Global case study: AI-driven cybersecurity operations at IBM Security.

Module 8: Building Security Quality Assurance Programs

- Developing sustainable security assurance strategies for organizations.
- Creating security improvement roadmaps and implementation plans.
- Measuring security maturity and organizational resilience.
- Establishing continuous improvement cultures in cybersecurity.
- Global case study: Enterprise security transformation programs used by leading technology companies.

Training Methodology

- Interactive instructor-led sessions focusing on practical security quality concepts.
- Real-world cybersecurity case studies from global organizations.
- Hands-on exercises involving security assessment and quality evaluation.
- Group discussions and collaborative problem-solving activities.
- Security testing demonstrations and practical simulations.
- Workshops focused on developing security assurance strategies.
- Knowledge assessments and professional feedback sessions.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com