



Privileged Access Management Service Description

Secure digital assets by protecting
elevated access entitlements everywhere



Table of Contents

1	DXC Digital Identity for UK Public Sector	3
1.1	DXC Overview	3
1.2	Identity is the New Security Perimeter	4
1.3	UK Public Sector Challenges	4
1.4	DXC Privileged Access Management Services	5
1.5	PAM Service Features	6
1.6	PAM Service Benefits	7
1.7	End-to-End PAM Services	7
1.8	User support and ticketing support.....	8
2	Case studies.....	9
2.1	DXC an Experienced Partner.....	9
2.2	Secure UK Government Delivery	9
2.3	CIAM for a Transport Ministry	11
2.4	National digital identity for 4 million citizens	11
2.5	City police digital transformation	11
2.6	UK Defence – Zero Trust and secure communications	11
2.7	Did you know?	12
3	DXC Delivery Approach.....	13
3.1	DXC IAM Capability Model.....	13
3.2	DXC IAM Delivery Methodology.....	13
3.2.1	IAM strategy definition	14
3.2.2	Identity programme	15
3.2.3	Managed operational services.	15
4	About DXC Technology	16

List of Tables

Table 1.	Incident Priorities and Impacts.	8
----------	---------------------------------------	---

List of Figures

Figure 1.	DXC Identity Services	3
Figure 2.	Identity is your security perimeter	4
Figure 3.	DXC PAM Services.....	5
Figure 4.	Erskine – Flagship UK Delivery Centre	10
Figure 5.	DXC IAM Capability Model	13
Figure 6.	DXC End-to-end IAM Methodology	14
Figure 7.	DXC PAM protects public service providers and users.	17

1 DXC Digital Identity for UK Public Sector

1.1 DXC Overview

DXC Technology delivers end-to-end Identity and Access Management services that enable UK public sector organizations to secure digital identities, enforce Zero Trust principles, and meet stringent compliance requirements such as GDPR, NHS Digital standards, and MoD security frameworks.

- Identity Governance and Administration (IGA) for compliant and accountable identity lifecycle management.
- Privileged Access Management (PAM) for safeguarding the privileged accounts that control your critical systems.
- Passwordless adaptive authentication for frictionless user experiences, making secure access easy to use access.
- Decentralised identity to enable use of citizen e-wallets to carry verified attributes and verified credentials to streamline access to public services for everybody while protecting their privacy and reducing the risk of data breaches.
- DXC Key and Certificate Services provide centralized management of encryption keys and certificates on a crypto agile platform to ensure secure communication, establish trust, and streamline regulatory compliance.
- Access Management services: Single Sign-On (SSO) across applications and IT services. Adaptive intelligent authentication and authorisation. Consistent enforcement of access policies everywhere. Secure work from anywhere and on any device. Improved authentication experiences without compromising security.
- Enable access by citizens and customers to public services via digital and physical channels with CIAM to enable service innovation, cost effective delivery while protecting privacy and ensuring security and compliance.

