BEMI
IT SOLUTIONS

BEMI TECH SOLUTIONS · CYBERSECURITY TRAINING SERIES

Identity & Access Management (IAM)

The Complete Guide

> From Authentication & Authorization to Enterprise IAM Governance

10	23+	5	100%
Chapters	Pages	IAM Pillars	Practical

Identity & Access Management is the foundation of modern cybersecurity. This guide covers everything from core IAM concepts and authentication protocols to enterprise governance, cloud identity, and privileged access — giving you the knowledge to design, implement, and manage IAM programs that protect your organization.

Ransford Slater · Bemi Tech Solutions · bemitechsolutions.com · Arlington, TX

TABLE OF CONTENTS

What's Inside

01 What Is Identity & Access Management?

The foundation of modern cybersecurity

Identity & Access Management (IAM) is the discipline that ensures the right people have access to the right resources at the right time — and that unauthorized access is prevented. It is the cornerstone of enterprise security, governing how users, systems, and applications are identified, authenticated, and authorized across every environment.

CORE IAM CONCEPTS

Identity

Who or what is requesting access — users, devices, applications, and services all have identities.

Authentication

Proving that an identity is who it claims to be — passwords, MFA, biometrics, certificates.

Authorization

What an authenticated identity is allowed to do — determined by policies, roles, and permissions.

Access Control

Enforcing authorization decisions — granting, restricting, or revoking access to resources.

WHY IAM MATTERS

- Identity is the #1 attack vector — over 80% of breaches involve compromised credentials
- Remote work and cloud adoption eliminated the traditional network perimeter
- Compliance frameworks (SOC 2, HIPAA, PCI-DSS) require strong IAM controls
- Insider threats — both malicious and accidental — are managed through IAM

80%	99.9%	$4.45M	#1
Breaches via credentials	Attacks blocked by MFA	Avg breach cost	Attack vector: Identity

02 Authentication vs Authorization

Two different problems — both critical

Authentication and authorization are often confused but they solve fundamentally different problems. Authentication answers 'Who are you?' — it verifies identity. Authorization answers 'What are you allowed to do?' — it enforces access policy. Both must work together for effective IAM.

AUTHENTICATION METHODS

- Something you know — passwords, PINs, security questions
- Something you have — hardware tokens, authenticator apps, smart cards
- Something you are — biometrics: fingerprint, face recognition, retina scan
- Somewhere you are — location-based or network-based access controls

MULTI-FACTOR AUTHENTICATION (MFA)

MFA combines two or more authentication factors. Even if an attacker steals a password, they still need the second factor to gain access. NIST SP 800-63 defines three authenticator assurance levels — organizations should target AAL2 or AAL3 for sensitive systems.

MFA BEST PRACTICES

- Use authenticator apps (TOTP) over SMS — SIM swapping attacks bypass SMS MFA
- Enforce phishing-resistant MFA (FIDO2/WebAuthn) for privileged and executive accounts
- Require MFA at every login — not just the first session
- Monitor for MFA fatigue attacks — repeated push notifications to trick users into approving

AUTHORIZATION MODELS

RBAC

Role-Based Access Control — access based on job role. Most common enterprise model.

ABAC

Attribute-Based Access Control — access based on user, resource, and environment attributes.

PBAC

Policy-Based Access Control — fine-grained policies combining multiple conditions.

DAC/MAC

Discretionary/Mandatory Access Control — owner-defined or system-enforced access rules.

03 Role-Based Access Control (RBA

The right access for the right people

BEMI
IT SOLUTIONS

Role-Based Access Control assigns permissions to roles rather than to individual users. Users are then assigned to roles based on their job function. This simplifies administration, enforces least privilege, and makes access auditing far more manageable at scale.

RBAC CORE COMPONENTS

- Roles — defined job functions: Admin, Manager, Analyst, Read-Only
- Permissions — specific actions on resources: read, write, delete, execute
- Users — assigned to one or more roles based on their function
- Role hierarchy — senior roles can inherit permissions from junior roles

DESIGNING RBAC EFFECTIVELY

RBAC BEST PRACTICES

- Apply least privilege — each role gets only the permissions it needs, nothing more
- Avoid role explosion — too many granular roles become unmanageable
- Conduct regular access reviews — remove roles users no longer need
- Separate duties — no single role should be able to approve and execute a transaction
- Document role definitions and approval workflows for audit purposes

RBAC VS OTHER MODELS

RBAC Strengths

Simple to manage, scales well, easy to audit, maps naturally to org structure.

RBAC Limitations

Struggles with complex, context-sensitive access needs — ABAC supplements it.

04 User Lifecycle Management

Joiner, Mover, Leaver — the identity lifecycle

Every identity has a lifecycle — it is created, modified as the user's role changes, and eventually deactivated when they leave the organization. Managing this lifecycle properly prevents orphaned accounts, over-provisioned access, and security gaps that attackers exploit.

