

Course No. 1940

Identity Governance & Administration (IGA) Training Course

**IDENTITY & ACCESS MANAGEMENT
INFORMATION TECHNOLOGY & CYBERSECURITY**

DURATION

5 Days

DELIVERY

Classroom



Course Overview

The Identity Governance & Administration (IGA) Training Course provides a comprehensive and practical framework for governing digital identities, managing access rights, and establishing effective identity administration across modern enterprise environments. The course focuses on ensuring that users receive appropriate access based on their roles and responsibilities while maintaining strong security, regulatory compliance, operational efficiency, and accountability.

Participants will explore the complete identity lifecycle, from identity creation and onboarding through role changes, access provisioning, periodic reviews, and identity deactivation. The program addresses access requests, approvals, role management, entitlement management, access certification, segregation of duties, policy enforcement, and identity governance controls.

The course examines how IGA supports cybersecurity, Zero Trust, risk management, internal controls, audit readiness, and business operations. Participants will learn how to establish governance frameworks that connect business requirements with identity and access decisions, reduce excessive or inappropriate access, and improve visibility across complex hybrid and cloud environments.

Through practical exercises, access governance scenarios, role-design workshops, certification simulations, and implementation planning, participants will develop the skills required to assess IGA maturity, identify governance gaps, improve identity administration processes, and establish a sustainable identity governance model aligned with organizational objectives.

Objectives

- By the end of the course, participants will be able to:
- Analyze the role of Identity Governance & Administration in enterprise cybersecurity.
- Identify key components of an effective IGA framework.
- Assess identity and access governance risks across organizational environments.
- Design identity lifecycle management processes from onboarding to termination.
- Apply role-based access principles to improve access governance.
- Develop effective access request and approval workflows.

- Establish entitlement management and access certification processes.
- Apply segregation of duties controls to reduce operational and security risks.
- Improve governance of privileged, sensitive, and high-risk access.
- Integrate identity governance with Zero Trust and broader cybersecurity strategies.
- Evaluate IGA controls across cloud, hybrid, and on-premises environments.
- Define governance policies, ownership structures, and accountability mechanisms.
- Develop metrics and reporting mechanisms for identity governance.
- Assess IGA maturity and prioritize improvement opportunities.
- Develop a practical roadmap for implementing and continuously improving IGA capabilities.

Who Should Attend

This course is designed for Identity and Access Management professionals, cybersecurity specialists, security architects, IT managers, systems administrators, identity administrators, access governance specialists, and professionals responsible for managing enterprise identities and access rights.

It is also suitable for risk and compliance professionals, internal auditors, governance specialists, enterprise architects, security operations teams, human resources and IT process owners, and managers responsible for access approvals, user lifecycle processes, segregation of duties, or regulatory compliance.

The course is particularly valuable for organizations seeking to strengthen identity governance, improve access visibility, reduce excessive privileges, automate identity administration, enhance audit readiness, and establish stronger controls across cloud, hybrid, and traditional technology environments.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the principles and architecture of Identity Governance & Administration.
- Map and manage the enterprise identity lifecycle.
- Identify inappropriate, excessive, dormant, and orphaned access.

- Design effective identity provisioning and deprovisioning processes.
- Establish role-based access models aligned with business responsibilities.
- Develop access request and approval workflows.
- Manage user entitlements and access rights across multiple systems.
- Conduct effective access certification and periodic access reviews.
- Implement segregation of duties controls and identify conflicting access.
- Govern sensitive and high-risk identities and entitlements.
- Support Zero Trust initiatives through stronger identity governance.
- Integrate IGA processes with human resources, IT, security, and business systems.
- Define IGA governance policies, ownership, responsibilities, and escalation mechanisms.
- Develop identity governance metrics, dashboards, and management reports.
- Assess organizational IGA maturity and identify control gaps.
- Develop an implementation roadmap for sustainable identity governance and administration.