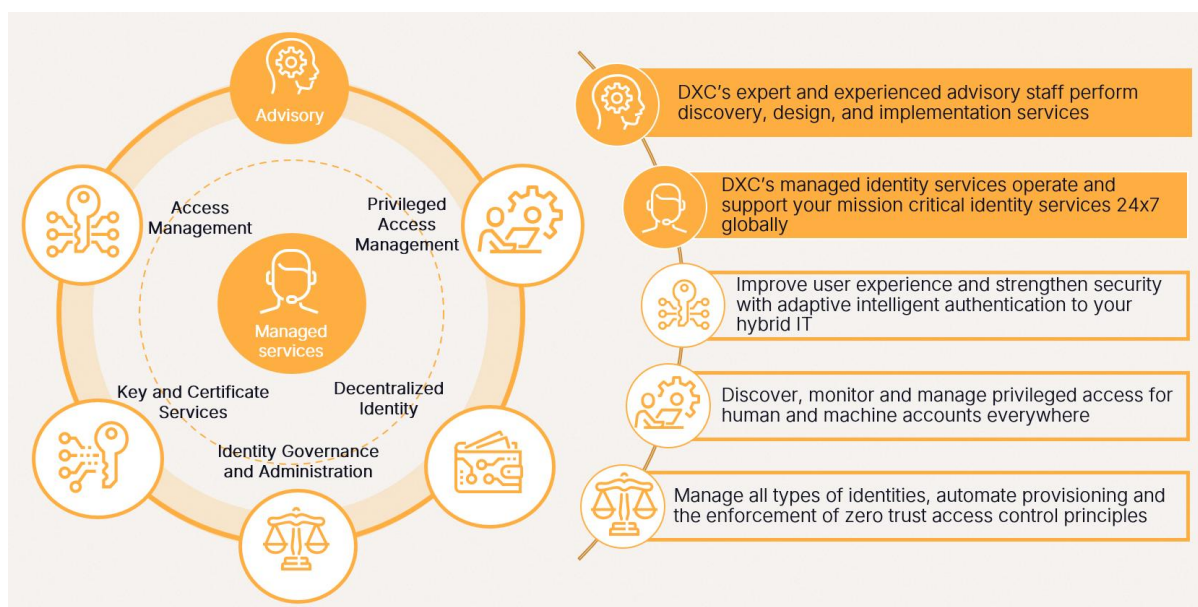


Figure 1. DXC Identity Services

1.2 Identity is the New Security Perimeter

Digital Identity is a foundation of any modern security infrastructure and a key pillar for a Zero Trust approach to security.

Digital identity is now central to how we live and work—whether logging into apps, accessing healthcare, or conducting financial transactions. DXC's solution positions identity as a foundational element of digital transformation, enabling secure, scalable, and privacy-respecting interactions.

DXC's Digital Identity services enhance privacy, build digital trust, maintain regulatory compliance, and drive operational efficiency across digital interactions that rely on trusted identity.

Commercial and government services have moved to digital channels to enable improved service delivery, greater efficiency and innovative service delivery. This shift to digital has also increased the focus on cybersecurity and regulatory compliance for data privacy. Identity has become increasingly the primary security control plane that determines who or what has access to which data and what they are allowed to do to that data.

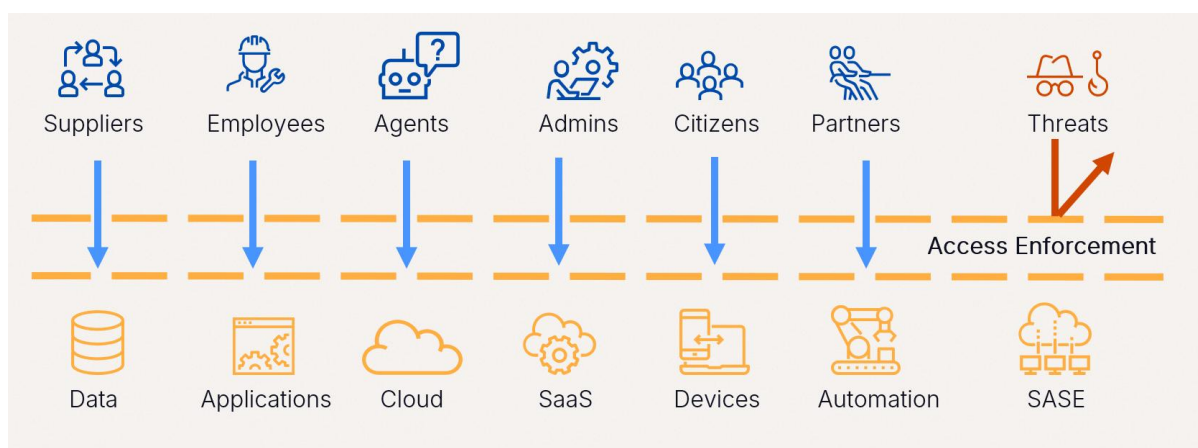


Figure 2. Identity is your security perimeter

1.3 UK Public Sector Challenges

UK Public Sector needs regulatory compliance, cost reduction, improved security stance, improved user authentication experiences, greater flexibility of service delivery, all while accelerating their shift to digital channels, and the growth in citizen adoption of digital channels and adoption of a Zero Trust security approach.

Government has complex hybrid and multi-cloud environments with geographically dispersed and remote and home working staff, citizens and a growing number of connected machines. How to deliver adaptive intelligent authentication that enforces access policies everywhere while facing fast changing threats?

