

Course No. 1938

Identity & Access Management (IAM) Strategy & Governance Training Course

IDENTITY & ACCESS MANAGEMENT
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION

5 Days

DELIVERY

Classroom



Course Overview

Identity & Access Management (IAM) Strategy & Governance Training Course provides a strategic and practical framework for developing, implementing, and governing enterprise identity and access management capabilities. The course focuses on establishing a structured approach to managing digital identities, access rights, authentication, authorization, privileged access, and identity-related risks across modern IT environments.

Participants will examine how identity and access management supports cybersecurity, regulatory compliance, operational efficiency, and business enablement. The program addresses the development of an IAM strategy aligned with organizational objectives, risk appetite, technology architecture, workforce requirements, and evolving cloud and digital transformation initiatives.

The course explores key governance areas including identity lifecycle management, access governance, role management, privileged access, segregation of duties, access certification, policy development, accountability, risk management, and audit readiness. Participants will learn how to establish clear ownership and decision-making structures for identity and access across business and technology functions.

Through practical assessments, governance scenarios, architecture exercises, access review simulations, and strategic planning workshops, participants will develop the ability to evaluate IAM maturity, identify control gaps, establish governance frameworks, prioritize initiatives, and create a sustainable roadmap for improving enterprise identity and access management.

Objectives

- By the end of the course, participants will be able to:
- Analyze the strategic role of identity and access management in enterprise cybersecurity.
- Assess current IAM capabilities, maturity, risks, and governance gaps.
- Develop an enterprise IAM strategy aligned with business and security objectives.
- Establish effective identity and access governance structures.
- Define ownership, accountability, and decision-making responsibilities for IAM.
- Design effective identity lifecycle management processes.

- Develop access governance and entitlement management frameworks.
- Apply least-privilege and segregation-of-duties principles.
- Strengthen privileged access governance and administrative identity controls.
- Establish effective access certification and periodic review processes.
- Align IAM policies and controls with organizational risk and compliance requirements.
- Define meaningful IAM performance and risk indicators.
- Evaluate technology, integration, and implementation dependencies.
- Prioritize IAM initiatives based on business value, security risk, and organizational readiness.
- Develop a practical roadmap for sustainable IAM transformation and governance.

Who Should Attend

This course is designed for IT managers, cybersecurity managers, information security professionals, IAM managers, security architects, enterprise architects, infrastructure managers, systems administrators, and technology professionals responsible for identity and access environments.

It is also highly relevant for risk and compliance professionals, internal auditors, governance specialists, data protection professionals, business process owners, HR technology teams, cloud security professionals, and senior decision-makers responsible for access governance, cybersecurity, digital transformation, or technology risk.

The course is particularly valuable for organizations seeking to establish or strengthen enterprise IAM governance, improve access control, reduce excessive privileges, enhance audit readiness, manage hybrid and cloud environments, and align identity security with broader business and cybersecurity strategies.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the strategic foundations of enterprise identity and access management.
- Assess IAM maturity across people, processes, technology, and governance.
- Identify identity-related security, operational, compliance, and business risks.

- Develop an enterprise IAM strategy and target operating model.
- Establish clear IAM governance structures and accountability mechanisms.
- Design effective identity lifecycle management frameworks.
- Develop role and entitlement management approaches.
- Apply least-privilege and segregation-of-duties controls.
- Establish effective privileged access governance.
- Design access certification and periodic entitlement review processes.
- Align IAM controls with risk management and compliance requirements.
- Define policies, standards, procedures, and governance controls for IAM.
- Develop IAM metrics, dashboards, and management reporting.
- Evaluate IAM technology architecture and integration requirements.
- Prioritize IAM transformation initiatives according to risk and organizational value.
- Develop a phased roadmap for IAM implementation, governance, and continuous improvement.

Course Outline

DAY 01

IAM Strategy, Business Alignment, and Maturity

- Foundations and strategic principles of identity and access management.
- The relationship between IAM, cybersecurity, and business enablement.
- Digital identity as an enterprise security asset.
- Identity and access risks across modern organizations.
- Workforce, customer, partner, contractor, and service identities.
- IAM in cloud, hybrid, remote, and digital environments.
- Assessing current IAM capabilities and maturity.
- Identifying organizational, technical, and process gaps.
- Defining IAM strategic vision and objectives.
- Aligning IAM priorities with business strategy and risk appetite.

DAY 01 — CONTINUED

PRACTICAL APPLICATION

Conduct an IAM maturity assessment for a representative organization and identify strategic priorities and major governance gaps.

DAY 02**Identity Lifecycle and Access Governance**

- Identity lifecycle management principles.
- Joiner, mover, and leaver processes.
- Identity provisioning and deprovisioning.
- Account creation, modification, suspension, and termination.
- Access request and approval workflows.
- Role management and entitlement structures.
- Role-based access control and access models.
- Least-privilege implementation.
- Segregation of duties and conflicting access.
- Access certification and periodic entitlement reviews.
- Business ownership of applications and access rights.

PRACTICAL APPLICATION

Design an end-to-end identity lifecycle and access governance process for employees, contractors, and third-party users.

DAY 03**IAM Governance, Policies, and Privileged Access**

- IAM governance principles and operating models.
- Defining IAM ownership and accountability.
- Governance committees and decision-making structures.
- Developing IAM policies, standards, and procedures.
- Risk-based access governance.

DAY 03 — CONTINUED

- Privileged identities and administrative access.
- Privileged access management governance.
- Emergency and temporary privileged access.
- Administrative account controls and monitoring.
- Access exceptions and risk acceptance.
- Audit trails, evidence, and governance reporting.

PRACTICAL APPLICATION

Develop an IAM governance framework covering ownership, policies, privileged access, exceptions, approvals, monitoring, and accountability.

DAY 04

IAM Technology, Integration, Risk, and Compliance

- Enterprise IAM architecture and core capabilities.
- Authentication, authorization, and identity federation.
- Single sign-on and multi-factor authentication.
- Integration with directories, applications, cloud platforms, and business systems.
- Identity governance and administration capabilities.
- Privileged access technologies and controls.
- Identity analytics and access intelligence.
- IAM risk assessment and control effectiveness.
- Regulatory, privacy, audit, and compliance considerations.
- Third-party and non-human identity risks.
- Monitoring, detection, and response to identity-related threats.

PRACTICAL APPLICATION

Analyze a hybrid IAM architecture and identify integration requirements, control weaknesses, compliance risks, and improvement priorities.

DAY 05

IAM Performance, Governance Maturity, and Transformation Roadmap

- Measuring IAM effectiveness and governance maturity.
- Key performance and risk indicators for IAM.
- Access review performance and control effectiveness.
- Monitoring excessive privileges and access anomalies.
- Executive IAM reporting and management dashboards.
- Evaluating IAM initiatives and business value.
- Building the IAM target operating model.
- Prioritizing IAM transformation initiatives.
- Developing business cases and investment priorities.
- Managing implementation risks and organizational change.
- Establishing continuous improvement mechanisms.

FINAL WORKSHOP

Develop an integrated IAM Strategy & Governance Framework covering current-state assessment, strategic objectives, governance model, identity lifecycle, access governance, privileged access, policies, technology architecture, risk and compliance, performance measurement, priorities, and a phased implementation roadmap.

Register or Request More Information

Course page: <https://quest-training.com/courses/identity-access-management-iam-strategy-governance-training-course>

Website: <https://quest-training.com>

Email: info@quest-training.com

Phone: +905016771440