Making a Career in Identity & Access Management (IAM)

Control who gets in. Control what they can do. Control when they leave.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 12 of 12 (Final)
AUDIENCE	Security professionals and IT engineers moving into IAM and PAM

Contents

Digitally signed by
Baba Shaheer Gutappa
Date: 2026.04.26
18:43:33 +01'00'

1. What Is IAM — and Why Does It Matter?

Identity and Access Management is the set of policies, processes and technologies that ensure the right people have the right access to the right resources — and that no one else does. Every time an employee logs into a system, every time an application calls an API, every time a contractor accesses a client system — IAM is the discipline that controls, monitors and governs that access.

IAM has moved from a back-office IT function to the strategic centre of cybersecurity. With the collapse of the traditional network perimeter — driven by remote work, cloud adoption and third-party access — identity has become the new perimeter. The vast majority of data breaches involve compromised credentials or excessive permissions. IAM is the field that prevents both.

Over 80% of data breaches involve compromised credentials or stolen identities. (Verizon DBIR, 2023). IAM is not a support function — it is the primary security control in every modern organisation.

Level	Typical UK Salary	Common Roles
Junior	£32,000 – £50,000	IAM Analyst, Identity Engineer (junior), AD/Azure AD Engineer
Mid	£52,000 – £75,000	IAM Engineer, PAM Engineer, Identity Architect, SSO Engineer
Senior	£75,000 – £105,000+	Senior IAM Architect, Head of Identity Security, PAM Programme Lead
Specialist	£600 – £1,100/day	IAM Consultant, CyberArk/SailPoint implementation specialist

Table 1: UK salary ranges for IAM and identity security roles (CW Jobs, 2024)

2. The Five Pillars of IAM

IAM is not a single product or technology — it is a discipline covering five interconnected areas. Understanding all five, and how they relate, is essential for any IAM professional.

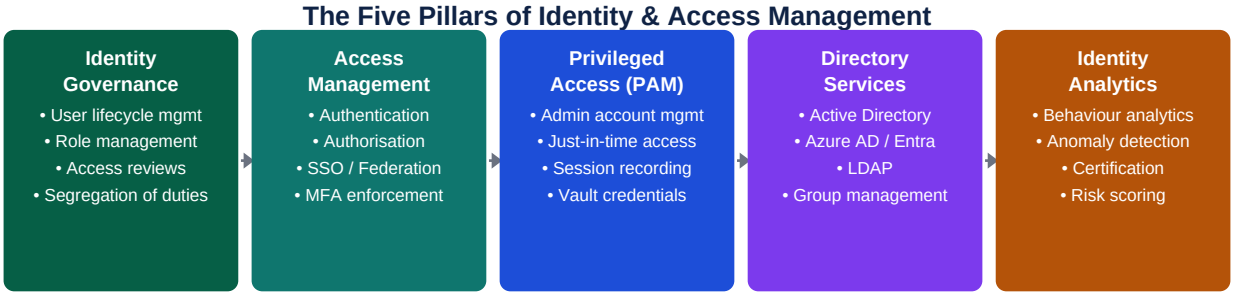


Figure 1: The five pillars of IAM — each addresses a different aspect of identity security.

Pillar	What It Covers	Key Technologies
Identity Governance & Administration (IGA)	User lifecycle (joiner/mover/leaver), role management, access certifications, segregation of duties	SailPoint, Saviynt, Oracle Identity Governance, Microsoft Identity Manager
Access Management	Authentication, authorisation, SSO, MFA, session management	Okta, Azure AD/Entra, Ping Identity, ForgeRock, Auth0
Privileged Access Management (PAM)	Admin account vaulting, just-in-time access, session recording, least privilege for privileged users	CyberArk, BeyondTrust, Delinea (formerly Thycotic), HashiCorp Vault
Directory Services	The central store of identity — users, groups, policies, organisational structure	Microsoft Active Directory, Azure AD/Entra ID, OpenLDAP, Google Cloud Identity
Identity Analytics & Intelligence	Detecting anomalous access patterns, risk-based authentication, certification campaigns	Varonis, Securonix, Microsoft Entra ID Protection, CyberArk Insight

Table 2: The five IAM pillars — coverage and key technologies

3. Authentication — Proving Who You Are

Authentication is the process of verifying that someone is who they claim to be. It is the gateway to every system. Getting authentication wrong is the single most common cause of security incidents — and getting it right is the single most impactful security control an organisation can implement.

