



Identity Governance and Administration

Service Description

DXC Technology



Table of Contents

1	DXC Identity Services for UK Public Sector.....	2
1.1	DXC Overview	2
1.2	Service Features.....	3
1.3	Service Benefits.....	4
1.4	Identity is the New Security Perimeter	4
1.5	User support and ticketing support.....	5
1.6	UK Public Sector Challenges	5
2	Case studies.....	7
2.1	DXC an Experienced Partner.....	7
2.2	Measurable results from IGA	7
2.3	Secure UK Government Delivery	8
2.4	UK Healthcare Provider	9
2.5	IGA Solution for Regulatory Compliance.....	9
2.6	National Digital Identity for 4 Million Citizens.....	10
2.7	City Police Digital Transformation	10
2.8	UK Defence Secure Communications	10
2.9	CIAM for a Transport Ministry	10
2.10	Did you know?	11
3	DXC Delivery Approach.....	12
3.1	DXC IAM Capability Model.....	12
3.2	DXC IAM Delivery Methodology.....	12
3.2.1	IAM strategy definition	13
3.2.2	Identity programme	14
3.2.3	Managed operational services.	14
4	About DXC Technology.....	15

List of Tables

Table 1.	Incident Priorities and Impacts.	5
----------	---------------------------------------	---

List of Figures

Figure 1.	DXC Identity Governance and Administration	3
Figure 2.	Identity is your security perimeter	5
Figure 3.	Erskine Site	8
Figure 4.	DXC IAM Capability Model	12
Figure 5.	DXC End-to-end IAM Methodology	13
Figure 6.	Identity enables public service providers and users.	16

1 DXC Identity Services 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.
- Decentralise 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.
- Enable access by citizens and customers to public services via digital and physical channels to enable service innovation, cost effective delivery while protecting privacy and ensuring security and 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.

DXC IGA services help UK public sector organizations to secure identities and meet compliance in complex hybrid and multi-cloud environments. We automate identity lifecycle management, enforce Zero Trust principles, and maintain continuous oversight of access for users, devices, applications and AI agents. This reduces unauthorized access risks, strengthens security posture, and accelerates digital transformation while ensuring compliance with UK regulations and standards such as GDPR and NHS Data Security Toolkit.

Helping UK government organizations modernize systems, strengthen security, and ensure compliance across hybrid and multi-cloud environments. DXC's digital identity services:

- Modernize legacy systems with scalable solutions for hybrid and multi-cloud environments.
- Provide expert advisory and managed services to streamline identity provisioning and access management.
- Automates policy enforcement and enables real-time auditing for compliance reporting.
- Leverages leading technologies: SailPoint, Microsoft Entra, Ping Identity, CyberArk, BeyondTrust, and Okta to deliver identity security.

With 450M+ identities managed, 3,200+ security experts, and UK-based SC/DV-cleared teams, DXC delivers secure, scalable identity services for mission-critical environments.

