



Identity Assessment Service Description

Measure Maturity and Define Improvement Roadmap



Table of Contents

1	DXC Identity Assessment for UK Public Sector	3
1.1	Identity Assessment Overview	3
1.2	DXC Overview	3
2	DXC Identity Assessment.....	4
2.1	Scope and Purpose	4
2.2	Identity Assessment packaged to fit your needs	5
2.2.1	Small Package (S)	5
2.2.2	Medium Package (M).....	5
2.2.3	Large Package (L)	5
2.2.4	DXC Identity Security Advisory Services.....	6
2.3	Project Goals and Deliverables	6
2.3.1	Work Package 1 - Preparation and Kick-Off.....	7
2.3.2	Work Package 2 – Interviews.....	8
2.3.3	Work Package 3 – Analysis	9
2.3.4	Work Package 4 – Strategy	9
2.4	Buyer responsibilities	11
3	DXC Delivery Approach.....	12
3.1	DXC IAM Capability Model.....	12
3.2	DXC IAM Delivery Methodology.....	13
3.2.1	IAM strategy definition	13
3.2.2	Identity programme	14
3.2.3	Managed operational services	14
4	Service Features and Benefits	16
4.1	Service Features.....	16
4.2	Service Benefits.....	16
5	Case studies.....	18
5.1	DXC an Experienced Partner.....	18
5.2	Secure UK Government Delivery	18
5.3	National digital identity for 4 million citizens	20
5.4	City police digital transformation	20
5.5	CIAM for a Transport Ministry	20
5.6	IAM strategy for a UK healthcare supply chain.....	21
5.7	IAM strategy for a UK based telecoms company.....	21
5.8	IAM strategy for a global leader in industrial software	22
5.9	IAM Strategy for a UK Transportation & Logistics Company	23
5.10	Did you know?	23
6	About DXC Technology.....	24

List of Tables

Table 1.	Preparation and kick off	7
Table 2.	Stakeholder Interviews.....	8
Table 3.	Analysis and Assessment	9
Table 4.	Identity Assessment strategy	9
Table 5.	Buyer's Responsibilities	11

List of Figures

Figure 1.	DXC Identity Assessment Key Aspect	4
Figure 2.	S/M/L Packages +Options	5
Figure 3.	DXC Identity Assessment Work Packages.....	6
Figure 4.	DXC IAM Capability Model	12
Figure 5.	DXC End-to-end IAM Methodology	13
Figure 6.	Erskine – Flagship UK Delivery Centre	19
Figure 7.	DXC Identity Assessment for Trusted Digital Public Services.	25

1 DXC Identity Assessment for UK Public Sector

1.1 Identity Assessment Overview

A fixed price advisory service, packaged as small, medium and large, covering your identity security, with the option to add on additional scope with additional consulting costs.

The identity assessment covers:

- **As-Is:** understand current identity assets, technical and business processes.
- **Goal state:** define a future identity technology fabric and process improvements.
- **Strategic roadmap:** transform efficiently with a prioritised plan for transformation.
- **Educate stakeholders:** on positive business impact from modern identity security.
- **Scaled:** Small/Medium/Large for accelerated off the shelf delivery.

1.2 DXC Overview

DXC Technology delivers comprehensive identity security services that help UK public sector organizations secure access, establish trust, and ensure compliance with GDPR, NHS Digital standards, and MoD security frameworks.

Public sector environments are complex, spanning hybrid and multi-cloud infrastructures, with geographically dispersed staff and citizens accessing services remotely and in person, with an increasing number of connected devices, IoT endpoints, RPA bots, and AI agents.

DXC Technology provides a full range of Identity and Access Management (IAM) services that include:

- 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 and Multi-Factor Authentication (MFA) adaptive authentication for frictionless user experiences, making secure access management easy to use.
- 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.

2 DXC Identity Assessment

2.1 Scope and Purpose

Our assessment identifies gaps in identity governance, authentication, and access controls, then defines a future-ready roadmap aligned with zero-trust principles. By consolidating and streamlining identity processes, adopting scalable identity platforms, we enable automation, improve operational efficiency, and prepare for emerging challenges such as quantum readiness and autonomous AI agents. DXC empowers the public sector to strengthen security, reduce compliance risk, and accelerate digital transformation with confidence.

