Faysal Aziz

Security Assurance Process

Risk-based assessment, control evidence and continuous improvement

FA-0691 · 1 day

Cybersecurity

Introduction

This one-day course introduces a structured approach to evaluating security controls and documenting confidence in their operation. It links risk, governance, assessment scope, testing evidence and follow-up actions.

Participants work through a supplied scenario to plan an assessment, interpret findings and prioritise improvements. The course introduces methods and tools; it does not promise that a brief assessment proves an organisation secure or replaces a complete audit or penetration test.

Learning outcomes

- Define assurance objectives, scope, roles and evidence requirements.
- Distinguish risk assessments, security audits, compliance checks and technical testing.
- Plan appropriate control-assessment activities for a supplied scenario.
- Interpret findings and document control effectiveness, limitations and corrective actions.
- Propose monitoring and improvement steps with clear ownership and follow-up.

Prerequisites

- Basic knowledge of information security concepts and IT infrastructure.
- Familiarity with IT operations within an organization is helpful but not mandatory.

Training outline

1. Assurance foundations and governance

- Defining Security Assurance: Objectives and scope.
- Importance of Security Assurance in organizational resilience.
- Overview of the Security Assurance lifecycle.
- Key principles guiding Security Assurance processes.
- Understanding the relationship between security assurance and risk management.
- Integrating security assurance with existing IT and security governance frameworks.
- Standard practices in the security assurance process.
- Roles and responsibilities in security assurance.
- Documentation and reporting for accountability and transparency.

2. Assessment methods and evidence

- Common methodologies: Risk Assessments, Security Audits, Compliance Checks.
- Tools and techniques for conducting security assessments.
- Scenario-based training on applying methodologies to real-world cases.

3. Controls and technical evaluation

- Designing and implementing security controls.
- Select controls appropriate to identified risks, requirements and operating constraints
- Control effectiveness and adjustment.
- Techniques for security testing: Penetration Testing, Vulnerability Assessments, Security Reviews.
- Tools used in security testing.
- Interpreting test results and evaluating security posture.

4. Continuous improvement and changing risks

- Monitoring and maintaining security controls.
- Using feedback mechanisms for continuous improvement.
- Review example assurance cases and the limitations of their evidence

Discuss how changing threats, technologies and organisational requirements affect assessment scope and follow-up.

5. Guided assurance simulation and next steps

Apply the process to a supplied case: define scope, identify evidence, evaluate selected controls and record findings.

- Review of key concepts and skills learned.
- Guidance on next steps and further resources.
- Q&A and feedback session.

© 2026 Faysal Aziz · Kuala Lumpur