Multi-cloud and hybrid environments, combined with geographically dispersed users and growing IoT ecosystems, require advanced orchestration and zero-trust security. Integration across fragmented government systems and data silos remains challenging, while balancing cost efficiency, scalability, and user experience. Additionally, skills shortages and risk-averse governance often slow adoption of innovative features like Passwordless authentication and decentralized identity. Compliance with stringent regulations like GDPR, NHS Digital standards, and MoD security frameworks adds operational complexity.

1.4 DXC Privileged Access Management Services

DXC Privileged Access Management (PAM) services enable secure access for people and machines to privileged accounts or roles and entitlements that provide elevated access rights. All while remaining compliant with regulations, protecting privacy and defending against cyber-attacks.

DXC's services support the UK public sector to drive efficiency and service modernisation. Services that strengthen identity security by tightly controlling access through managing the provisioning of accounts, roles and access entitlements while logging and auditing all changes. Managing identities for people, machines and AI agents both on premises and in the cloud, across applications, services, and IT infrastructure of the public sector and commercial suppliers.

DXC Identity services are powered by industry-leading technology such as CyberArk, BeyondTrust, Microsoft, SailPoint, Ping Identity, RedHat, Okta, Thales, AWS, GCP, and ServiceNow underpinned with expert advisory and managed security services.

DXC is experienced in deploying large PAM solutions for complex clients providing mission critical services. Improving the experience for employees, partners, and suppliers by providing the right access when it is needed to support productivity and operational efficiency but not granting more access than is required for longer than is absolutely needed.

The following diagram provides an overview of the DXC PAM services being detailed in this service description.

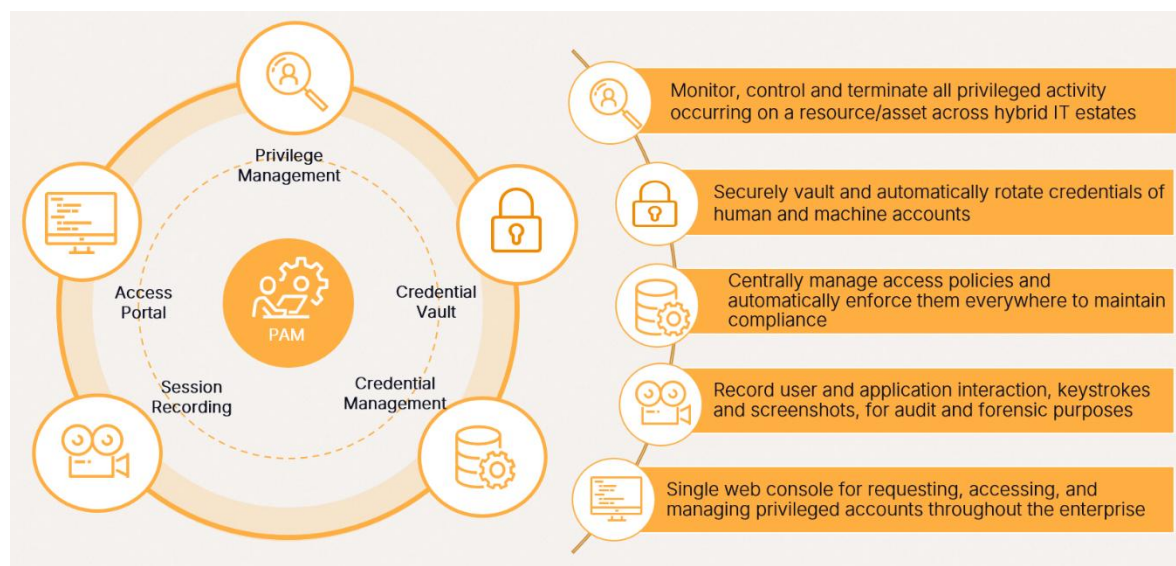


Figure 3. DXC PAM Services

DXC ensures secure, scalable, and compliant identity security services for your mission-critical environments. DXC is qualified and experienced to design, implement and support your identity solutions:

- With 450M+ identities managed globally,
- 3,200+ security professionals,
- and UK-based SC/DV-cleared teams.

DXC's Digital Identity portfolio is composed of five main capabilities:

1. Identity Governance and Administration
2. Privileged Access Management

3. Access Management
4. Decentralised Identity
5. Key and Certificate Services

1.5 PAM Service Features

Deterring cyber-attacks, reducing the cost of regulatory-compliance, and enabling nimble adaptation to new ways of delivering public services is key to digital success.