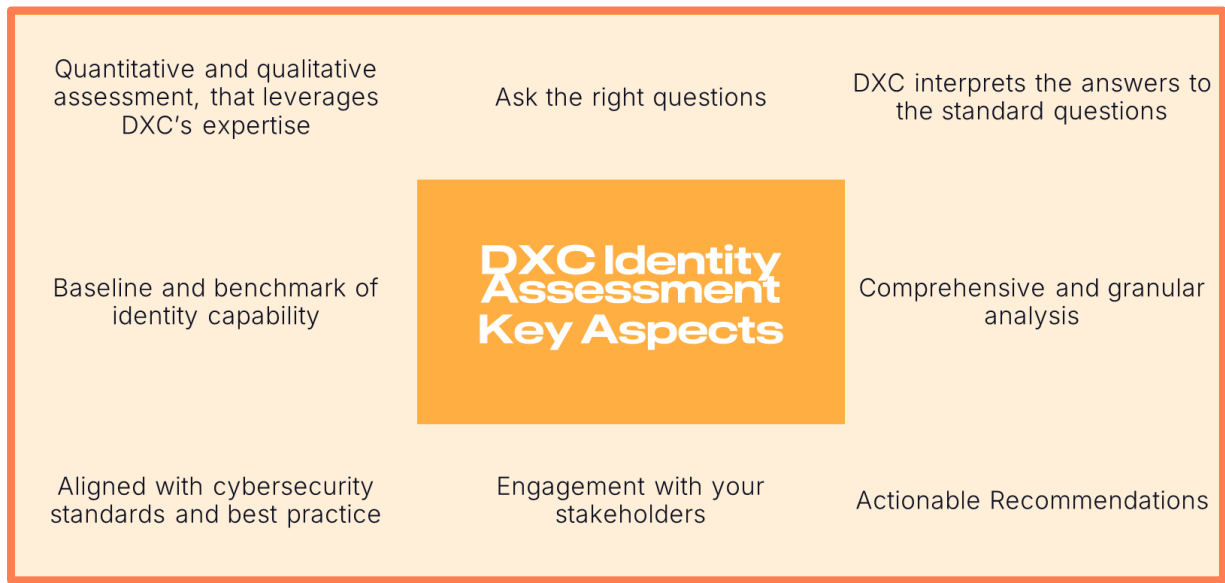


Figure 1. DXC Identity Assessment Key Aspect

Our Identity Assessment evaluates critical components of your identity ecosystem to ensure security, compliance, and efficiency:

- **Regulatory Compliance.** Ensuring adherence to industry standards and regulations.
- **Cost Reduction.** Streamlining identity management processes to reduce operational costs from wasteful processes and minimize unnecessary licenses.
- **Improve productivity.** Provide employees with the access they require from day one and speedy but compliant changes to their access as and when required.
- **Cybersecurity.** Enhancing security measures to protect against cyber threats.
- **User Authentication.** Improving user authentication experiences for improved accessibility without compromise to security.
- **Business Growth and Transformation.** Supporting business expansion and transformation initiatives.
- **Zero-Trust Security.** Identity security that is fit for now and the future.

DXC Identity Assessment empowers UK public sector organizations to strengthen identity security, achieve regulatory compliance, and accelerate adoption of Zero Trust principles. This service provides a comprehensive evaluation of your current identity environment, including governance, authentication, and access controls, to identify gaps and risks. Based on this analysis, we define a future-ready architecture and deliver a clear, actionable roadmap that supports compliance, operational efficiency, and digital transformation goals.

Designed for scalability and predictability, Identity Assessment is offered at a fixed price and aligned with UK government frameworks such as GDPR, NHS Digital standards, and MoD

security requirements. It addresses the complexity of hybrid and multi-cloud environments, remote workforces, and growing IoT and AI-driven ecosystems. Leveraging DXC's deep expertise and trusted technology partnerships, the service ensures secure identity management while reducing compliance overhead and improving resilience.

By preparing organizations for emerging challenges like quantum readiness and enabling automation across identity processes, Identity Assessment helps the public sector deliver secure, citizen-centric services with confidence. The result is a flexible, future-proof identity strategy that enhances trust, reduces risk, and accelerates the growth of digital channels.

2.2 Identity Assessment packaged to fit your needs

Our Digital Identity Assessment packages provide structured, actionable insights to strengthen identity governance and security posture across government departments. The packed advisory services come in degaukt sizes to fiut your needs with the freedom to extned the scope of any of the three standard packages.

