



Zero Trust Strategy and Governance Training Course

31 January – 4 February 2027
Johannesburg

Zero Trust Strategy and Governance Training Course

Ref: 773_158817 **Date:** 31 January – 4 February 2027 **Location:** Johannesburg **Fees:** 4500 Euro

Overview

Zero Trust Strategy and Governance Training Course is a five-day advanced course for cybersecurity leaders, enterprise architects, identity teams, risk managers, and transformation governance functions who leave with a Zero Trust Transformation Roadmap. Participants connect protect surfaces, identity and device trust, policy decisions, enforcement points, segmentation, data and application access, telemetry, ownership, investment sequencing, and measures into an enterprise operating model. Agile Leaders Training Center develops practical zero trust strategy and governance capability.

Who Should Attend

- Cybersecurity leadership functions responsible for enterprise security direction and investment priorities
- Enterprise architecture functions responsible for cross-domain technology principles and target states
- Identity and access functions responsible for trust signals, access policy, and least privilege
- Risk management functions responsible for assurance, decision rights, and control evidence
- Digital transformation governance functions responsible for sequencing capabilities and accountable ownership

The course assumes participants can evaluate enterprise security decisions and operating dependencies, and leaves out product configuration, identity administration, penetration testing, and detailed network implementation.

Departments and Industries

The course supports departments and industries coordinating enterprise zero trust decisions across business and technology domains.

- Banking cybersecurity and enterprise architecture
- Energy digital operations and risk governance
- Healthcare identity and data protection
- Telecommunications network and security strategy
- Public-service technology transformation

Learning Objectives

By the end of this course, participants will be able to:



- Apply zero trust principles to enterprise decisions
- Analyze protect surfaces and trust dependencies
- Build policy decision and enforcement governance
- Prioritize identity, device, data, application, and segmentation capabilities
- Evaluate telemetry, metrics, ownership, and assurance
- Build a Zero Trust Transformation Roadmap

Course Agenda

Day 1: Frame the Zero Trust Strategy

- NIST Zero Trust Architecture Principle Map
- Protect Surface Definition Method
- Enterprise Trust Dependency Canvas
- Explicit Verification Decision Criteria
- Assume Breach Scenario Analysis

Day 2: Design Policy and Enforcement Governance

- Policy Decision Point Operating Model
- Policy Engine Decision Logic Map
- Policy Administrator Responsibility Matrix
- Policy Enforcement Point Placement Method
- Decision Rights and Exception Governance Charter

Day 3: Sequence Pillars and Access Capabilities

- CISA Zero Trust Maturity Model Assessment
- Identity and Device Trust Signal Matrix
- Least Privilege Access Policy Pattern
- Data and Application Access Control Map
- Segmentation Capability Dependency Model

Day 4: Govern Investment, Telemetry, and Assurance

- Zero Trust Capability Investment Portfolio
- Telemetry and Analytics Coverage Matrix
- Cross-Functional Ownership RACI
- Zero Trust Outcome and Risk Metric Tree
- Assurance Evidence and Review Cycle



Day 5: Practice the Transformation Roadmap

- Exercise: Define Protect Surfaces and Dependencies
- Exercise: Map Policy Decisions and Enforcement Points
- Exercise: Prioritize Pillar Maturity Gaps
- Exercise: Sequence Investments and Accountability
- Capstone: Zero Trust Transformation Roadmap

Practical Exercises

The course uses suggested activities based on banking, energy, healthcare, telecommunications, and public-service scenarios.

- Suggested activity: define protect surfaces and map identities, devices, applications, data, and trust dependencies.
- Suggested activity: assign policy decision, administration, enforcement, exception, and assurance responsibilities.
- Suggested activity: assess maturity gaps and prioritize capabilities through risk, dependency, and value criteria.
- Suggested activity: assemble investments, ownership, metrics, and review gates into a transformation roadmap.

FAQs

Who suits zero trust strategy and governance training, and what does it assume?

Cybersecurity, architecture, identity, risk, and transformation governance functions suit the training; it assumes experience evaluating enterprise security decisions and dependencies.

How does zero trust strategy and governance differ from network security architecture training?

Zero trust strategy and governance defines enterprise decisions, ownership, capability sequencing, metrics, and assurance, while network security architecture training concentrates on technical network patterns and implementation.

What are policy decision and enforcement points in zero trust architecture?

Policy decision capabilities evaluate context and authorize access, while enforcement points apply those decisions at the resource boundary under governed policy and monitored conditions.



How should an enterprise prioritize a zero trust transformation roadmap?

An enterprise should prioritize protect-surface risk, identity and device dependencies, data sensitivity, application pathways, maturity gaps, enabling telemetry, accountable ownership, and feasible investment sequences.

Which metrics support zero trust governance?

Zero trust governance uses measures tied to access decisions, trust-signal coverage, privilege reduction, policy exceptions, enforcement reach, telemetry quality, control evidence, risk reduction, and roadmap delivery.

Conclusion

Participants take back a Zero Trust Transformation Roadmap linking protect surfaces, policy decisions, enforcement, capability priorities, investment, ownership, telemetry, metrics, and assurance. It changes disconnected security initiatives into a governed enterprise sequence. The roadmap supports coordinated decisions across cybersecurity, architecture, identity, risk, and transformation functions.