Features and capabilities of DXC PAM Services:

1. **Privilege Visibility.** Deep visibility into privileged accounts and credentials across complex government IT ecosystems, identifying vulnerabilities and misconfigurations proactively to reduce security risks and ensure compliance with stringent UK public sector regulations.
2. **Credential Management.** Implement lifecycle management for privileged credentials, including secure generation, storage, and automated rotation, ensuring that sensitive government systems remain protected against unauthorized access and credential misuse.
3. **User Accountability.** Track and analyse privileged user actions in real time, including internal administrators and external suppliers, to maintain transparency, detect anomalies, and meet UK government compliance and audit requirements.
4. **Least Privileged.** Apply comprehensive least-privilege controls across all identities whether human or machine, ensuring every user and automated process operates with only the permissions required, significantly reducing potential attack surfaces and reinforcing security for essential government systems and services.
5. **Robust Logging.** Generate comprehensive audit trails capturing every privileged access event, providing clear evidence for compliance audits, investigations, and governance reporting, aligned with UK public sector security standards.
6. **DevSecOps Integration.** Seamlessly connect PAM capabilities with modern automation frameworks, including DevOps pipelines, robotic process automation bots, and IT service management platforms, enabling secure and efficient operations across government technology environments.
7. **Automated Workflows.** Streamline privileged access provisioning and compliance checks through automated workflows, reducing manual effort, accelerating approvals, and ensuring adherence to UK government security policies.
8. **ITSM Integration.** Enhance governance by linking PAM processes with ITSM systems, enabling automated validation and approval of privileged change requests, ensuring accountability and compliance with public sector change management protocols.
9. **Session Recording.** Capture detailed session activity—including keystrokes and video—for privileged accounts, providing forensic evidence and assurance against misuse, while supporting UK government audit and security requirements.
10. **JIT.** Deliver secure, time-bound privileged access through Just-In-Time provisioning, minimizing exposure by granting elevated permissions only when necessary, and automatically revoking them after use to protect sensitive government systems.

1.6 PAM Service Benefits

Protect “The keys to the kingdom” privileged accounts and elevated access rights that bad actors are seeking to takeover and exploit to steal data, deploy ransomware or disrupt your critical operations.

1. **Control Privilege.** Gain complete control of privileged accounts across critical government IT systems, ensuring secure access, preventing misuse, and enhancing resilience against sophisticated cyber threats targeting public services.
2. **Zero Trust.** Implement Zero Trust principles by enforcing least privilege and continuous authentication, safeguarding sensitive public sector data while enabling secure, verified access for employees and third-party suppliers.
3. **Detect and Respond.** Protect government networks from insider threats and ransomware by monitoring privileged activity, detecting anomalies early, and applying proactive controls to safeguard sensitive citizen data and critical public sector operations.
4. **Recover Fast.** Minimise breach exposure with rapid detection and automated response, reducing downtime and accelerating remediation to maintain uninterrupted public services and compliance with UK government security standards.
5. **Minimise Privileges.** Eliminate unnecessary standing privileges across systems to shrink attack surfaces, ensuring only time-bound, approved access for critical tasks and reducing opportunities for exploitation or compromise.
6. **Regulatory Compliance.** Maintain compliance with UK and EU regulations including GDPR, PCI DSS, DORA, and NIS2 through robust privileged access controls, audit trails, and continuous monitoring.
7. **Accelerate Transformation.** Support secure digital transformation initiatives by protecting privileged access across legacy and cloud systems, ensuring trusted delivery of modernised government services for citizens.
8. **User Accountability.** Monitor and record privileged actions by administrators and suppliers, ensuring accountability, compliance, and providing insights for targeted security training across public sector teams.
9. **Insurance Qualification.** Strengthen cyber insurance eligibility by demonstrating robust privileged access management, regulatory compliance, and proactive risk mitigation strategies aligned with UK public sector security frameworks.
10. **Strong Authentication.** Enhance security posture with enforced multi-factor authentication, secure credential vaulting, and automated password rotation, reducing credential theft risks and ensuring resilience against sophisticated cyberattacks.

1.7 End-to-End PAM Services

Secure and manage privileged accounts and elevated entitlements to protect against threat actors, maintain regulatory compliance, and drive operational efficiency.

Advisory Services

- Identity Risk Assessment: Identify exposure points in privileged identity.
- Strategy and Roadmap: Define an identity security strategy aligned with regulatory compliance and your organisational goals.
- Tool Selection: Recommend PAM tools and identity security platforms.