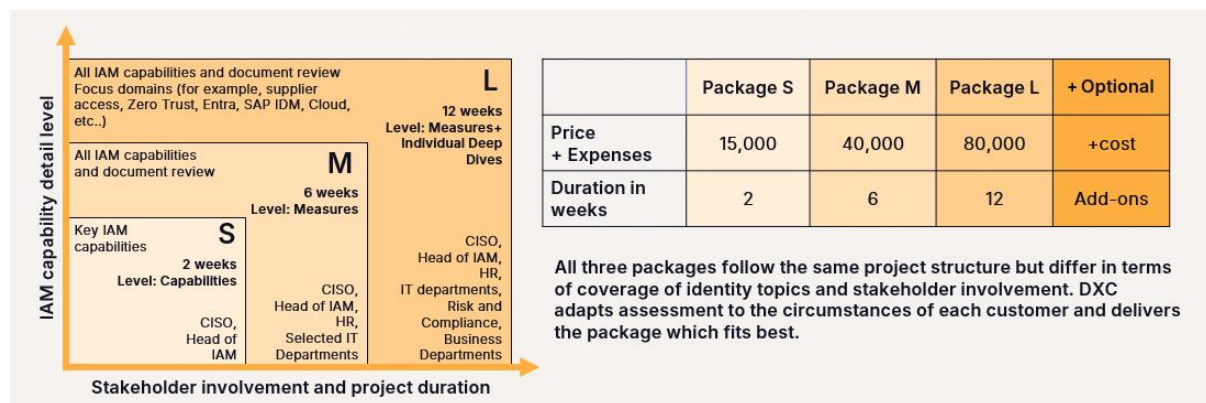


Figure 2. S/M/L Packages +Options

2.2.1 Small Package (S)

Ideal for organizations seeking a quick, focused evaluation, small package delivers key identity capability assessments within 2 weeks. It includes 4 structured interviews with stakeholders such as the CISO and Head of Identity and Access Management, resulting in a 10-page strategy document or slide deck. Priced at £15,000, it offers a cost-effective way to identify gaps, align with compliance requirements, and support digital transformation initiatives.

2.2.2 Medium Package (M)

Designed for broader coverage, the medium package provides a comprehensive review of all identity assessment capabilities and document analysis. It focuses on critical domains such as supplier access, Zero Trust, Entra, SAP IDM, and cloud environments. Over 6 weeks, we conduct 10 interviews with stakeholders including the CISO, Head of IAM, HR, and selected IT departments. The outcome is a 15-page strategy document with actionable recommendations. Priced at £40,000, this package delivers deeper insights to strengthen security posture and accelerate modernization.

2.2.3 Large Package (L)

For organizations requiring an in-depth, enterprise-wide assessment, the **Large Package** offers the most extensive engagement. Covering all identity capabilities and document reviews, it includes a strong focus on Zero Trust, supplier access, Entra, SAP IDM, and cloud identity management. Spanning 12 weeks and involving 20 interviews, this package combines maturity measures with individual deep-dive analysis. The result is a 30-page

strategy document outlining a detailed roadmap for identity governance and security enhancements. Priced at £80,000, it ensures a robust identity strategy aligned with organizational goals and regulatory requirements.

2.2.4 DXC Identity Security Advisory Services

DXC provides a broad range of cybersecurity advisory and consulting services beyond just identity and access management. We can drill deep into specific business process topics or product technology challenges adapting and extending one of the three standard advisory service packages to meet the Buyers particular requirements.

- **Identity Risk Assessment:** Identify exposure points in identity and access flows.
- **Strategy and Roadmap:** Define an access management strategy aligned with regulatory compliance and business goals.
- **Tool Selection:** Recommend access management tools and identity security platforms.
- **Regulatory Compliance:** Alignment with DORA, UK Digital Trust Framework, eIDAS 2.0, GDPR, and NIS2.

2.3 Project Goals and Deliverables

In line with the scope requested by the Buyer, DXC provides the following deliverables aligned with the goals for each Work Package (WP):

Preparation & Kick-Off	Interviews	Analysis	Strategy
Key Goals - Understand business drivers - Review/define identity vision - Review current strategy - Determine target goals - Identify stakeholders - Schedule interviews - Agree project plan			
Deliverables - Kick-off Presentation - Assessment plan			
Key Goals - Configure questions by topics and stakeholder roles - Understand as-is situation by reading documents and analysing current issues - Perform interviews and score each question accordingly - Review insights with sponsor			
Deliverables - Focused questions - Interviews and workshops			
Key Goals - Understand As-Is-State - Define future identity design - List gaps for each capability - Review reference documents - Draft assessment report - Draft executive presentation - Review drafts with sponsor			
Deliverables - Identity assessment report - Future architecture vision			
Key Goals - Alert on urgent risks - Document as-is and gaps - Visualize target architecture - Perform cost benefit analysis - Plan improvement roadmap - Review with project sponsor - Executive presentation			
Deliverables - Executive presentation - Strategy roadmap			

Figure 3. DXC Identity Assessment Work Packages

WP1 Deliverables:

- Kick-off presentation
- Assessment plan

WP2 Deliverables:

- Focused interview questions
- Interviews and workshops with stakeholders

WP3 Deliverables:

- Identity assessment document
- Future architecture vision

WP4 Deliverables:

- Executive presentation
- Strategy roadmap

The approach is a clear and structured process for managing an identity assessment, ensuring that each phase is thoroughly planned, executed, with clear goals and have outcome-based deliverables.