Authentication factors and methods

Factor	What It Is	Examples	Security Level
Something you know	Knowledge-based — requires memorisation	Password, PIN, security questions	Low — can be stolen, guessed or phished
Something you have	Possession-based — requires a physical token	TOTP app (Authenticator), hardware key (YubiKey), SMS code	Medium-High — SMS is weak; hardware key is very strong
Something you are	Biometric — requires a physical characteristic	Fingerprint, face ID, retina scan	High — hard to steal, but can be spoofed with effort
Somewhere you are	Location-based — requires network location	IP address range, GPS location, network segment	Medium — easily bypassed with VPN
Something you do	Behavioural — usage patterns	Typing rhythm, mouse movement, device behaviour	Low-Medium — supplementary factor only

Table 3: Authentication factors — types, examples and security level

Modern authentication protocols

- **SAML 2.0 (Security Assertion Markup Language):** XML-based standard for exchanging authentication and authorisation data between an Identity Provider (IdP) and a Service Provider (SP). Foundation of enterprise SSO. Used heavily in corporate environments.
- **OAuth 2.0:** Authorisation framework — allows applications to access resources on behalf of a user without sharing credentials. Powers 'Login with Google/Microsoft' flows. Note: OAuth is for authorisation, not authentication.
- **OpenID Connect (OIDC):** Authentication layer built on top of OAuth 2.0. Adds identity — the IdP confirms who the user is via an ID token. The modern standard for consumer and developer-facing authentication.
- **FIDO2 / WebAuthn:** Passwordless authentication using public key cryptography. The user authenticates with a hardware key or device biometric — no password sent over the network. Highly phishing-resistant.
- **Kerberos:** Authentication protocol used in Microsoft Active Directory environments. Ticket-based system — users receive a Kerberos ticket that proves their identity to services. Understanding Kerberos attacks (Pass-the-Ticket, Kerberoasting) is essential for IAM security.

4. Authorisation — Controlling What You Can Do

Authentication answers 'who are you?' — authorisation answers 'what are you allowed to do?'. These are separate concerns and must be implemented separately. A user who has successfully authenticated still needs to be authorised before they can access any specific resource.

Model	How It Works	Strengths	Common Use
RBAC — Role-Based Access Control	Access granted based on the user's role (e.g. 'Finance Analyst', 'IT Admin')	Simple to manage at scale. Roles map to job functions.	Enterprise applications, Active Directory group membership, cloud IAM
ABAC — Attribute-Based Access Control	Access granted based on attributes of the user, resource and environment (time, location, department, classification)	Very granular. Handles complex policies. Supports dynamic decisions.	Cloud platforms, data classification systems, Zero Trust implementations
PBAC — Policy-Based Access Control	Access governed by explicit policies written in policy language (e.g. OPA, XACML)	Auditable policies. Separation of policy from application code.	Cloud-native applications, microservices, Kubernetes
MAC — Mandatory Access Control	Access governed by security labels — users cannot override labels (top secret, secret, unclassified)	Highest assurance. Cannot be overridden by users.	Government and military systems, classified environments
DAC — Discretionary Access Control	Resource owner controls who can access their resource	Flexible — owners manage their own resources	File system permissions, shared drives

Table 4: Access control models compared

The Principle of Least Privilege — users get the minimum access needed for their job.
Every permission above the minimum is a risk. Excessive permissions are the most common misconfiguration found in IAM security assessments.

5. Privileged Access Management (PAM)

Privileged accounts — domain admins, local admins, service accounts, database administrators, cloud super-admins — are the keys to the kingdom. If an attacker obtains a privileged account, they can access everything. PAM is the discipline of protecting, controlling and monitoring these accounts.