- Regulatory Compliance: Alignment with DORA, UK Digital Trust Framework, eIDAS 2.0, GDPR, and NIS2.

Managed Services

- 24/7 Monitoring: Continuous oversight of identity usage and system access.
- Audit and Activity Logs: Maintain immutable logs of access and interactions.
- Expert Support: Provide skilled teams to manage your identity security infrastructure.

Delivery Services

- Session Management: Enforce access policies and record credential usage.
- Workflow Integration: Integrate with ITSM tools for change management, user provisioning and credential reset.
- Automated Onboarding: Use identity proofing and credential issuance for seamless onboarding.

1.8 User support and ticketing support

Users can manage the status and priority of their support tickets. When Incidents are either detected by DXC or reported by authorized Customer personnel, DXC will classify them according to the priorities listed in the table below.

Table 1. Incident Priorities and Impacts.

Priority	Operational Impact	Business Impact
Critical (P1)	Failure on multiple Devices, systems, or user accounts.	Major impact on Customer's business
High (P2)	Failure of single system or Device.	High impact on Customer's business
Medium (P3)	Specific feature of system or Device unavailable or malfunctioning, or single user failure.	Limited impact on Customer's business
Low (P4)	No operational impact.	No business impact

2 Case studies

2.1 DXC an Experienced Partner

DXC is experienced in deploying large enterprise privileged access management solutions. Improving the user experience for system administrators, developers, testers, employees, partners, and suppliers.

DXC provides end to end services from expert privileged access management policy advisory, design, and implementation through to managed identity security services. DXC offers integrated management of digital identities and credentials to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Digital Identity Services are powered by industry-leading technology companies such as CyberArk, Microsoft, Ping Identity, BeyondTrust, AWS, GCP, Salesforce, ServiceNow, Oracle, Okta, Thales, and DigiCert.

DXC has over 30 years of experience with modernizing identity solutions. We know how to run what you have while deploying the latest technology to maximise efficiency and service improvements in the public sector. We are helping our public sector customers run their mainframes and deploy the latest autonomous AI agents safely and effectively.

- **Trusted relationships.** We're committed to delivering mission critical access management services for customers in banking, government, healthcare, energy and manufacturing.
- **Efficiency expertise.** We help you consolidate multiple legacy solutions into a single integrated solution leveraging your existing identity security investments and the capabilities of the latest identity security platforms.

2.2 Secure UK Government Delivery

DXC Technology provides secure, accredited delivery capabilities across three UK locations (Newcastle, Farnborough and Erskine) ensuring compliance with government security standards and supporting mission-critical programmes. Our Erskine Delivery Centre is a flagship facility designed for high-assurance services to UK Public Sector clients.

Comprehensive Service Portfolio:

- **Networks and Testing** – Secure network design, validation, and performance assurance.
- **Service Management** – ITIL-aligned operations for consistent, reliable service delivery.
- **Cybersecurity Services** – Advanced threat protection, monitoring, and incident response.
- **Identity Services** – End-to-end IAM solutions for citizen and workforce security.
- **Operational Account Delivery** – Dedicated teams for account governance and continuity.
- **Peripheral Packaging** – Secure configuration and deployment of end-user devices.
- **Project and Programme Management** – Agile and waterfall methodologies for complex initiatives.
- **Architecture and Engineering Design** – Scalable, secure solutions tailored to government requirements.



Figure 4. Erskine – Flagship UK Delivery Centre

Identity Services Expertise at Erskine includes:

- **Microsoft Entra** – Cloud identity and access management for secure digital services.
- **CyberArk** – Privileged Access Management to protect critical accounts and credentials.
- **SailPoint** – Identity governance for compliance and lifecycle management.
- **Thales** – Encryption and key management for data protection and trust assurance.

Physical and Operational Capabilities at Erskine:

- **Build Labs** – Secure environments for solution development and integration.
- **Visitors Centre** – Controlled access for client engagement and demonstrations.
- **544,000 ft² Campus** – Large-scale facility supporting complex government programmes.
- **Data Centre (170 racks)** – High-capacity infrastructure for hosting secure workloads.
- **Accreditations:** ISO 27001 & ISO 9001 – Certified for information security and quality management.
- **Modern Workplace Build Centre** – End-to-end deployment of secure digital workplace solutions.
- **24/7 Network Operations Centre (NOC) & Shared Service Desk** – Continuous monitoring and support for critical services.