2.3.1 Work Package 1 - Preparation and Kick-Off

To ensure the success of our identity assessment project, we will begin by understanding the business drivers and reviewing or defining the identity vision. This will involve a thorough review of the current strategy and the determination of target goals. Identifying key stakeholders is crucial, and we will schedule interviews with them to gather their insights and requirements. Finally, we will agree on a comprehensive project plan to guide the execution of the project.

Table 1. Preparation and kick off

WP1	Preparation & Kick-Off
Description	This Work Package describes all activities needed to plan and prepare the project.
Input	Project scope document Documentation of existing Identity Assessment processes and infrastructure Additional input from various stakeholders
Activities	Workshop Planning • Prepare and plan project • Identify relevant stakeholders • Define kick-off date and workshop schedule • Define the project goals • Understand business drivers and Identity Assessment vision • Introduce the methodology • Introduce the approach to Identity Assessment strategy Create list of available customer documents related to Identity Assessment Gather and review customer documents
Deliverables	Conduct Kick-off workshop Create Kick-off presentation and assessment plan • Project Goal • Project plan • Stakeholder list • Interview schedule List of existing Identity Assessment documentation
Assumptions	Average duration of workshops is approximately 2 (S), 6 (M) or 12 (L) weeks Identity Assessment business drivers are clear, Identity Assessment vision is defined General assumptions as listed in chapter 3.6 apply
Buyer Obligations	Provide input to project goals and business drivers Provide input to Identity Assessment vision Describe current Identity Assessment strategy Identify stakeholders Schedule interviews Provide necessary information and relevant existing Identity Assessment documentation Customer obligations as listed in chapter 3.6 apply
Acceptance Criteria	Workshop conducted Documents delivered (Project goal definition, Project plan, Stakeholder list, Interview schedule, List of existing Identity Assessment documentation). Deliverables will be provided as PowerPoint templates, Excel lists, etc. as appropriate.

Limitations (Small)	Scope of Key identity assessment capabilities. Engaged stakeholders to include CISO, Head of Identity Assessment, Business application owner, Identity Assessment support and help desk.
Limitations (Medium)	Scope of all Identity Assessment capabilities and Identity Assessment architecture document review. Engaged stakeholders to include CISO, Head of IAM, HR, Selected IT Departments
Limitations (Large)	Scope of all Identity Assessment capabilities and document review. 4 focus domains (for example, supplier access, Zero Trust, Entra, SAP IDM, Cloud, etc.) Engaged stakeholders to include CISO, Head of IAM, HR, Selected IT Departments

2.3.2 Work Package 2 – Interviews

To conduct a thorough identity assessment, we will begin by configuring questions tailored to specific topics and stakeholder roles. This will help us gather relevant and focused information. We will then understand the current (as-is) situation by reviewing existing documents and analysing current issues. Following this, we will perform interviews with key stakeholders, scoring each question accordingly to quantify the insights gathered.

Finally, we will review these insights with the project sponsor to ensure alignment and validate our findings. This structured approach will provide a comprehensive understanding of the current identity system and inform future improvements.

Table 2. Stakeholder Interviews

WP2	Stakeholder interviews
Description	This Work Package describes all activities needed to organize and conduct interviews to gather necessary information from various stakeholders.
Input	Stakeholder list Interview schedule All documents and information collected during project planning and preparation
Activities	Prepare interview questions Conduct interviews with selected stakeholders or stakeholder groups via Teams (1 – 3 h each) - Document stakeholder's view of the current state and expectations for the future state - Document challenges and suggestions for improvements - Schedule follow-up calls to clarify remaining open topics (if needed) Complete Future State definition
Deliverables	Interview questions Conduct Interviews Documented stakeholder responses Documented current state, expectations, challenges and suggestions for improvements Follow-up calls (if needed)
Assumptions	Interviews can be conducted via Teams (<i>on-site interviews incur additional cost</i>) Several interviews per day can be conducted on consecutive days The interviewed stakeholder can answer the questions General assumptions as listed in chapter 3.6 apply
Buyer Obligations	Facilitate interviews Ensure availability of stakeholders Customer obligations as listed in chapter 3.6_apply

