

ZERO TRUST STRATEGY & CYBERSECURITY GOVERNANCE



GENTEX[®]
TRAINING CENTER



Introduction

The Zero Trust Strategy & Cybersecurity Governance Training Course prepares security leaders and governance professionals to design, govern, and sustain a modern Zero Trust programme. Perimeter-based security no longer protects hybrid work, cloud platforms, and third-party access. Zero Trust replaces implicit trust with continuous verification of users, devices, and workloads. This course connects Zero Trust architecture with the governance structures that make it durable. Furthermore, it covers policy design, identity controls, segmentation, monitoring, and executive reporting. As a result, participants leave able to align security investment with business risk and regulatory obligation.

Zero Trust Strategy & Cybersecurity Governance Course Objectives

- Explain Zero Trust principles and how they differ from perimeter security models.
- Apply the NIST SP 800-207 Zero Trust Architecture reference model.
- Map maturity against the CISA Zero Trust Maturity Model.
- Design identity-centric controls using IAM, MFA, and privileged access management.
- Plan micro-segmentation and least-privilege access across networks and workloads.
- Align security governance with ISO/IEC 27001 and the CIS Controls.
- Build security policies, standards, and control ownership structures.
- Define security metrics, KPIs, and KRIs for board-level reporting.
- Integrate Zero Trust with third-party and supply chain risk management.
- Prepare a phased Zero Trust roadmap with funding and governance milestones.

Course Methodology

- Interactive lectures with real breach and Zero Trust adoption case studies.

LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Architecture workshops using NIST SP 800-207 design patterns.
- Maturity assessment exercises against the CISA model.
- Simulated security governance committee decisions.
- Templates for policy sets, roadmaps, and executive security dashboards.

Who Should Take This Course

- Chief information security officers and security managers.
- IT and infrastructure leaders responsible for architecture.
- Governance, risk, and compliance professionals in technology.
- Identity, network, and cloud security engineers.
- Internal auditors reviewing cybersecurity controls.
- Executives and board members sponsoring security programmes.

Zero Trust Strategy & Cybersecurity Governance Course Outlines

Day 1: Foundations of Zero Trust and Security Governance

- Zero Trust principles: verify explicitly, least privilege, assume breach.
- Why perimeter security fails in cloud and hybrid environments.
- The NIST SP 800-207 Zero Trust Architecture reference model.
- Governance structures, roles, and security accountability.
- Security policy hierarchy and control ownership.
- Aligning security strategy with business objectives.



LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Case study: lessons from a major breach and a Zero Trust response.

Day 2: Identity, Access, and Device Trust

- Identity as the new security perimeter.
- Identity and access management (IAM) and identity providers.
- Multi-factor authentication (MFA) and passwordless authentication.
- Privileged access management (PAM) and just-in-time access.
- Device trust, endpoint posture, and mobile device management.
- Conditional access policies and continuous authentication.
- Workshop: designing an identity-centric access policy set.

Day 3: Network Segmentation and Workload Protection

- Micro-segmentation concepts and implementation approaches.
- Software-defined perimeter and secure access service edge (SASE).
- Least-privilege network and application access.
- Workload and container security basics.
- Data classification, encryption, and data loss prevention.
- Logging, SIEM, and continuous monitoring architecture.
- Workshop: planning a micro-segmentation rollout.

Day 4: Frameworks, Standards, and Control Assurance

- The CISA Zero Trust Maturity Model and maturity pillars.
- ISO/IEC 27001 controls and ISMS alignment.
- The CIS Controls and their mapping to Zero Trust.



LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Risk assessment and control testing for security programmes.
- Incident response, detection, and threat intelligence integration.
- Third-party and supply chain security oversight.
- Workshop: mapping controls to a maturity assessment.

Day 5: Roadmap, Metrics, and Executive Reporting

- Building a phased Zero Trust implementation roadmap.
- Business case, funding, and resource planning.
- Security metrics, KPIs, and KRIs for leadership.
- Executive dashboards and board-level security reporting.
- Change management and security culture adoption.
- Measuring programme value and continuous improvement.
- Course review, assessment, and action planning.

Conclusion

By successfully completing Zero Trust Strategy & Cybersecurity Governance, participants will gain a comprehensive understanding of Zero Trust architecture, identity-centric controls, segmentation, and the governance frameworks that sustain them. They will also acquire practical skills in maturity assessment, control mapping, roadmap planning, and executive security reporting. In addition, the course prepares them to align security strategy with business and regulatory expectations. Gentex Training Center delivers this programme with a strong focus on applied practice and measurable security improvement.





FAQs for Zero Trust Strategy & Cybersecurity Governance course

Q1 What is the "Zero Trust Strategy & Cybersecurity Governance" course about?

It is a five-day programme that explains how to design and govern a Zero Trust security programme. It covers Zero Trust principles, identity and access controls, micro-segmentation, monitoring, security frameworks, and executive reporting, so security strategy aligns with real business risk.

Q2 What are the key benefits of the "Zero Trust Strategy & Cybersecurity Governance" course?

Participants gain a practical route from perimeter thinking to continuous verification, which reduces breach impact and lateral movement. The course also improves security governance, sharpens control assurance, strengthens audit and regulatory readiness, and gives leadership clear metrics for funding decisions and programme oversight.

Q3 What skills will I gain from the "Zero Trust Strategy & Cybersecurity Governance" course?

Participants gain Zero Trust architecture design, identity and access control implementation, network micro-segmentation and monitoring design, and security governance, control assurance, and executive reporting. These four skills cover both the technical and governance sides of a Zero Trust programme.



Q4 What tools, methods, or standards are covered in the "Zero Trust Strategy & Cybersecurity Governance" course?

The course covers NIST SP 800-207 Zero Trust Architecture, the CISA Zero Trust Maturity Model, ISO/IEC 27001, the CIS Controls, IAM and identity providers, MFA and passwordless authentication, privileged access management, conditional access policies, micro-segmentation, SASE, SIEM, data loss prevention, and security KRIs and dashboards.

Q5 How is the "Zero Trust Strategy & Cybersecurity Governance" course applied in real-world practice?

Participants apply the methods inside their own organisations. They assess current maturity, redesign access policies, plan segmentation phases, map controls to standards, build security dashboards, and prepare funding cases for leadership. Many leave with a phased Zero Trust roadmap ready to present.