2.3 CIAM for a Transport Ministry

Citizen identity and access management for 2.5 million citizens and 20k civil servants for access to 20 transport ministry applications. DXC designed and delivered a CIAM solution which integrated with the citizen electronic identity scheme and supported SAML and OpenID standards for application integration.

Business Challenge:

- Lacked authentication methods that integrated with the citizen e-ID scheme.
- Poor user experience and complex registration and authentication journeys.
- Need for enhanced security to meet external cyber threats.

How DXC helped:

- Provided an experienced security architect to design and lead the delivery.
- Enabled national e-ID scheme (SPID) as primary access mechanism.
- Strong authentication with smart card and mobile authenticator integration.
- Onboarded 2.5 million citizens, 20 K civil service identities and 20 Applications.

Business Outcomes:

- Consistent user experience across four IT environments and 20 applications.
- National e-ID supported for citizens, companies and professionals.
- SSO to multiple citizen transport services.
- Improved security posture with strong Passwordless and multi-factor authentication.

2.4 National digital identity for 4 million citizens

Protecting the privileged access for the high security critical infrastructure which provides the signing keys and digital identity certificates for 4 million people.

- Achieved GDPR, ETSI, and eIDAS compliance, ensuring secure and trusted digital identity services for 6,500+ government and commercial services.
- Improved operational efficiency with automated privileged account lifecycle, credential rotation, and streamlined workflows.
- Enhanced security posture by eliminating privileged threats and providing full visibility of risks to management.

2.5 City police digital transformation

DXC secured a 9-year contract to modernize the UK's largest police force:

- Implemented cloud-based ERP and AI-driven workforce planning.
- Delivered real-time resource allocation, reducing administrative overhead and improving frontline policing.
- Expected multi-million-pound savings through streamlined operations.

2.6 UK Defence – Zero Trust and secure communications

DXC deployed Zero Trust architecture and quantum-safe encryption for UK defence clients:

- Introduced Hermes private 5G platform for secure battlefield communications.
- Enabled continuous identity verification in contested environments.

- Supported coalition interoperability and mission readiness at scale.
- Did you know?
- DXC applied machine learning to vastly improve a cumbersome manual process of transformer station installations for an electricity supplier.
- DXC deployed an innovative security strategy and solution for a national institute for insurance against accidents at work to strengthen resiliency to malware attacks.
- DXC simplified IT infrastructure and increased automation to help a railway engine and carriage maker achieve a 62% reduction in critical IT incidents.
- DXC implemented a vision for smart factories using a next-generation digital manufacturing execution system and the digital thread framework for an international aeronautics company.

2.7 Did you know?

- DXC applied machine learning to vastly improve a cumbersome manual process of transformer station installations for an electricity supplier.
- DXC deployed an innovative security strategy and solution for a national institute for insurance against accidents at work to strengthen resiliency to malware attacks.
- DXC simplified IT infrastructure and increased automation to help a railway engine and carriage maker achieve a 62% reduction in critical IT incidents.
- DXC implemented a vision for smart factories using a next-generation digital manufacturing execution system and the digital thread framework for an international aeronautics company.

3 DXC Delivery Approach

3.1 DXC IAM Capability Model

DXC's Identity and Access Management (IAM) capability model delivers a robust framework designed to secure digital identities and uphold zero-trust principles across hybrid and multi-cloud environments for UK public sector organizations. Our approach ensures secure and accountable connectivity between people, devices, applications, and critical data systems, granting access only to authorized entities.

By integrating advanced Identity Governance and Administration (IGA), Access Management (PAM), and Adaptive Authentication, DXC enables public sector bodies to minimize risk, achieve stringent regulatory compliance, and provide seamless user experiences. This model supports:

- Centralized policy enforcement for consistent security controls.
- Federated identity management to enable secure collaboration across agencies.
- Scalable solutions capable of managing millions of identities across on-premises and cloud environments.