Acceptance Criteria	Interviews conducted Interview results documented
Limitations (Small)	Up to 4 interviews (1-2 hours each) will be conducted via Teams Up to 1 follow-up calls (up to 1h) to clarify open topics will be conducted (if necessary)
Limitations (Medium)	Up to 10 interviews (1-2 hours each) will be conducted via Teams Up to 2 follow-up calls (up to 1h) to clarify open topics will be conducted (as required)
Limitations (Large)	Up to 20 interviews (1-2 hours each) will be conducted via Teams (Ref Chart- S/M/L) Up to 5 follow-up calls (up to 1h) to clarify open topics will be conducted (if necessary)

2.3.3 Work Package 3 – Analysis

To conduct a thorough identity assessment, we will first understand the current state by reviewing interview results and document findings. Next, we will define the future identity design and list gaps for each capability area. We will draft an assessment report and an executive presentation and review these drafts with the project sponsor to ensure alignment and validate our findings.

Table 3. Analysis and Assessment

WP3	Analysis and Assessment
Description	This Work Package describes all activities needed to review and assess interview results
Input	Interview results
Activities	Review interview results and document findings Comment and assess responses Describe Identity Assessment current state (identify gaps, document findings, list examples)
Deliverables	Identity Assessment current state Identity Assessment future state
Assumptions	All activities can be performed remotely General assumptions as listed in chapter 3.6 apply
Buyer Obligations	Actively participate in all activities as contributor and reviewer Customer obligations as listed in chapter 3.6 apply
Acceptance Criteria	Review and assessment of interview results completed Identity Assessment current state Identity Assessment future state

2.3.4 Work Package 4 – Strategy

To ensure a comprehensive identity assessment, we will start by highlighting any urgent risks and documenting the current (as-is) state and gaps. We will then visualize the target architecture and perform a cost-benefit analysis to evaluate potential improvements. Based on these insights, we will plan an improvement roadmap and review our findings and plans with the project sponsor. Finally, we will present our conclusions and recommendations in an executive presentation to ensure alignment and approval.

Table 4. Identity Assessment strategy

WP4	Identity Assessment strategy
------------	-------------------------------------

Description	This Work Package describes all activities needed to complete the definition of a holistic Identity Assessment strategy
Input	Interview results Identity Assessment current state Identity Assessment future state Additional input from various stakeholders
Activities	Define Identity Assessment future state Conduct gap analysis Identify recommendations based on gap analysis Rate recommendations in terms of effort and business benefits Identify quick wins Create Identity Assessment strategy document • Identity Assessment future capability model • Identity Assessment governance model • Identity Assessment service model (user and technical support) • Define services and Identity Assessment solution building blocks • Describe high-level Identity Assessment architecture • Define high-level Identity Assessment work streams • Define high-level Identity Assessment implementation roadmap • High-level estimation of implementation resourcing and potential cost • Impact assessment for business change • Validate design proposals with key stakeholders • Creation of Business Case Recommendations Validate design proposals with key stakeholders Prepare executive presentation Review final presentation Conduct final presentation workshop (approx. 4h)
Deliverables	Identity Assessment strategy document Executive presentation Presentation of results in a final presentation workshop (one day, remote)
Assumptions	General assumptions as listed in chapter 3.6 apply
Buyer Obligations	Facilitate presentation workshop Actively participate in all activities as contributor and reviewer Customer obligations as listed in chapter 3.6 apply
Acceptance Criteria	Presentation workshop conducted Identity Assessment strategy document finalized
Limitations (Small)	Identity Assessment strategy document with approx. 10 pages/slides
Limitations (Medium)	Identity Assessment strategy document with approx. 15 pages/slides
Limitations (Large)	Identity Assessment strategy document with approx. 30 pages/slides

2.4 Buyer responsibilities

The project requires active engagement from a project sponsor and involvement of customer staff with the relevant knowledge and experience at the interviews or workshops.

Table 5. Buyer's Responsibilities

Ref#	Buyer's Responsibilities
C01	Buyer will have named at least one executive sponsor as the designated consumer of the executive presentation.
C02	Buyer appoints a contact person for the DXC delivery team who is responsible for planning resources and time of customer staff.
C03	Buyer appoints a person responsible for project managing to book resources, schedule interview dates, review meetings, timely feedback on draft documents and booking meetings for executive presentations.
C04	Buyer contact person ensures that the Buyer staff involved in the project or people affected and interested are informed appropriately.
C05	Buyer employees have the necessary knowledge and enough time to contribute to the project both at the interviews and to answer follow-up questions by phone or email.
C06	Buyer provides DXC employees with an appropriate work environment including internet connections, if needed when working at the Buyer's location.
C07	The project is managed according to DXC's project management and solution-specific methodologies.

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.

