Enterprise Security Architecture (TOGAF-based) Training Course

Professional Development Training Course Outline

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

Course Introduction

Enterprise Security Architecture (ESA) is a critical component of modern organizational strategy, ensuring that security policies, processes, and technologies are aligned with business objectives. Leveraging the TOGAF framework, this course enables participants to design, implement, and manage robust security architectures that mitigate risks, enhance compliance, and protect digital assets. It addresses emerging threats, regulatory requirements, cloud integration, identity and access management, threat modeling, and secure system design, providing a holistic approach to safeguarding enterprise IT infrastructure. Through real-world case studies and interactive workshops, participants will gain practical insights into the development of enterprise-wide security strategies that balance risk, cost, and business value.

Enterprise Security Architecture (TOGAF-based) Training Course emphasizes a structured approach to security governance, risk management, and compliance, guided by industry best practices and TOGAF principles. Participants will learn to integrate security into enterprise architecture frameworks, optimize security operations, implement risk-based controls, and align security architecture with organizational strategy. By connecting business, information, application, and technology domains, this course prepares IT and security professionals to proactively anticipate threats, enforce policies, and ensure the resilience and sustainability of enterprise systems.

Programme Curriculum

Enterprise Security Architecture (TOGAF-based) Training Course

Introduction

Enterprise Security Architecture (ESA) is a critical component of modern organizational strategy, ensuring that security policies, processes, and technologies are aligned with business objectives. Leveraging the TOGAF framework, this course enables participants to design, implement, and manage robust security architectures

that mitigate risks, enhance compliance, and protect digital assets. It addresses emerging threats, regulatory requirements, cloud integration, identity and access management, threat modeling, and secure system design, providing a holistic approach to safeguarding enterprise IT infrastructure. Through real-world case studies and interactive workshops, participants will gain practical insights into the development of enterprise-wide security strategies that balance risk, cost, and business value.

Enterprise Security Architecture (TOGAF-based) Training Course emphasizes a structured approach to security governance, risk management, and compliance, guided by industry best practices and TOGAF principles. Participants will learn to integrate security into enterprise architecture frameworks, optimize security operations, implement risk-based controls, and align security architecture with organizational strategy. By connecting business, information, application, and technology domains, this course prepares IT and security professionals to proactively anticipate threats, enforce policies, and ensure the resilience and sustainability of enterprise systems.

Course Objectives

1. Understand Enterprise Security Architecture concepts and TOGAF principles.
2. Develop integrated security strategies aligned with business goals.
3. Apply TOGAF-based frameworks to design secure enterprise architectures.
4. Identify, assess, and manage security risks across organizational layers.
5. Integrate security governance into enterprise architecture planning.
6. Design secure data, application, and network architectures.
7. Implement identity and access management frameworks.
8. Apply threat modeling and vulnerability assessment techniques.
9. Ensure compliance with regulatory and industry security standards.
10. Develop strategies for cloud security and hybrid IT environments.
11. Integrate business continuity and disaster recovery into security architecture.
12. Monitor and evaluate security architecture effectiveness and maturity.
13. Foster a security-aware culture within enterprise operations.

Organizational Benefits

- Improved enterprise-wide security posture
- Strong alignment of security strategy with business objectives
- Enhanced risk management and threat mitigation
- Compliance with industry and regulatory standards
- Optimized investment in security technologies
- Streamlined security governance processes
- Reduced operational and cyber risks
- Enhanced resilience and business continuity
- Strengthened stakeholder trust and confidence
- Improved decision-making with integrated security insights

Target Audiences

- Enterprise architects and IT managers
- Chief Information Security Officers (CISOs)
- Security analysts and risk managers
- IT governance and compliance officers
- Cloud and network security professionals

- Application security engineers
- Security consultants and auditors
- Senior management overseeing IT and security strategy

Course Duration: 5 days

Course Modules

Module 1: Introduction to Enterprise Security Architecture

- Overview of enterprise security concepts and frameworks
- TOGAF architecture principles and components
- Security governance structures and policy alignment
- Key challenges in enterprise security architecture
- Emerging threats and regulatory considerations
- Case Study: Designing ESA for a multinational enterprise

Module 2: Security Governance & Compliance

- Establishing security governance frameworks
- Defining roles, responsibilities, and accountability
- Compliance with ISO, NIST, and regulatory requirements
- Security policy lifecycle management
- Metrics and KPIs for security governance effectiveness
- Case Study: Compliance implementation in a financial institution

Module 3: Risk Management & Threat Assessment

- Identifying enterprise risks across business and IT domains
- Threat modeling methodologies and techniques
- Vulnerability assessment and prioritization
- Risk treatment strategies and mitigation plans
- Integration of risk management with enterprise architecture
- Case Study: Risk-based ESA deployment in a government agency

Module 4: Secure Data Architecture

- Data classification, labeling, and protection strategies
- Encryption standards and secure storage practices
- Data flow mapping and secure integration points
- Access control models for sensitive data
- Data privacy and compliance considerations
- Case Study: Secure data architecture for a healthcare provider

Module 5: Application & Network Security Architecture

- Designing secure application frameworks and APIs
- Network segmentation, monitoring, and intrusion detection
- Secure cloud and hybrid network integration
- Application vulnerability management
- Secure communication protocols and encryption
- Case Study: Enterprise network security redesign in a retail organization

Module 6: Identity & Access Management

- Identity lifecycle management and provisioning
- Role-based and attribute-based access controls
- Authentication, authorization, and single sign-on strategies
- Privileged account management and monitoring
- Integration with enterprise applications and services
- Case Study: Implementing IAM in a multi-branch financial institution

Module 7: Business Continuity & Disaster Recovery

- Aligning business continuity plans with ESA
- Disaster recovery planning for IT systems
- Risk-based prioritization of critical assets
- Backup, replication, and redundancy strategies
- Testing and continuous improvement of recovery plans
- Case Study: Disaster recovery implementation in a telecom company

Module 8: Monitoring, Evaluation & Continuous Improvement

- Security metrics, dashboards, and reporting
- Continuous monitoring of ESA effectiveness
- Maturity assessments and gap analysis
- Incident response and remediation integration
- Lessons learned and iterative improvement of ESA
- Case Study: Continuous monitoring program for a government enterprise

Training Methodology

- Instructor-led presentations on TOGAF and ESA frameworks
- Interactive group exercises and scenario-based workshops
- Case study analysis and real-world enterprise examples
- Hands-on labs for threat modeling and secure architecture design
- Templates and tools for governance, risk, and compliance processes
- Action planning and peer 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