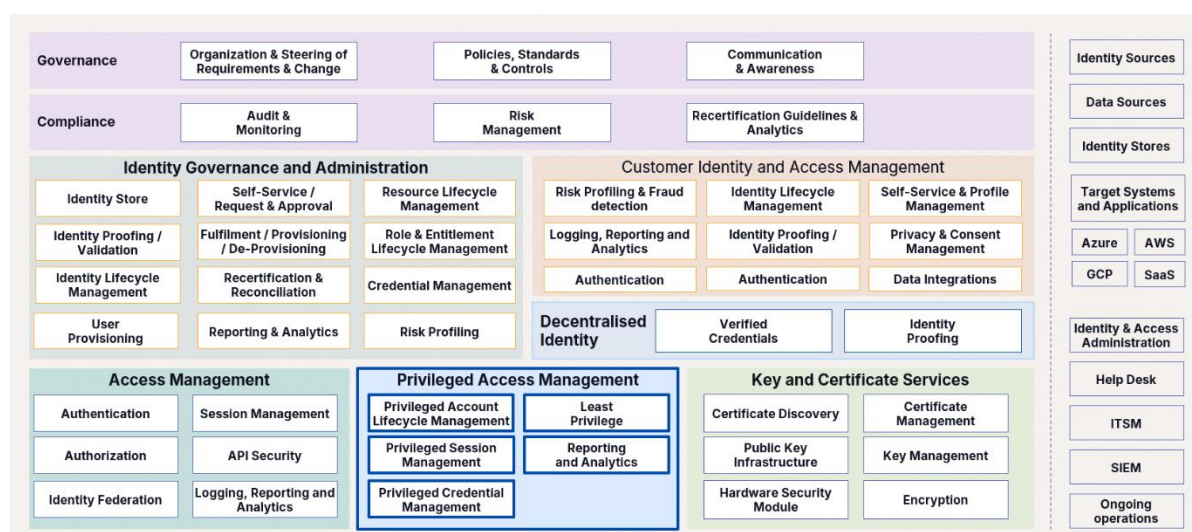


Figure 5. DXC IAM Capability Model

Beyond technology, DXC's IAM services deliver strategic value through a maturity-assessed roadmap that aligns identity capabilities with your technology and service objectives. We assess current-state identity processes, define a future-state architecture, and implement best practices using our extensive library of security blueprints. Our zero-trust adoption accelerators and identity fabric approach ensure resilience against evolving threats while enabling digital transformation. With deep expertise in Microsoft Entra, SailPoint, CyberArk, Ping Identity, BeyondTrust, Azure, AWS, GCP, Oracle, ServiceNow, and leading IAM platforms, DXC provides end-to-end advisory, implementation, and managed services to help clients modernize identity management and maintain compliance in complex, dynamic environments.

3.2 DXC IAM Delivery Methodology

DXC has defined a comprehensive approach for the definition and execution of IAM programmes based on decades of experience operating identity services for our customers.

This best-practice approach allows DXC to support customers at any maturity level during the whole IAM program from defining the IAM vision and strategy through design and implementation of the selected solution right up to fully managed IAM operational services.

DXC has defined blueprints and reusables from other projects which include:

- Framework for IAM governance,
- Framework for application onboarding,
- Automated build
- Deployment framework
- and others.

Identity is complex and a multi-year programme of work. DXC's experience of designing, implementing and then supporting, sometimes for decades, IAM solutions, directly informs our practical and pragmatic approach to successful service delivery. Our advisory is directly informed by our practical long-term delivery experience. DXC has been there with our customers running many generations of IT technology in our 50-year history while also deploying the latest technology and modernizing while squeezing value from the legacy assets.