ACCELERATE DELIVERY AND REDUCE RISK WITH DXC IAM CAPABILITY MODEL

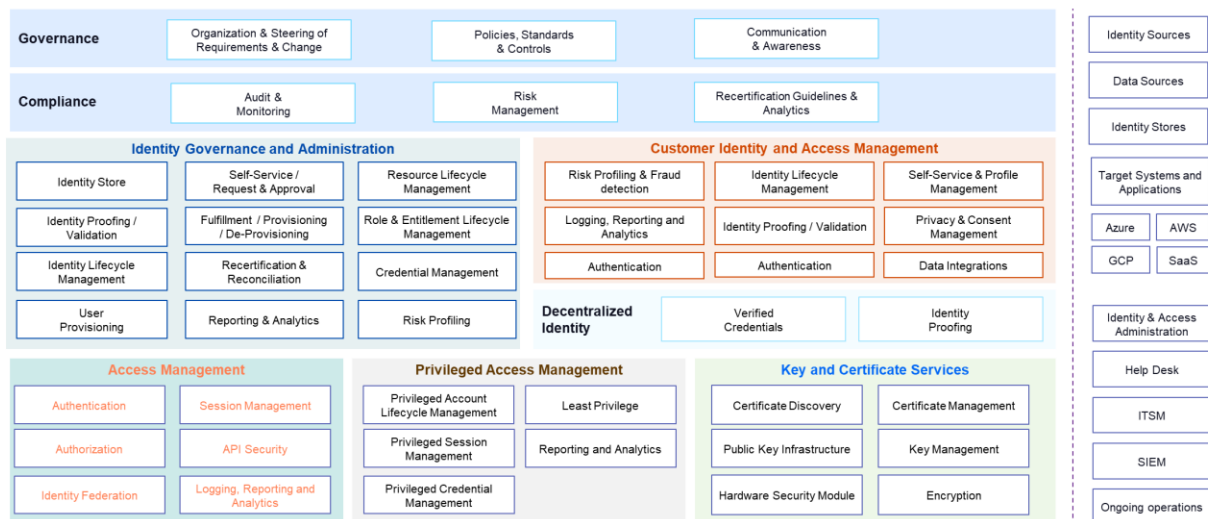


Figure 4. DXC IAM Capability Model

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.

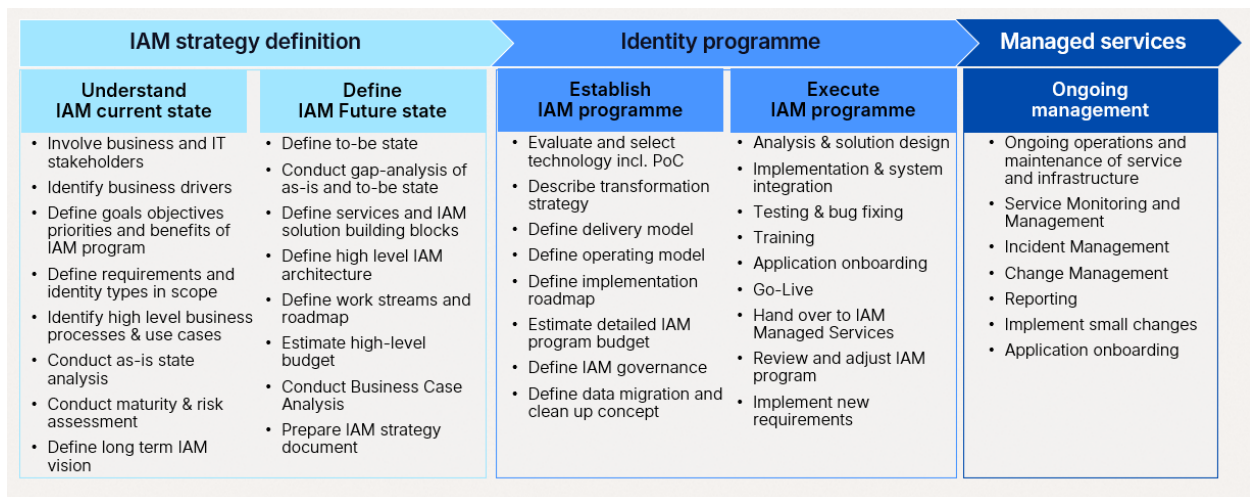


Figure 5. DXC End-to-end IAM Methodology

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 minor changes
- 40. Application onboarding

4 Service Features and Benefits

4.1 Service Features

DXC Identity Assessment for the UK Public Sector addresses your critical identity security priorities, regulatory compliance, cost reduction, improved security posture, quantum readiness, growth in machine identities, and flexible service delivery while accelerating digital channel growth and enabling a Zero Trust security approach.