THE JOINER-MOVER-LEAVER MODEL

Joiner

New employee or contractor onboarding — create account, assign roles, provision systems.

Mover

Role change or transfer — update roles, remove old access, add new access immediately.

Leaver

Employee departure — disable account on last day, revoke all access, archive data.

Re-Joiner

Returning employee — restore appropriate access, do not reactivate old permissions.

PROVISIONING & DEPROVISIONING

- Automated provisioning via HR system integration eliminates manual errors
- Role-based templates accelerate onboarding with consistent access sets
- Immediate deprovisioning on termination prevents data exfiltration
- Orphaned accounts — accounts not tied to active users — are a top attack vector

DEPROVISIONING CHECKLIST

- Disable AD/Azure AD account on last working day
- Revoke all SSO sessions and MFA registrations
- Remove from all distribution groups and shared mailboxes
- Disable or transfer service account ownership
- Archive email and files per data retention policy
- Document all access removed for audit trail

05 Single Sign-On, MFA & Federation

One identity, many systems

BEMI IT SOLUTIONS

Single Sign-On (SSO) allows users to authenticate once and access multiple applications without re-entering credentials. Federation extends this across organizational boundaries — allowing users from one organization to access resources in another using their existing identity.

SSO PROTOCOLS

SAML 2.0

XML-based protocol for enterprise SSO — widely used for web apps and cloud services.

OAuth 2.0

Authorization framework — allows apps to access resources on behalf of a user.

OpenID Connect

Identity layer on top of OAuth 2.0 — used for modern web and mobile app authentication.

SCIM

System for Cross-domain Identity Management — automates user provisioning across systems.

IDENTITY PROVIDERS (IDP)

- Microsoft Entra ID (Azure AD) — leading enterprise IdP for Microsoft environments
- Okta — cloud-native IdP with broad app integrations and MFA capabilities
- Google Workspace — IdP for Google-centric organizations
- Ping Identity — enterprise federation and SSO for complex hybrid environments

Microsoft Entra ID | **Okta** | **Ping Identity** | **OneLogin** | **Auth0**

Google Workspace | **CyberArk Idaptive**

FEDERATION & B2B ACCESS

Federation allows organizations to trust identities from external partners, customers, or cloud providers. Instead of creating separate accounts for external users, their home organization authenticates them and asserts that identity to the target system. This is the foundation of B2B collaboration and cloud access.

06 Privileged Access Management (P

Securing the most powerful accounts

Privileged Access Management secures accounts with elevated permissions — administrators, service accounts, root users, and any identity that can modify systems, access sensitive data, or manage other accounts. These are the highest-value targets for attackers, and 74% of data breaches involve privileged credential abuse.

PAM CORE CAPABILITIES

Password Vaulting

Store privileged credentials encrypted. Auto-rotate after each use. No shared passwords.

Session Recording

Capture every privileged session — keystrokes, commands, screen activity — for audit.

Just-In-Time Access

Grant elevated rights only when needed, for a defined time window, then auto-revoke.

Threat Analytics

Detect anomalous privileged behavior in real time and alert before damage occurs.

PAM BEST PRACTICES

- Eliminate shared admin passwords — every privileged session must be individually authenticated
- Enforce MFA for all privileged accounts — no exceptions
- Implement just-in-time access — remove standing privileges wherever possible
- Record and monitor all privileged sessions — real-time and retrospective review

CyberArk | **BeyondTrust** | **Delinea** | **HashiCorp Vault** | **Sailpoint**

07 IAM in Cloud Environments

Identity is the cloud perimeter

In cloud environments, there is no network perimeter. Identity is the only perimeter that matters. Every cloud provider — AWS, Azure, and Google Cloud — has a comprehensive IAM system that controls access to every resource. Misconfigured cloud IAM is one of the leading causes of cloud data breaches.

AWS IAM

- IAM users, groups, roles, and policies control access to every AWS service
- Use IAM roles instead of long-term access keys — roles provide temporary credentials
- Apply the principle of least privilege — start with deny-all and grant only what is needed
- Enable AWS CloudTrail to audit all IAM actions across your account

MICROSOFT ENTRA ID (AZURE AD)

- The identity backbone for Microsoft 365, Azure, and thousands of integrated SaaS apps
- Conditional Access policies enforce MFA, device compliance, and location-based controls
- Privileged Identity Management (PIM) provides just-in-time elevation for Azure roles
- Identity Protection uses ML to detect and remediate risky sign-ins automatically

GOOGLE CLOUD IAM

- Resource hierarchy — Organization, Folder, Project — with inherited permissions
- Predefined roles map to common job functions; custom roles allow fine-grained control
- Workload Identity Federation eliminates service account keys for external workloads

CLOUD IAM COMMON MISTAKES

- Granting Owner or Admin roles when read-only is sufficient
- Using long-term access keys instead of IAM roles with temporary credentials
- Not enabling MFA on root/global administrator accounts
- Leaving unused service accounts and API keys active
- Not auditing IAM policies regularly for permission creep

IAM Governance & Compliance

Audit, review, and stay compliant

IAM governance ensures that access rights are appropriate, reviewed regularly, and aligned with business needs and compliance requirements. Without governance, access accumulates over time — users collect permissions they no longer need, creating a growing attack surface that auditors and attackers will both find.