Core PAM capabilities

- **Credential vaulting:** Privileged account passwords are stored in an encrypted vault and never disclosed to users. When a user needs privileged access, they check out a session — they never see the actual password. CyberArk Digital Vault is the market leader.
- **Just-in-Time (JIT) access:** Privileged access is granted only when needed and automatically revoked when the task is complete. A sysadmin does not have permanent domain admin — they request it, use it for 2 hours, and it is removed. Massively reduces attack surface.
- **Session recording:** Every privileged session is recorded — all commands typed, all screens viewed, all data accessed. Recordings are stored for audit purposes and provide evidence for incident investigations.
- **Least privilege for service accounts:** Service accounts (used by applications and automation) are notoriously overpermissioned. PAM programmes audit and restrict service account permissions — and rotate their passwords automatically.
- **Privileged Threat Analytics:** Monitoring privileged account behaviour for anomalies — an admin accessing systems they never normally touch, at unusual hours, is a red flag. Tools: CyberArk PTA, BeyondTrust.

PAM Platform	Market Position	Key Strengths	Typical Deployment
CyberArk	Clear market leader	Most comprehensive PAM — vault, JIT, session mgr, threat analytics. Standard in financial services and government.	Large enterprise, financial services, government
BeyondTrust	Strong #2	Good combination of PAM + endpoint privilege management (EPM). Easier to deploy than CyberArk.	Enterprise, healthcare, manufacturing
Delinea (Thycotic/Centrify)	Growing	Cloud-friendly PAM. Secret Server for vaulting. Strong for hybrid cloud environments.	Mid-market to enterprise, cloud-first orgs
HashiCorp Vault	Open-source / DevOps	Developer-focused secrets management. Excellent for dynamic credentials in CI/CD pipelines.	Tech companies, DevOps teams
Microsoft PIM	Native Azure	Privileged Identity Management — JIT for Azure AD roles. Free with Azure AD P2.	Microsoft-centric organisations

Table 5: Major PAM platforms — market position and strengths

6. Identity Governance and Administration (IGA)

IGA is the operational backbone of IAM — the processes and tools that manage identity throughout the user lifecycle. From the day someone joins an organisation to the day they leave, IGA governs what access they have, whether it is appropriate, and whether it is being reviewed.

The Joiner-Mover-Leaver (JML) process

The JML process is the most fundamental IGA concept. Every access-related problem in most organisations traces back to a failure in one of these three stages:

Stage	What Happens	Common Failures	IAM Controls
Joiner — new starter	New employee account created, appropriate access granted based on role	Too much access granted (copy from previous employee). Access granted before background checks complete.	Role-based provisioning from HR system. Access request workflow with manager approval. Automated triggers from HR.
Mover — role change	Employee changes department, promoted or transfers — access should change	Old access not removed. New access added but incompatible with old access (creates SoD violation).	Automated de-provisioning of old role on transition. SoD policy enforcement. Manager re-certification.
Leaver — employee leaves	Employee leaves — all access must be immediately removed	Accounts left active for weeks after departure. Service accounts forgotten. Third-party access not revoked.	HR-triggered immediate account disable. Automated deprovisioning. Contractor/vendor access review. Token revocation.

Table 6: Joiner-Mover-Leaver process — stages, common failures and controls

Access certifications

Access certifications (also called access reviews or access recertification) are periodic exercises where managers or resource owners review and confirm that each user's access is still appropriate. They are required by most compliance frameworks (SOX, PCI DSS, ISO 27001) and are a core IGA activity. Platforms like SailPoint and Saviynt automate the scheduling, workflow and reporting of certification campaigns.

7. Single Sign-On (SSO) and Federation

Single Sign-On allows users to authenticate once and gain access to multiple applications without re-entering credentials. Federation extends this across organisational boundaries — a user authenticates with their company identity provider and accesses a partner or SaaS application without a separate account.

Concept	What It Means	Standard Used	Example
SSO	One login grants access to multiple internal applications	SAML, OIDC, Kerberos	Employee logs into their laptop — automatically authenticated to email, HR system, file share
Federated Identity	Identity trusted across organisation boundaries	SAML, OIDC, WS-Federation	University student uses their university login to access Microsoft 365 or Zoom
Social Login	Third-party identity provider used for authentication	OAuth 2.0 + OIDC	'Login with Google' on a consumer app — Google confirms identity
SCIM	Automated provisioning/deprovisioning across cloud apps	SCIM 2.0	When Okta adds a user, it automatically creates their Salesforce and Slack accounts

