CAMBRIDGE CYBER ADVISERS

Identity Access Management (IDAM) and Privileged Access Management (PAM)

Service Definition Document. Version 1.0

19 January 2026

Identity & Access Management (IDAM) & Privileged Access Management (PAM)

1. Introduction

This Service Definition Document describes the **Identity & Access Management (IDAM) and Privileged Access Management (PAM)** service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides a structured, comprehensive approach to designing, assessing, and improving identity governance, access control, and privileged access security across an organisation's technology estate.

Modern organisations rely on complex identity ecosystems spanning cloud, on-premise, hybrid environments, and third-party integrations. Attackers increasingly target identity weaknesses, misconfigurations, and privileged accounts to gain persistence and escalate access. Effective IDAM and PAM controls are therefore essential to reducing risk, supporting compliance, and enabling secure digital transformation.

CCA's IDAM & PAM service combines governance review, technical assessment, architecture design, and operational uplift aligned to NCSC, ISO 27001, NIST, and Zero Trust principles. The service delivers a clear understanding of identity risks, maturity, and required improvements to strengthen access security and reduce attack surface.

2. Service Overview

The IDAM & PAM service provides a holistic review and enhancement of identity governance, authentication, authorisation, and privileged access controls. The service evaluates the effectiveness of identity processes, technical controls, and operational practices across cloud and on-premise environments.

Activities include:

- Review of identity governance, joiner-mover-leaver (JML) processes, and access lifecycle management
- Assessment of authentication and authorisation mechanisms
- Evaluation of directory services (e.g., Azure AD / Entra ID, Active Directory)
- Review of privileged access controls, vaulting, session management, and break-glass processes
- Assessment of MFA, conditional access, and Zero Trust alignment

- Analysis of identity tooling (IGA, PAM platforms, SSO, federation)
- Review of cloud identity configuration and access policies
- Assessment of service accounts, machine identities, and API keys
- Mapping findings to recognised frameworks (e.g., NIST, ISO 27001, NCSC Zero Trust)
- Detailed reporting with prioritised remediation guidance
- Executive and technical debrief sessions

Service Features

- Comprehensive assessment of identity governance and access controls
- Review of directory services, cloud identity, and hybrid identity architecture
- Assessment of privileged access tooling and operational processes
- Evaluation of MFA, conditional access, and Zero Trust alignment
- Analysis of IGA, SSO, federation, and PAM platforms
- Review of service accounts, machine identities, and secrets management
- Maturity scoring across IDAM and PAM domains
- Detailed reporting with actionable recommendations
- Executive summary with risk-based prioritisation
- Optional advisory, design, and implementation support

Service Benefits

- Strengthens identity security and reduces attack surface
- Improves governance, access lifecycle management, and compliance
- Supports Zero Trust adoption and modern authentication practices
- Identifies misconfigurations and weaknesses before they are exploited
- Enhances operational efficiency and reduces identity-related incidents
- Supports alignment with NCSC, ISO 27001, and regulatory requirements
- Enables informed investment decisions based on risk and maturity
- Improves resilience across cloud and hybrid identity environments

3. Service Scope

The service includes, but is not limited to, identity governance review, access control assessment, privileged access evaluation, cloud identity configuration review, and maturity scoring. Activities may include JML process assessment, directory services review, PAM tooling evaluation, conditional access analysis, and Zero Trust alignment assessment.

4. Delivery Methodology

CCA follows a structured, phased approach using our standard methodology:

- Scoping and Planning
- Documentation Review and Stakeholder Interviews

- Technical and Process Assessment
- Analysis and Reporting
- Executive and Technical Debrief

5. Deliverables

- Executive Summary Report
- Technical Findings Report
- IDAM & PAM Maturity Assessment
- Risk Register and Impact Analysis
- Prioritised Remediation Roadmap
- Optional Advisory and Implementation Support Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- Draft report within 10 working days of assessment completion
- Final report within 15 working days
- Weekly progress updates for longer engagements

7. Governance and Assurance

Activities align with NCSC guidance, ISO 27001, NIST identity standards, and Zero Trust principles. Where required, engagements will be managed by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include findings report, maturity scoring, risk register, impact assessment, executive summary, remediation roadmap, and optional evidence pack.

Incident Management

The service evaluates identity-related incident readiness but does not manage customer incidents.

Disaster Recovery

Not applicable.

Availability

CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time.

8. Security and Data Protection

- Confidential handling of customer data
- UK-based assessment team
- Secure environments for data processing
- Data retained for 30 days then destroyed
- GDPR, NCSC, and ISO 27001-aligned practices

GDPR & Data Privacy

- Personal data minimisation
- DPIA support available
- Findings anonymised unless requested otherwise

Accreditations

- ISO 27001-aligned practices
- NCSC-aligned methodologies

Staff Security Clearance

SC-cleared staff available upon request; BPSS as a minimum for all CCA consultants.

9. Customer Responsibilities

Customers must provide scoping information, documentation, stakeholder access, and support remediation actions.

Technical Requirements

- Scoping information
- Documentation access
- Contact details for key personnel

Supported Browsers/Devices

Not applicable.

Access Restrictions

Customer must designate authorised individuals for scope approval, change requests, access to customer systems and/or services, and receipt of outputs.

10. Service Constraints

Activities are limited to agreed scope and timeframes; some may require controlled windows for identity or directory service testing.

11. Pricing

- Pricing is engagement-based and determined by scope, duration, and complexity. Pricing is based on:
  Number of identity systems and directories in scope
- Complexity of cloud and hybrid identity environments
- Depth of PAM tooling and process assessment
- Duration of engagement

Typical engagements range from 2–10 weeks depending on breadth and complexity.
Day-rate pricing is available and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering is typically completed via Purchase Order following confirmation of service purchase. CCA will invoice at the end of every calendar month, providing a detailed breakdown of services delivered, including VAT/expenses. Consolidated invoices can be provided. Invoices may be issued electronically or via post.

12. Exit and Offboarding

- Findings delivered
- Knowledge transfer completed
- Data destroyed within 30 days (certificate available)

Onboarding

- Requirements workshop
- Scope definition
- Stakeholder identification
- Communication validation

Offboarding

- Walkthrough of findings
- Delivery of reports
- Optional remediation workshop
- Secure data destruction

Training Provided

- IDAM & PAM awareness session
- Zero Trust and identity governance briefing
- Optional tabletop exercises

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; work completed to date will be invoiced
- Provider may terminate only under defined exceptions (e.g., breach of Rules of Engagement or safety concerns)

14. Contact and Support

A delivery manager is assigned for each engagement. Support is available via email and phone during delivery hours.

Included as standard:

- Email and phone support during the engagement
- Delivery manager assigned
- Access to reporting team for clarifications

Enhanced support packages available for ongoing identity governance and PAM uplift programmes.