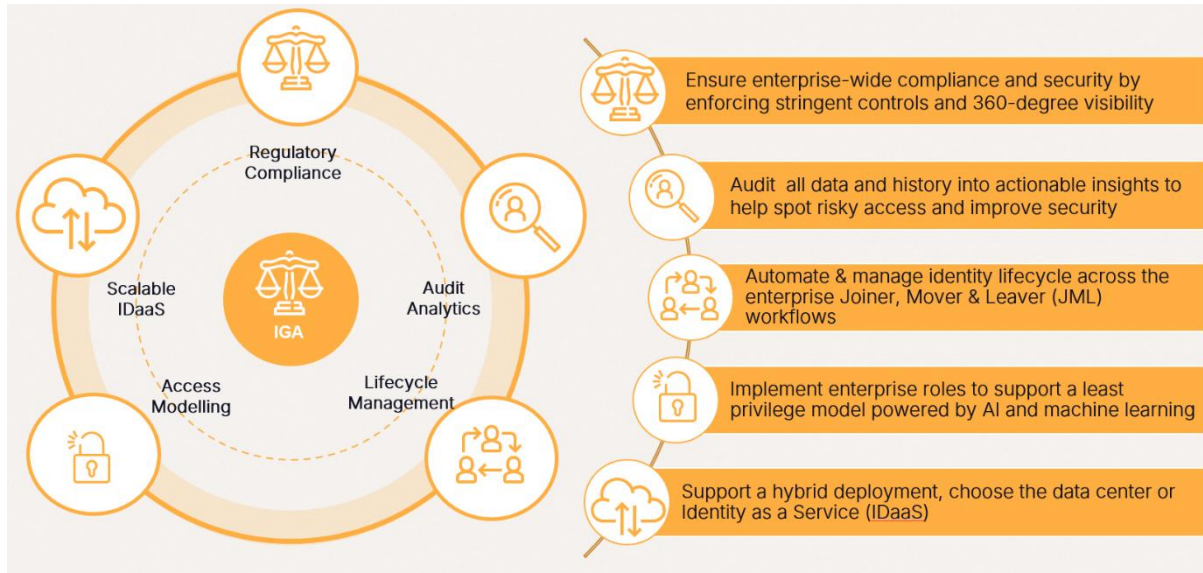


Figure 1. DXC Identity Governance and Administration

1.2 Service Features

- End-to-end consulting, design, implementation, and operational support.
- Securely manage citizen, supplier, government workforce, and machine identities such as RPA bots, scripts, applications, APIs, and AI agents.
- Automate user lifecycle for joiners, movers, and leavers (JML) so new starters in the HR system have their IT accounts created for their start date with minimum access for the job role assigned so they are productive from day one.
- Enable secure access and automatically enforce governance policies. Gathering lots of data is useless unless people can access it in a timely fashion and do so in line with regulations and operational best practices.
- Define and automate user friendly recertification approval workflows. Line managers need to be asked to certify access in business language they understand and not the technical language of IT systems and Microsoft Active Directory group names.
- Automatically detect entitlement conflicts and enforce separation of duties. Avoid users gradually snowballing access as they move between roles and enforce access in line with their current job role. Those outliers with exceptional access need to be detected and remediated.
- Discover and map patterns of entitlements for role mining. Actual patterns of entitlements usually reflect the needs of different job roles and teams, which when understood make it easier to manage through meaningful access roles.
- Credential management for passwords and multi factor authentication methods.
- Flexible delivery options of on-premises, SaaS, and hybrid. Resilience, data sovereignty, or simply making best use of existing IT assets can determine the best place to host your identity services.
- Realtime provisioning and de-provisioning of access rights. We all work in increasingly flexible ways across multiple teams and with people inside and outside our organizations so we need access that can flex to meet today's job role and the current project without compromise to regulations and access policies.

1.3 Service Benefits

- Reduce compliance risk by managing and monitoring all identities. Threat actors will target your weakest point, so we need to manage all identities from employees, contractors, agency staff, system accounts, RPA bots and emerging AI agents.
- Automation of provisioning reduces risks and boosts overall productivity. Delays of days or weeks for access for new starters or those moving between jobs or projects, those lost unproductive hours soon add up across large organisations and reduce the efficiencies of more flexible working.
- Ensure compliance with PCI DSS, GDPR, DORA, and NIS2. IGA automates enforces access policies and processes while also automating the creation of intelligent audit reports.
- Reduce audit expenses while improving reporting data quality. Manually tracking who has what access and how it was granted is simply impossible in modern complex hybrid IT estates.
- Meet digital sovereignty requirements with flexible local hosting options. Data sovereignty and the need for resilience requires data and systems are hosted in the right place.
- Enhance security posture using Zero Trust and least privilege principles. Taking a Zero Trust approach to security is recommended by the national Cyber Security Centre (NCSC) and is core to the methodology taken by DXC towards identity security.
- Govern access centrally for employees, partners, citizens, and machines. Identity has become the primary security control plane that determines who and what gets access to which data and IT services.
- Reduce insider threats and ransomware risk through identity controls. Ransomware attacks continue to be a business model that drive cyber criminals and state actors seeking to breach and disrupt critical national systems.
- Achieve a zero-trust approach to your identity security. DXC has placed Zero Trust as core to our internal approach to security with DXC and shapes the approach we take to our customers for the services we provide and the solutions we build for our customers.
- Self-service and automated credential management cuts helpdesk demand. People forget passwords when they go on holiday. Having automated methods for self-service reset of passwords or other credentials reduces wasted work time without rising compromise to the security of ID verification and onboarding process by help desk staff who only want to help and can be socially engineered to a manipulative caller. Simplifies audit reporting, improving compliance and governance visibility. Seeing quickly who has what access and highlighting the accounts with the greatest risk so that they can be targeted for remediation automatically reduces the effort in creating audit reports while helping to quickly move the dial on compliance by making your identity security visible to all stakeholders.

1.4 Identity is the New Security Perimeter

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.