Table 7: SSO, federation and related identity concepts

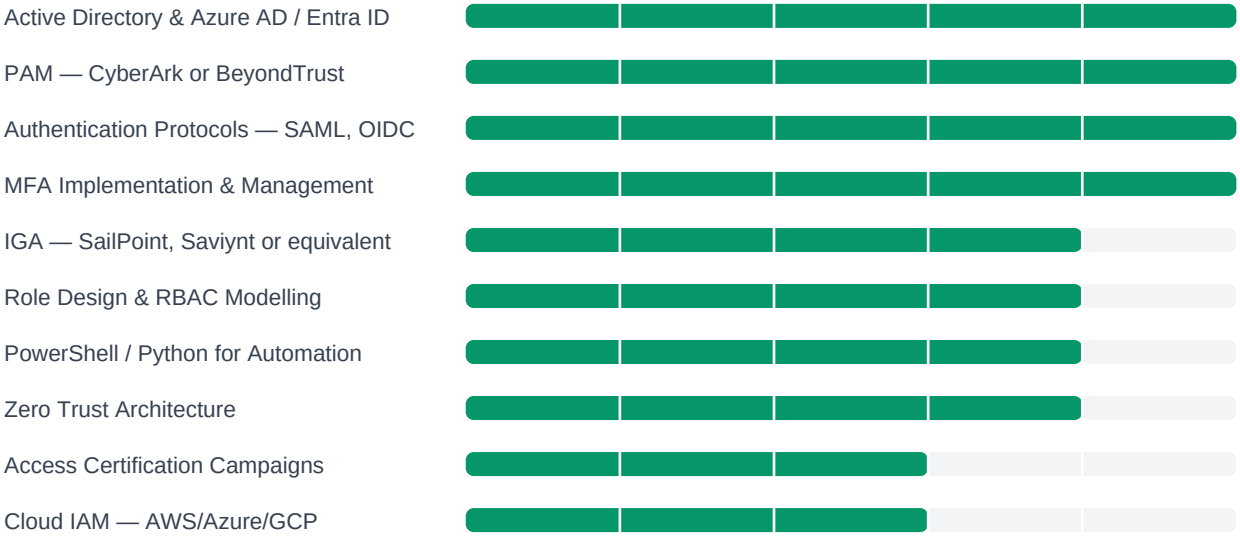
8. Zero Trust and the Identity Perimeter

Zero Trust treats identity as the primary security perimeter. Every access request — regardless of where it comes from — must be verified. IAM professionals are central to Zero Trust implementation because identity is where verification happens.

Figure 2: Zero Trust identity flow — every access request authenticated, evaluated and logged.

9. Core Skills and Tools

Skills expected at mid-level IAM engineer:



Tool / Platform	Category	What It Does	Cost
Microsoft Active Directory / Entra ID	Directory & Identity Platform	The dominant enterprise identity platform. AD for on-premise, Entra ID for cloud. Knowing both is essential.	Included with Microsoft 365
Okta	Identity Platform / SSO	Market-leading cloud identity platform. SSO, MFA, lifecycle management, API access management.	Commercial
CyberArk	PAM	Market-leading PAM platform. Credential vault, session management, JIT access, threat analytics.	Commercial
SailPoint IdentityNow / IIQ	IGA	Market-leading IGA platform. Role mining, access certification, joiner/mover/leaver automation.	Commercial
BeyondTrust	PAM + EPM	PAM plus endpoint privilege management. Good for organisations reducing local admin rights.	Commercial
Azure AD / Entra ID PIM	PAM (Microsoft)	Privileged Identity Management for Azure roles. JIT access, approval workflows, access reviews.	Free with Azure AD P2
HashiCorp Vault	Secrets Management	Dynamic secrets, credential rotation, PKI. Essential for DevOps/cloud IAM.	Free / Commercial
Ping Identity	SSO / Federation	Enterprise SSO and federation platform. Strong in financial services.	Commercial
Saviynt	IGA / Cloud PAM	Modern IGA with strong cloud PAM capabilities. Growing competitor to SailPoint.	Commercial
PowerShell / Graph API	Automation	Automate AD and Entra ID tasks. Essential skill — most IAM engineers automate user lifecycle.	Free

Table 8: Core tools for IAM professionals

10. Career Paths in IAM

IAM offers clear career progression from operational roles to architecture and leadership. It is one of the highest-paying technical specialisms in cybersecurity — particularly for specialists in CyberArk, SailPoint or Okta who are consistently in short supply. It also bridges technical and business roles more than most.