Our assessment evaluates identity governance, authentication, and cryptographic practices to ensure trusted digital interactions and transactions. It delivers a clear roadmap for secure, compliant, and future-ready identity management empowering UK public sector organizations to build trust and resilience. The scope of the assessment includes:

- **Comprehensive identity system review**
Performs a full evaluation of identity systems across all environments, identifying security gaps, compliance risks, and operational inefficiencies.
- **Platform mapping for architectural clarity**
Maps legacy and modern identity platforms to provide clear architectural insights, highlighting integration challenges and modernization opportunities.
- **Future-State architecture design**
Designs a secure, scalable identity architecture aligned with UK security standards, ensuring compliance and resilience against evolving threats.
- **Regulatory compliance documentation**
Thoroughly documents GDPR, NCSC, and other compliance requirements, ensuring identity processes meet legal and regulatory obligations consistently.
- **Zero trust integration**
Assesses governance frameworks and integrates Zero Trust principles into identity and access management for enhanced security posture.
- **Identity lifecycle automation**
Evaluates and implements automation for provisioning and de-provisioning processes, reducing manual effort and improving operational efficiency.
- **Multi-Factor authentication configuration**
Validates and configures MFA and adaptive access controls across platforms, ensuring strong authentication and user-friendly security measures.
- **Actionable roadmap development**
Generates a prioritized roadmap based on assessment findings, focusing on identity security improvements and operational optimization.
- **Scalable assessment packages**
Offers flexible assessment packages tailored to organizations of varying sizes, ensuring cost-effective and comprehensive identity evaluations.
- **Vendor partnership utilization**
Leverages DXC's partnerships with leading identity technology vendors to deliver advanced solutions and best-in-class implementation support.

4.2 Service Benefits

Identity assessment is essential for the UK public sector to safeguard citizen data, ensure compliance, and enable secure, efficient digital services driving trust, reducing risk, and accelerating transformation. The benefits include:

- **Accelerates public service transformation**
A flexible, scalable identity platform enables government departments to modernize services quickly, integrate emerging technologies, and deliver citizen-centric digital experiences, supporting efficiency and long-term transformation goals.
- **Ensures regulatory and legislative compliance**

Automated compliance processes help public bodies maintain adherence to UK data protection laws, GDPR, and sector-specific regulations, reducing manual effort and ensuring audit readiness across all agencies.

- **Improves operational efficiency**
Automated user provisioning streamlines onboarding for civil servants and contractors, reducing administrative overhead and freeing resources to focus on delivering high-quality public services rather than manual identity management.
- **Drives innovation in citizen services**
Secure identity solutions enable new digital channels and services, fostering innovation and improving accessibility for citizens, while expanding engagement opportunities across diverse communities and demographics.
- **Enhances citizen and staff Experience**
Optimized authentication journeys reduce friction for citizens accessing online services and staff using internal systems, minimizing frustration and improving satisfaction with government digital platforms.
- **Achieves Zero Trust security**
Implementing least privilege and just-in-time access strengthens security across government networks, ensuring sensitive citizen data and critical infrastructure remain protected from evolving cyber threats.
- **Speeds up inter agency collaboration**
Unified single sign-on simplifies identity integration across departments and agencies, accelerating collaboration and reducing complexity during joint initiatives or structural changes within the public sector.
- **Strengthens security posture**
Comprehensive identity governance minimizes risks associated with unauthorized access, enforces security policies consistently, and ensures resilience against cyberattacks targeting public sector systems and citizen data.
- **Supports digital transformation initiatives**
Robust identity automation and governance underpin large-scale modernization programs, enabling secure access and compliance while driving efficiency and innovation across government services.
- **Aligns identity strategy with public sector goals**
A well-defined identity strategy supports policy objectives, operational resilience, and long-term sustainability, ensuring technology investments align with the mission to deliver secure, efficient, and inclusive public services.

5 Case studies

5.1 DXC an Experienced Partner

DXC provides end to end services from expert certificate policy advisory, design, and implementation through to managed Identity Assessment. DXC offers centralized management of digital identities, encryption keys, and certificates to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Key & Certificate Services is powered by industry-leading technologies from Microsoft, Thales, and DigiCert.

DXC is helping our clients shift workloads to hybrid and multi-cloud environments while keeping data secure and compliant, using suitable encryption and private key services that lets workloads and data reside on the cloud without being accessible to the cloud service provider. DXC is experienced in deploying large mission critical systems that span hybrid cloud environments and existing data centres.