Course Outline

DAY 01

Foundations of Identity Governance & Administration

- Understanding Identity Governance & Administration and its business value.
- Relationship between IGA, IAM, cybersecurity, risk management, and Zero Trust.
- Identity governance principles and operating models.
- Digital identity types and enterprise identity sources.
- Identity lifecycle management.
- Joiner, mover, and leaver processes.
- Identity ownership and accountability.
- Identity repositories and authoritative sources.
- Identity data quality and reconciliation.
- Common identity governance risks and control gaps.
- Assessing organizational identity governance maturity.

DAY 01 — CONTINUED

PRACTICAL APPLICATION

Map the identity lifecycle of a representative organization and identify governance gaps, ownership issues, and access-control risks.

DAY 02

Identity Administration, Provisioning, and Access Management

- Identity creation and account provisioning.
- Automated and manual provisioning processes.
- User onboarding and access assignment.
- Role changes and access modification.
- Employee transfers and organizational mobility.
- Identity deprovisioning and access termination.
- Managing contractors, third parties, and external users.
- Entitlement management across enterprise applications.
- Access request and approval workflows.
- Access exceptions and temporary access.
- Improving identity administration efficiency and control.

PRACTICAL APPLICATION

Design an end-to-end identity administration workflow covering onboarding, role changes, access requests, approvals, provisioning, modifications, and termination.

DAY 03

Role Management, Access Certification, and Governance Controls

- Role-based access control principles.
- Business roles and technical roles.
- Role engineering and role design.
- Role mining and access pattern analysis.

DAY 03 — CONTINUED

- Entitlement classification and risk assessment.
- Access certification and periodic access reviews.
- Manager and application-owner certification.
- Identifying excessive and inappropriate access.
- Dormant, orphaned, and unnecessary accounts.
- Segregation of duties principles.
- Identifying and managing conflicting access.
- Remediation and exception management.

PRACTICAL APPLICATION

Conduct an access certification exercise, identify inappropriate access and segregation-of-duties conflicts, and develop remediation actions.

DAY 04

IGA Architecture, Integration, Risk, and Compliance

- Enterprise IGA architecture and core components.
- Integrating identity governance with business applications.
- Integration with human resources and organizational systems.
- Directory and identity platform integration.
- Cloud and hybrid identity governance.
- Governing application and database access.
- Managing privileged and high-risk entitlements.
- Identity governance risk assessment.
- Policy-based access controls.
- Audit trails and evidence management.
- Regulatory compliance and audit readiness.
- Integrating IGA with cybersecurity operations and risk management.

DAY 04 — CONTINUED

PRACTICAL APPLICATION

Develop an IGA architecture and integration model for a hybrid enterprise environment with multiple applications, identity sources, cloud platforms, and high-risk access requirements.

DAY 05**IGA Strategy, Governance, Measurement, and Implementation**

- Developing an enterprise IGA strategy.
- Establishing identity governance structures and decision rights.
- Defining roles, responsibilities, ownership, and accountability.
- Developing IGA policies, standards, and procedures.
- Establishing access governance committees and review mechanisms.
- Measuring IGA performance and control effectiveness.
- Key identity governance metrics and risk indicators.
- Building management dashboards and reporting.
- Assessing IGA maturity and prioritizing improvement initiatives.
- Automating identity governance and administration processes.
- Managing implementation risks and organizational change.
- Developing a sustainable IGA operating model.
- Building a phased implementation and transformation roadmap.

FINAL WORKSHOP

Develop an integrated Identity Governance & Administration strategy covering identity lifecycle management, provisioning, role management, entitlement governance, access certification, segregation of duties, risk management, compliance, automation, performance measurement, maturity assessment, and implementation planning.



Register or Request More Information

Course page: <https://quest-training.com/courses/identity-governance-administration-iga-training-course>

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

Email: info@quest-training.com

Phone: +905016771440