Role	What You Do	Where You Work	UK Salary
IAM Analyst / AD Engineer	Day-to-day identity operations — account management, group policy, access requests, provisioning.	Large enterprises, NHS, government	£32k–£50k
IAM Engineer	Implement and maintain IAM platforms — SSO, MFA, PAM configuration, lifecycle management.	Financial services, tech companies	£52k–£70k
PAM Engineer / Specialist	Implement and run PAM programmes — CyberArk or BeyondTrust deployment, vault management, session management.	Banks, critical infrastructure, consulting	£58k–£80k
IGA Engineer / Analyst	Implement IGA platforms — SailPoint, Saviynt. Role model, certification campaigns, provisioning connectors.	Large enterprises, consulting firms	£55k–£75k
IAM Architect	Design IAM strategy and architecture — Zero Trust identity, PAM programme, IGA roadmap, cloud identity.	Large enterprises, consulting	£75k–£105k
Head of Identity Security	Own the identity security programme. Team management. Interface with CISO and board.	Large enterprises, financial services	£90k–£120k+
IAM Consultant	Independent implementation and advisory — CyberArk, SailPoint, Okta specialist.	Self-employed, big 4 consulting	£600–£1,100/day

Table 9: Career paths in IAM (Reed, 2024; CW Jobs, 2024)

11. The Learning Roadmap

IAM has one of the clearest entry paths in cybersecurity for people coming from IT operations or system administration backgrounds. If you already manage Active Directory or Azure AD, you are already doing IAM — the security specialisation adds depth to that foundation.

1 — Master Active Directory and Azure AD / Entra ID
If you do not know AD deeply — users, groups, OUs, GPOs, trusts, Kerberos — start here. Microsoft Learn has excellent free content on both AD and Entra ID. Build a home lab with a domain controller. 4–6 weeks.

2 — Learn authentication protocols
Understand SAML 2.0, OAuth 2.0 and OpenID Connect. Know how SSO flows work step by step. Understand Kerberos authentication and its common attack vectors (Pass-the-Ticket, Kerberoasting, Golden Ticket). 3–4 weeks.

3 — Get hands-on with MFA and Conditional Access
Set up Azure AD Conditional Access in a free tenant. Configure MFA requirements. Test Named Locations and device compliance policies. This is one of the most in-demand IAM skills in UK organisations using Microsoft 365. 2 weeks.

4 — Learn PAM concepts and CyberArk basics
CyberArk offers free training on their Blueprint programme. Understand credential vaulting, JIT access, session recording. Even theoretical CyberArk knowledge is valued — the platform is everywhere. 3–4 weeks.

5 — Study IGA — SailPoint or Saviynt
SailPoint University has free training. Understand the joiner/mover/leaver model, role management and access certifications. IGA specialists are chronically scarce and well-paid — this is a high-value specialisation. 3–4 weeks.

6 — Get the Microsoft SC-300 certification
SC-300 (Identity and Access Administrator) is the most relevant Microsoft identity certification. Validates Entra ID, Conditional Access, PIM, B2B/B2C. Highly valued by UK employers. 4–6 weeks.

7 — Add PAM certification
CyberArk Defender (entry) then CyberArk Sentry — the most widely required PAM certifications. BeyondTrust University offers free training. Either platform certification opens senior PAM engineer roles.

8 — Apply for IAM roles
Active Directory Engineer, IAM Analyst and Identity Engineer roles are widely available. With SC-300 and CyberArk Defender your CV is competitive for mid-level positions. Financial services, NHS, government and MSSPs all hire regularly.

Timeline from IT background: 9–14 months to IAM engineer.
From AD/Azure AD background: 4–8 months adding security specialisation.