DXC has over 30 years of experience with modernizing cryptography solutions, as well as established relationships with strategic suppliers of quantum-ready technology, including AWS, CyberArk, DigiCert, Google, Microsoft and Thales.

- **Trusted relationships.** We're committed to delivering mission critical cryptographic services for customers in banking, government, healthcare, energy and manufacturing.
- **Administrative expertise.** We help you consolidate management of your cryptographic keys and certificates, ensuring crypto agility for quantum safe encryption and addressing the challenges of reduced certificate validity periods in the coming years.

5.2 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 6. 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.

5.3 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.

5.4 City police digital transformation

DXC secured a 9-year contract to modernize IT services for 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.

5.5 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 Password less and multi-factor authentication.

5.6 IAM strategy for a UK healthcare supply chain

The organization faced identity management challenges in a heavily outsourced IT environment with limited access control and fragmented IAM process. DXC delivered a comprehensive identity assessment and roadmap aligned with organizational security objectives. DXC defined in partnership with key stakeholders the global IAM policies and target architecture to strengthen identity lifecycle and privileged access controls. DXC used structured methodology, the DXC IAM capability model and reusable components to fast-track IAM maturity improvements and reduce complexity.

Business Challenge:

- Heavily outsourced IT environment with little control of access by the customer
- Capability mismatch between service providers and customer's need for controls
- High number of identities (> 100.000) without proper identity lifecycle processes in place

How DXC Helped:

- Skilled DXC resources evaluated current state identity services.
- Close collaboration with the customer and its suppliers.
- Conducted IAM maturity assessment and gap analysis.
- Developed a comprehensive IAM strategy based on DXC IAM Capability Model.
- Defined IAM improvement roadmap.
- Defined IAM target architecture.

Business Outcomes:

- DXC's structured methodology and reusables greatly accelerated the assessment process.
- Actionable IAM strategy in alignment with overall security strategy and upcoming projects.
- Clear way forward along the defined IAM improvement roadmap.

5.7 IAM strategy for a UK based telecoms company

DXC applied our holistic IAM methodology to assess the current IAM maturity, define a desired IAM future state and document a detailed IAM implementation roadmap to guide transformation. *"The collaboration and knowledge sharing, and expert guidance has meant we have delivered an almost impossible task on time."* – Customer

Business Challenge:

- Digital identity capabilities and processes inconsistently implemented across the organization
- No clarity over identity governance, roles, and responsibilities for the organization
- Decentralized and manual access management for ~100.000 users
- Insufficient control of privileged access management
- High cost of administrative overhead

How DXC Helped:

- Developed a comprehensive digital identity strategy, based on DXC IAM Capability Model.
- Embedded DXC subject matter experts in agile team to collaborate closely with customer.
- Documented identity current state, future state blueprint, and gap analysis.
- Defined a high-level digital identity roadmap.

Business Outcomes:

- Enabled actionable, comprehensive, and holistic identity strategy
- Increased awareness of current IAM posture and required improvements
- Business case obtained buy-in from senior management to the digital identity roadmap

5.8 IAM strategy for a global leader in industrial software

DXC Assessed IAM state and maturity, defined a 5-year IAM strategy with a clear implementation roadmap and strong business case for executive buy-in. Unified management of large number of partner and customer identities was key to success for the customer.

Business Challenge:

- Need flexible IAM capabilities to enable growth strategy and regular company acquisitions
- Manual management of an increasing number of identities becoming increasingly complex
- Disjointed platforms for managing internal, external, partner, and customer identities
- High number of partner (>20.000) and customer (>200.000) identities

How DXC Helped:

- Conducted IAM current state and gap analysis.
- Defined IAM future state.
- Developed a comprehensive and holistic IAM strategy, based on DXC IAM Capability Model.
- Defined a high-level IAM roadmap and IAM target architecture.
- Development of business case to support IAM roadmap.

Business Outcomes:

- Actionable, comprehensive, and holistic IAM strategy.
- Increased awareness of current IAM posture and required improvements.
- Clear implementation roadmap, including achievable benefits.
- Technology recommendations considering existing IAM services, assets, and licenses.
- Business case to obtain buy-in from senior management to the IAM roadmap.

5.9 IAM Strategy for a UK Transportation & Logistics Company

The organization faced fragmented IAM implementation, resulting in inconsistent processes and security gaps across its IT environment.

- Strengthened IAM governance by defining clear roles, responsibilities, and global IAM policies to improve control and compliance.
- Enhanced security posture through improved privileged access and credential management to reduce risks and vulnerabilities.
- Delivered a structured IAM roadmap and long-term program to streamline identity processes and optimize operational costs.

5.10 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.

6 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 Identity Assessment for Trusted Digital Public Services.



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. Public