CONCEPT

Identity and Access Management (IAM): Identity Governance, Authentication and Privileged Access

Identity and Access Management (IAM): Identity Governance, Authentication and Privileged Access

Introduction:

Identity and access management IAM failures rarely look dramatic: a leaver whose account stays active, a mover who keeps old entitlements, a shared administrator password, or an access review signed without being read. Each one widens the attack surface and weakens audit evidence. This Core Concept course trains practitioners to run IAM as a governed discipline, from identity life cycle and federation to authentication strength, role design, access certification, segregation of duties and privileged access management. Participants build an IAM Control Assessment and Improvement Roadmap for their own organisation.

Course Objectives:

- Map an organisation's identity sources, directories, applications and access flows into an IAM reference architecture
- Operate joiner, mover and leaver processes with provisioning and de-provisioning controls that leave an audit trail
- Select authentication methods, multi-factor options and federation protocols against NIST SP 800-63B authenticator assurance levels
- Design role-based and attribute-based access models with segregation of duties rules and a toxic combination matrix
- Run access reviews, certification campaigns and privileged access controls, including vaulting, just-in-time elevation and session recording
- Build an IAM Control Assessment and Improvement Roadmap with metrics and audit evidence for the organisation's own estate

Target Audience:

- Staff who administer user accounts, directory services and provisioning workflows
- Staff who operate authentication, single sign-on and multi-factor authentication services
- Staff who run access reviews, entitlement clean-up and segregation of duties checks
- Staff who manage administrator, service and emergency accounts and privileged access tools
- Staff who prepare identity and access evidence for internal and external audit

Course Outline:

Day 1: IAM Foundations, Identity Life Cycle and Current-State Assessment

- IAM Building Blocks: Identification, Authentication, Authorisation and Accountability
- IAM Reference Architecture: Authoritative Sources, Directories, Identity Provider and Target Applications
- Joiner, Mover and Leaver Process Mapping from HR Record to Account Removal
- Identity Types Inventory: Employees, Contractors, Service Accounts and Machine Identities
- IAM Current-State Maturity Assessment Template and Gap Log

Day 2: Directory Services, Federation and Authentication Standards

- Directory Services and LDAP Schema Design for Groups, Attributes and Organisational Units
- SAML Assertions, Identity Provider and Service Provider Trust Configuration
- OAuth Authorisation Flows and OpenID Connect ID Tokens for Single Sign-On
- NIST SP 800-63B Authenticator Assurance Levels AAL1, AAL2 and AAL3
- Multi-Factor Authentication Options: OTP, Push, Cryptographic Keys and Phishing-Resistant Authenticators

Day 3: Access Models, Provisioning and Access Certification

- Role-Based Access Control: Role Mining, Role Engineering and Birthright Access
- Attribute-Based Access Control Policies Using User, Resource and Context Attributes
- Automated Provisioning Connectors, Request Workflows and Approval Chains
- Access Review and Certification Campaign Design: Scope, Reviewers and Revocation Tracking
- Segregation of Duties Rule Set and Toxic Combination Matrix Build

Day 4: Privileged Access Management, Zero Trust Identity and IAM Risk

- Privileged Account Discovery: Administrator, Service, Break-Glass and Shared Accounts
- Privileged Credential Vaulting, Password Rotation and Check-Out Controls
- Just-in-Time Elevation, Least Privilege Enforcement and Privileged Session Recording
- Zero Trust Identity Principles: Continuous Verification and Context-Aware Access Decisions
- Identity Governance and Administration Tooling Capabilities at Overview and Selection Criteria

Day 5: IAM Case Work, Metrics and the Control Roadmap

- Case Study: Orphaned Accounts and Excess Entitlements Found During an Audit in a Financial Services Firm
- Case Study: Privileged Credential Misuse in a Healthcare Provider's Infrastructure Team
- IAM Key Metrics: Leaver Revocation Time, Review Completion Rate and Privileged Account Coverage
- Audit Evidence Pack: Provisioning Logs, Certification Sign-Offs and Exception Registers
- IAM Control Assessment and Improvement Roadmap Drafting and Peer Challenge

Skills You Will Gain:

- Identity Life Cycle Management
- Federated Single Sign-On Configuration
- Authenticator Assurance Selection
- Role Engineering
- Access Certification Management
- Segregation of Duties Analysis
- Privileged Account Control
- IAM Audit Evidence Preparation

Why Attend This Course:

- Return with an IAM Control Assessment and Improvement Roadmap built around your own directories, applications and privileged accounts
- Close the leaver, mover and orphaned account gaps that auditors and attackers find first
- Turn access reviews from signed spreadsheets into campaigns that remove access and prove it
- Compare identity and privileged access practice with peers from finance, healthcare, energy, telecoms and public services

Conclusion:

Identity is now the control that most other security controls depend on. The course moves from IAM building blocks and the joiner, mover and leaver process, through directory services, SAML, OAuth, OpenID Connect and authenticator assurance levels, to role and attribute-based access, provisioning, access certification and segregation of duties, then to privileged access management, zero trust identity and governance tooling. The final day applies case study work to audit and credential misuse scenarios and produces an IAM Control Assessment and Improvement Roadmap.