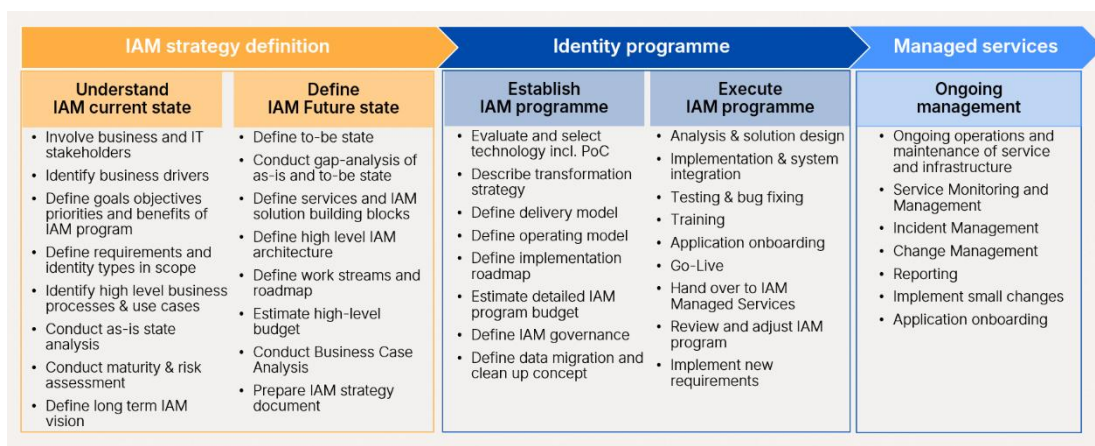


Figure 6. DXC End-to-end IAM Methodology

3.2.1 IAM strategy definition

Understand Identity and Access Management (IAM) current state:

1. Involve business and IT stakeholders
2. Identify business drivers
3. Define goals objectives priorities and benefits of IAM program
4. Define requirements and identity types in scope
5. Identify high level business processes & use cases
6. Conduct as-is state analysis
7. Conduct maturity & risk assessment
8. Define long term IAM vision

Define IAM Future state:

9. Define to-be state.
10. Conduct gap-analysis of as-is and to-be state.

11. Define services and IAM solution building blocks.
12. Define high level IAM architecture.
13. Define work streams and roadmap.
14. Estimate high-level budget.
15. Conduct Business Case Analysis.
16. Prepare IAM strategy document.

3.2.2 Identity programme

Establish IAM programme:

17. Evaluate and select technology incl. PoC
18. Describe transformation strategy
19. Define delivery model
20. Define operating model
21. Define implementation roadmap
22. Estimate detailed IAM program budget
23. Define IAM governance
24. Define data migration and clean up concept

Execute IAM programme:

25. Analysis & solution design
26. Implementation & system integration
27. Testing & bug fixing
28. Training
29. Application onboarding
30. Go-Live
31. Hand over to IAM Managed Services
32. Review and adjust IAM program
33. Implement new requirements

3.2.3 Managed operational services.

Ongoing management:

34. Ongoing operations and maintenance of service and infrastructure
35. Service Monitoring and Management
36. Incident Management
37. Change Management
38. Reporting
39. Implement small changes
40. Application onboarding

4 About DXC Technology

DXC Technology (NYSE: DXC) is a leading global provider of information technology services. We're a trusted operating partner to many of the world's most innovative organizations, building solutions that move industries and companies forward. Our engineering, consulting and technology experts help clients simplify, optimize and modernize their systems and processes, manage their most critical workloads, integrate AI-powered intelligence into their operations, and put security and trust at the forefront. Learn more on dxc.com.

Every day we deliver excellence for our customers and colleagues. We use the power of technology to deliver mission-critical IT services that move the world. Our customers entrust us to deliver what matters most. We are DXC.

An Employer of Choice

We inspire and take care of our people. We work to create a culture of learning, diversity and inclusion for all our people to grow and reach their full potential.

A Trusted Technology Partner

We understand technology and are committed to delivering excellence for our customers.

A Company that Cares.

We are committed to improving the communities in which we live and work. We are good stewards of our company, our customers and the world.

Deliver Mission Critical

We deliver the mission-critical IT services that move the world.

Entrusted to Deliver

Every day, we earn our customers' trust by delivering transformative technologies to ensure the success, safety and well-being of businesses and people worldwide.

Delivery Excellence

Our delivery excellence gives planes flight, helps patients heal, and increases the scale and speed of commerce.

Deliver What Matters Most

We are proud of the work we do and the trust and confidence our customers place in us to deliver what matters most.

Start planning now for crypto-agility and a post-quantum future.

Learn more at

dxc.com/digital-identity

dxc.com/key-and-certificate-services



Figure 7. DXC PAM protects public service providers and users.



DXC Technology
110 Pinehurst Road,
Farnborough Business Park,
Farnborough, Hampshire,
England, GU14 7BF

[DXC.com](https://www.dxc.com)

About DXC Technology

DXC Technology (NYSE: DXC) is a leading enterprise technology and innovation partner delivering software, services, and solutions to global enterprises and public sector organizations — helping them harness AI to drive outcomes at a time of exponential change with speed. With deep expertise in Managed Infrastructure Services, Application Modernization, and Industry-Specific Software Solutions, DXC modernizes, secures, and operates some of the world's most complex technology estates. Learn more on [dxc.com](https://www.dxc.com).

© 2025 DXC Technology Company. All rights reserved. Public