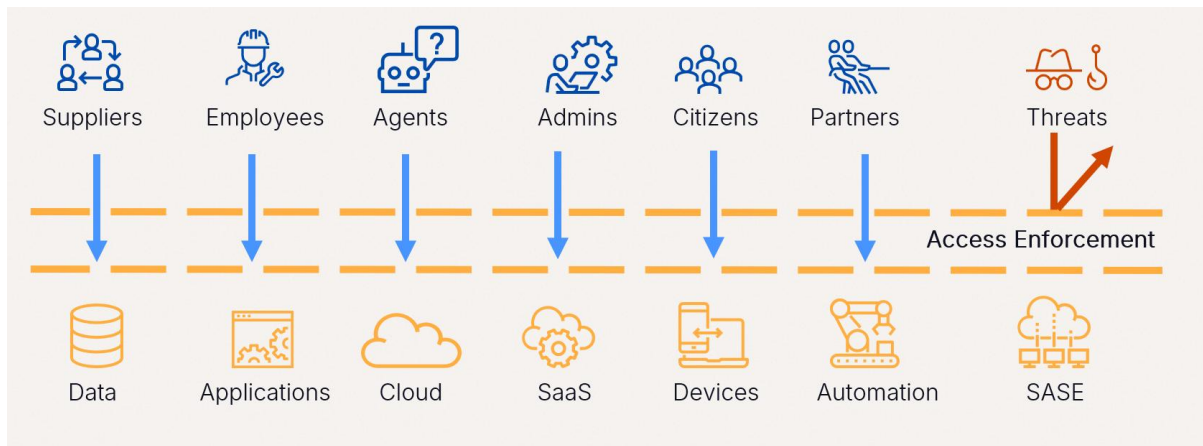


Figure 2. Identity is your security perimeter

1.5 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

1.6 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?

People want to work from anywhere and on any device. How to Single Sign-On (SSO) across applications and IT services via any device from anywhere?

Users expect smooth authentication via any channel. How to improve user experience while strengthening authentication assurance?

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.

2 Case studies

2.1 DXC an Experienced Partner

DXC is experienced in deploying large enterprise identity governance and administration solutions. Improving the experience for employees, partners, and suppliers. We also operate some large customer and citizen portals that allow people to interact securely through a digital channel with companies and government agencies.

Value DXC brings the UK public sector:

- **Compliance and Assurance:** Align with National Cyber Security Centre (NCSC) Zero Trust principles and NHS Care Identity standards.
- **Operational Efficiency:** Reduce onboarding time by up to 70% through automated JML (Joiner/Mover/Leaver) processes.
- **Risk Reduction:** PAM reduces privileged account compromise risk by 90%.
- **Scalability:** Support millions of identities across hybrid and multi-cloud environments.

DXC provides end to end services from expert identity security policy advisory, design, and implementation through to managed identity security services. DXC offers centralized management of digital identities and credentials to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's IGA services are powered by industry-leading technology companies such as Microsoft, Ping Identity, SailPoint, RedHat, CyberArk, Oracle, and Okta.

DXC has over 30 years of experience with modernizing identity governance and administration 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 Measurable results from IGA

DXC Identity Governance and Administration (IGA) services automate identity lifecycle management, enforce Zero Trust principles, and provide continuous oversight of access for users, devices, and applications. This approach reduces unauthorized access risks, accelerates digital transformation, and ensures compliance with regulatory standards across hybrid and multi-cloud environments.

Our IGA solutions drive measurable results:

- 20–30% efficiency gains with faster onboarding.

Avoid new staff waiting weeks for the access required to do their job and provide the required access, and only the required access, from day one.

- 20% faster IAM migration through automation.

Taking a factory approach and automating the onboarding on new applications and the migration of existing applications from your old tools into your modern IGA solution.

- 10x faster provisioning via self-service.

By shifting to user self-service, line manager approvals and automated approvals user satisfaction improves and time to access is reduced.

2.3 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 3. Erskine Site

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.

2.4 UK Healthcare Provider

Securing compliance through IGA automation. Enabling seamless access control and regulatory assurance:

- Compliance and Audit Closure – Resolved audit findings and strengthened regulatory compliance posture.
- Centralized SaaS IGA – Standardized processes with API integration and automated identity lifecycle management.
- Operational Efficiency – Improved user experience, reduced helpdesk workload, and eliminated process delays.
- Cost Optimization – Achieved savings by decommissioning legacy systems and streamlining identity management.