12. Certifications That Matter

Certification	Level	Provider	Focus	Why It Matters
SC-300 — Identity and Access Administrator	Mid	Microsoft	Entra ID, Conditional Access, PIM, B2B/B2C, application integration	The most sought-after IAM certification for Microsoft-stack organisations — a large proportion of UK enterprises.
CyberArk Defender	Beginner–Mid	CyberArk	CyberArk PAM platform — vault administration, access control, session management	Entry-level CyberArk cert. Required or strongly preferred for PAM engineer roles.
CyberArk Sentry	Mid	CyberArk	Advanced CyberArk — complex deployments, integrations, troubleshooting	Mid-level CyberArk cert. Opens senior PAM roles at financial services and government.
Okta Certified Professional	Mid	Okta	Okta platform — SSO, MFA, lifecycle management, API access	Highly valued for organisations using Okta — increasingly common in UK tech and SaaS companies.
SailPoint Certified IdentityNow Engineer	Mid	SailPoint	SailPoint IGA platform — source management, role modelling, certifications	IGA specialists are scarce. SailPoint cert validates the most in-demand IGA platform skill.
CIAM — Certified Identity and Access Manager	Mid	IDPRO / (ISC)2	Vendor-neutral IAM programme management, governance, compliance	Emerging vendor-neutral certification for IAM professionals moving into management.
CompTIA Security+	Beginner	CompTIA	Broad security foundations including identity and access concepts	Good baseline before specialising. Required by some employers as prerequisite.

Table 10: IAM certifications in order of relevance and progression

13. Case Study — A Credential Breach Through Overpermissioned Accounts

> This fictional case study is based on common real-world IAM failure patterns.
> Overpermissioned accounts and stale access are involved in the majority of breaches.

The Organisation

Meridian Legal LLP is a 400-person UK law firm. They use Microsoft 365 and an on-premise file server for client case files. There is no PAM programme, no access certification process and no automated leavers procedure. Access is managed manually by a single IT administrator.

The problem — discovered during an IAM assessment

IAM assessment findings — three critical issues

Issue 1: A former senior partner who left 14 months ago still has an active Azure AD account with a valid Microsoft 365 licence, access to all client SharePoint sites and a mailbox containing confidential case correspondence. No one removed their account when they left.

Issue 2: A paralegal who was promoted to associate 2 years ago has both their old paralegal permissions and their new associate permissions — including access to the partners' billing system they should never have had.

Issue 3: The IT admin account 'admin_backup' with domain admin rights was created during a system migration 3

What happens — the breach

The former partner's account is compromised

A threat actor obtains the former partner's email address and password from a dark web credential dump — from a breach of a third-party service where she reused her password. No MFA is enforced on the account.

The attacker logs into Microsoft 365 using the valid credentials. Because the account was never deprovisioned, they have full access to 14 months of client case files, correspondence and commercially sensitive documents — all of which are exfiltrated over three days before the firm detects the unusual access pattern.

The IAM controls that would have prevented each failure

- **Automated leavers process:** Integration between HR system and Azure AD — when employment ends, account is automatically disabled within 24 hours. No manual dependency.
- **MFA enforcement via Conditional Access:** Even with valid credentials, the attacker would have been blocked — no way to satisfy the MFA challenge without access to the former partner's phone
- **Access certification campaign:** A quarterly review would have flagged the active account for a departed employee within 90 days of departure
- **Privileged account management:** The 'admin_backup' account would have been discovered, its purpose validated, and either deleted or vaulted with a rotated password
- **Mover process review:** Role change workflow with automatic removal of old access when new access is granted — preventing the paralegal/associate access accumulation

The entire breach was caused by a single IAM process failure: no leavers procedure.
An automated joiner/mover/leaver process would have cost roughly £15,000 to implement.
The breach — investigation, legal costs, ICO notification, client impact — cost £380,000+.

14. Breaking In — Getting Your First Role

IAM is one of the most accessible cybersecurity specialisms for people coming from IT operations, system administration or helpdesk backgrounds. You are likely already doing parts of IAM — managing AD accounts, handling access requests, setting up new starters. The specialisation adds security depth and strategy.