ACCESS REVIEWS & CERTIFICATION

- Quarterly access reviews — managers certify that their team's access is still appropriate
- Automated access recertification campaigns reduce manual effort and improve consistency
- Revoke access immediately when reviews identify inappropriate permissions
- Document all review outcomes for audit evidence

COMPLIANCE REQUIREMENTS

IAM IN MAJOR COMPLIANCE FRAMEWORKS

- SOC 2 — CC6.1 requires logical access controls, user authentication, and access reviews
- PCI-DSS — Req 7 & 8 mandate least privilege, unique IDs, and MFA for all admin access
- HIPAA — Access controls, audit logging, and workforce authorization for ePHI systems
- NIST SP 800-53 — AC-2 (Account Management) and AC-6 (Least Privilege) are key controls
- ISO 27001 — A.9 covers access control policies, user access management, and reviews

SEPARATION OF DUTIES (SOD)

Separation of Duties prevents any single user from having enough access to execute and conceal a fraudulent transaction. For example, the person who approves a payment should not also be able to process it. IAM systems enforce SoD by preventing conflicting role combinations from being assigned to the same user.

09

Building an IAM Program

A practical roadmap for any organization

BEMI
IT SOLUTIONS

Building an IAM program doesn't have to happen all at once. Start with the highest-impact controls and expand systematically. The goal is a mature identity security posture that scales with your organization.

4-STEP IAM ROADMAP

01

Discover & Inventory

Identify every user, service account, and privileged identity across all systems. You cannot protect what you cannot see. Use IAM discovery tools to find shadow accounts and orphaned identities.

02

Enforce MFA & SSO

Implement MFA on every account — starting with administrators and executives. Deploy SSO to centralize authentication and reduce password sprawl across systems.

03

Implement RBAC & Least Privilege

Define roles based on job functions. Assign only the permissions each role needs. Conduct an access review to remove excessive permissions already in place.

04

Govern & Monitor Continuously

Run regular access reviews, monitor IAM logs for anomalies, automate provisioning and deprovisioning, and expand PAM controls to privileged accounts.

10 IAM Career Pathways

Certifications, roles, and how to break in

IAM is one of the fastest-growing specializations in cybersecurity. Organizations are investing heavily in identity security, and skilled IAM professionals are in high demand. Whether you're starting out or transitioning from another IT role, there is a clear pathway into this field.

IAM JOB ROLES

IAM Analyst

Day-to-day access management, provisioning, access reviews, and helpdesk escalations.

IAM Engineer

Design and implement IAM systems — SSO, MFA, directory services, PAM tools.

IAM Architect

Design enterprise-wide identity strategy across on-prem, cloud, and hybrid environments.

Identity Security Manager

Lead IAM programs, governance, compliance, and vendor management at org level.

KEY CERTIFICATIONS

RECOMMENDED CERTIFICATIONS FOR IAM PROFESSIONALS

- CompTIA Security+ — foundational certification covering IAM, access control, and authentication
- Microsoft SC-300 — Identity and Access Administrator Associate (Azure/Entra ID focused)
- Okta Certified Professional / Administrator — vendor-specific, highly valued in Okta shops
- CISSP — covers IAM as part of the Access Control domain (for senior professionals)
- CISM — management-level certification for IAM governance and program leadership
- CyberArk Defender / Sentry — PAM-specific certifications for CyberArk environments

GETTING STARTED IN IAM

- Learn Active Directory and Microsoft Entra ID — they power most enterprise IAM environments
- Get hands-on with Okta, AWS IAM, or Azure AD using free developer/trial accounts
- Study the NIST SP 800-63 digital identity guidelines and NIST SP 800-53 AC controls
- Build a home lab: set up AD, configure SSO, and practice access reviews

Active Directory | **Microsoft Entra ID** | **Okta** | **AWS IAM** | **CyberArk**

SailPoint | **Saviynt** | **BeyondTrust**

WHAT'S NEXT

Continue Your IAM Journey

You now have a solid foundation in Identity & Access Management. Identity is the new perimeter — and mastering it is one of the highest-value skills in cybersecurity today.

%¶ Watch the Full IAM Training
Free on YouTube @insightswithrayslater

Ø=Ý Zero Trust Security Guide
The companion ebook — kokumorix.gumroad.com/l/lwnzy

Ø<ß Visit bemitechsolutions.com
More courses, ebooks, and cybersecurity resources

Ø=Üç Get the Full Zero Trust Ebook
kokumorix.gumroad.com/l/bmuaev