2.5 IGA Solution for Regulatory Compliance

End-to-end design, implementation, and operation ensuring regulatory compliance for a German bank.

- Unified identity visibility - Delivered a consolidated view of all identities and access rights across the organization.
- Regulatory Compliance - Ensured adherence to BAFIN, MaRisk, BAIT, and internal governance frameworks.
- Automated & Transparent Processes - Implemented traceable identity lifecycle management with simplified role-based access and accountability for non-personal accounts.

2.6 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.

2.7 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.

2.8 UK Defence 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.

2.9 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.

2.10 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), Privileged 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.

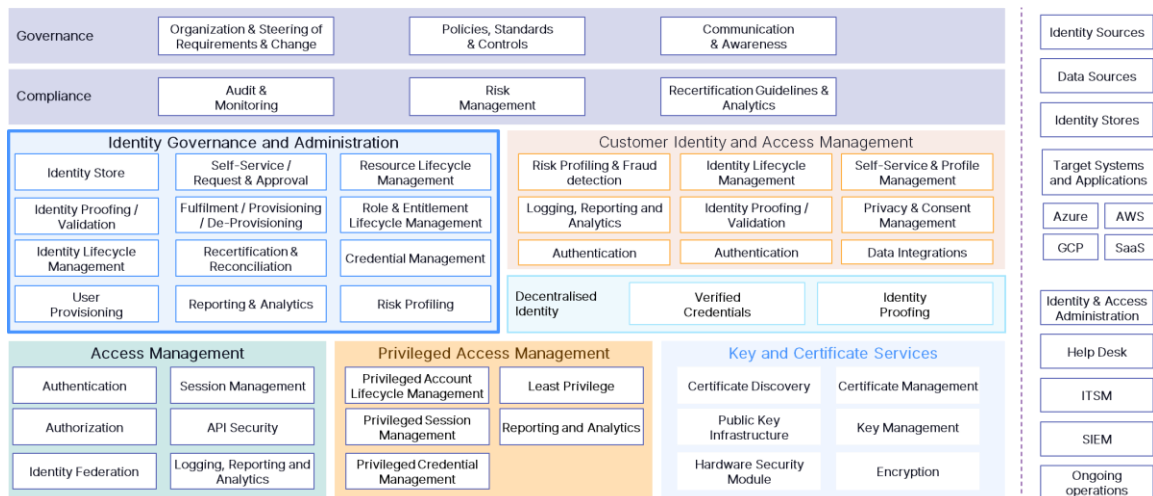


Figure 4. DXC IAM Capability Model

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 holistic 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.

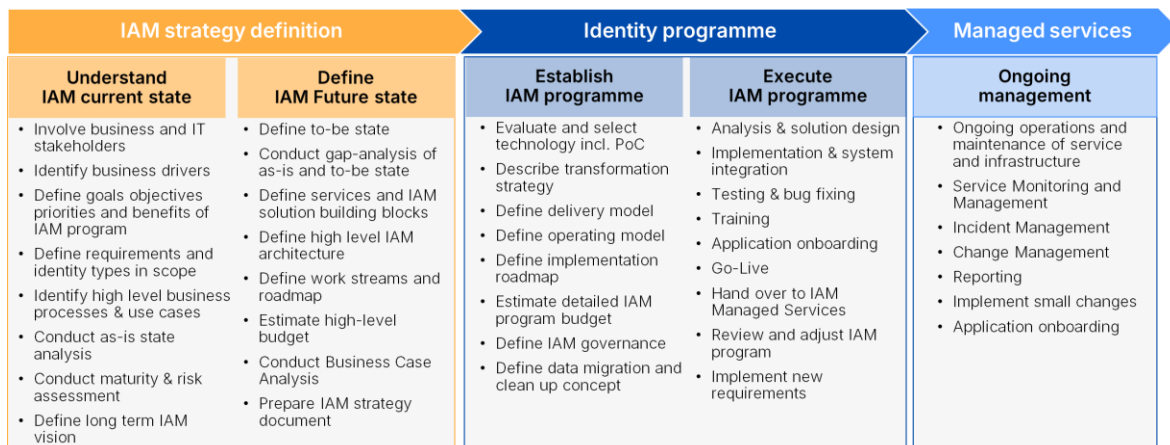


Figure 5. DXC End-to-end IAM Methodology

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 are 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.

Learn more at

<https://dxc.com/us/en/offerings/security/digital-identity>



Figure 6. Identity enables 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).

© 2026 DXC Technology Company. All rights reserved. DXC Public