Build visible evidence of IAM skill

- **Free Azure AD / Entra ID tenant:** Create a free Microsoft 365 developer tenant. Configure Conditional Access policies, set up MFA, enable PIM for a test admin role, configure an enterprise application with SSO. Screenshot everything — this is your lab portfolio
- **CyberArk Blueprint training:** CyberArk offers free online training. Complete the Defender track. Even without a live platform, the certification demonstrates you understand the market-leading PAM product
- **SailPoint University free courses:** Complete the SailPoint IdentityNow fundamentals. IGA specialists are genuinely scarce — any validated IGA platform knowledge is valuable
- **Active Directory attack lab:** Build an AD lab using Windows Server Evaluation (free). Install BloodHound. Run it against your own domain. See what privilege escalation paths exist. This demonstrates both AD knowledge and security thinking
- **Write a JML process design:** Document how you would design a joiner/mover/leaver process for a 200-person company. Include the HR integration, the access request workflow, the certification schedule. Shows IAM programme thinking beyond just tooling

Where to Look	Notes
CyberSecurityJobs.com	Search 'IAM engineer', 'identity engineer', 'PAM engineer', 'CyberArk', 'SailPoint'
LinkedIn	IAM roles post heavily — recruiters actively seek CyberArk and SailPoint specialists. SC-300 in your profile gets attention
Financial services (banks, insurers)	Largest IAM programmes in UK. Banks run dedicated IAM teams with constant hiring needs
NHS / public sector	Large AD environments, complex identity programmes. Entry-level accessible with SC-300
Big 4 and consulting (Deloitte, KPMG, Accenture, IBM)	IAM consulting practices — implementation projects across multiple clients. Excellent for breadth
CyberArk / SailPoint / Okta partner firms	System integrators that implement these platforms hire platform-certified engineers constantly

Table 11: Where to find IAM roles

Interview questions to prepare for

- What is the difference between authentication and authorisation? Give a practical example of each.
- Walk me through how SAML SSO works — step by step from user login to application access.
- What is a Kerberoasting attack and how would you detect and prevent it?
- Explain the Joiner-Mover-Leaver process. What are the most common failure points?

- What is Just-in-Time access and why is it better than standing privileged access?
- How would you approach an access certification campaign for an organisation with 5,000 users?
- What is Segregation of Duties (SoD) and why is it important?
- A user reports they can still access systems from their previous role. Walk me through how you investigate and remediate this.

The best IAM interview answer:
"Here is my Azure AD Conditional Access lab. Here is the CyberArk Defender cert."
Platform-specific knowledge consistently beats general identity theory.

15. References

1. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 10 April 2026].
2. CyberArk (2024) *CyberArk Blueprint Training and Certification.* Available at: https://www.cyberark.com/resources/training/ [Accessed: 10 April 2026].
3. IDPro (2024) *CIAM — Certified Identity and Access Manager.* Available at: https://idpro.org/cidpro/ [Accessed: 11 April 2026].
4. Microsoft (2024) *SC-300: Microsoft Identity and Access Administrator.* Available at: https://learn.microsoft.com/en-us/certifications/identity-and-access-administrator/ [Accessed: 11 April 2026].
5. Microsoft (2024) *What is Privileged Identity Management (PIM)?* Available at: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/ [Accessed: 12 April 2026].
6. NIST (2022) *Digital Identity Guidelines (SP 800-63-3).* Available at: https://doi.org/10.6028/NIST.SP.800-63-3 [Accessed: 12 April 2026].
7. NIST (2020) *Zero Trust Architecture (SP 800-207).* Available at: https://doi.org/10.6028/NIST.SP.800-207 [Accessed: 12 April 2026].
8. Okta (2024) *Okta Certified Professional Programme.* Available at: https://www.okta.com/training/certification/ [Accessed: 13 April 2026].
9. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 13 April 2026].
10. SailPoint (2024) *SailPoint University — Identity Security Training.* Available at: https://university.sailpoint.com [Accessed: 13 April 2026].
11. Verizon (2023) *Data Breach Investigations Report 2023.* Available at: https://www.verizon.com/business/resources/reports/dbir/ [Accessed: 14 April 2026].

This is the final document in the Cybersecurity Career Series by Babashaheer.

01 — Ethical Hacking | 02 — Career Tree | 03 — Digital Forensics & IR
04 — Malware Analysis | 05 — Network Security | 06 — Application Security
07 — Cloud Security | 08 — SOC / Blue Team | 09 — GRC
10 — Threat Intelligence | 11 — OT/ICS/SCADA | 12 — IAM (this document)

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 12 of 12.