

A Gartner G-Cloud 15 Service Definition for Cloud Consulting: Cloud Security — Cyber Security Identity and Access Management (IAM) Modernisation

2026

Gartner G-Cloud 15 Service Definition

© 2026 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This Gartner G-Cloud 15 Service Definition, including all supporting materials, is proprietary to Gartner, Inc. and/or its affiliates and is for the sole internal use of the intended recipients. Because this Gartner G-Cloud 15 Service Definition may contain information that is confidential, proprietary or otherwise legally protected, it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.

Gartner

Service Summary

Gartner's fast-track cyber security Identity and Access Management (IAM) modernisation service offers clients an affordable, low-risk approach to quickly improving the control of digital identities and entitlements maintained in repositories throughout their organisation. It substantially reduces risks posed by poor IAM practices and control of user/administrator accounts and access privileges.

Service Description

The Gartner cyber security IAM modernisation service comprises four phases. Clients can select any or all phases within the scope of an engagement.

Phase 1 — IAM strategy and target service architecture definition

This work includes investigation of the requirements to manage internal, supply chain/ecosystem and customer identities and entitlements; matching the needs of the business to environmental, regulatory and legal constraints and requirements to define an IAM strategy that will guide IAM policy and IAM life cycle process management for the organisation. The IAM governance and life cycle process review and revision, Phase 2, is typically undertaken in parallel with and informs the organisation's definition of an IAM strategy.

The strategy will:

- Create a roadmap for IAM improvement that prioritises the most important Identity Governance and Administration (IGA) capabilities, while considering dependencies, risks and costs
- Consider the depth, complexity and consistency of the organisation's processes for access requests, workflows and provisioning, and balance procedural versus technology changes to deliver the most cost-effective and lowest-risk outcomes
- Define a target IAM architecture for the organisation at a conceptual level
- Conduct a gap analysis to specify the gaps between current and target states

Phase 2 — IAM governance and life cycle processes review and revision

Review any recommended revisions to an organisation's IAM governance and identity and access life cycle processes review and revision. This covers the following:

- Identity and access management governance:
 - Auditing and reporting, including event collection, access monitoring and reporting
 - Access re-certification and attestation
 - Role engineering and mining.
- Identity management processes:
 - Provisioning and workflow management, including account provisioning and deactivation for Joiners, Movers and Leavers (JML)
 - Self-service administration
 - Directory services — Management and maintenance of authoritative identity and entitlement stores
- Access management processes:

- Access policy administration
- Privileged Access Management (PAM) covers the security of privileged user credential storage and management, fine-grained access control, and privileged user access monitoring and recording
- Authorisation services — Discretionary, Role Based and Context or Attribute Based Access Control services (DAC, RBAC and ABAC)

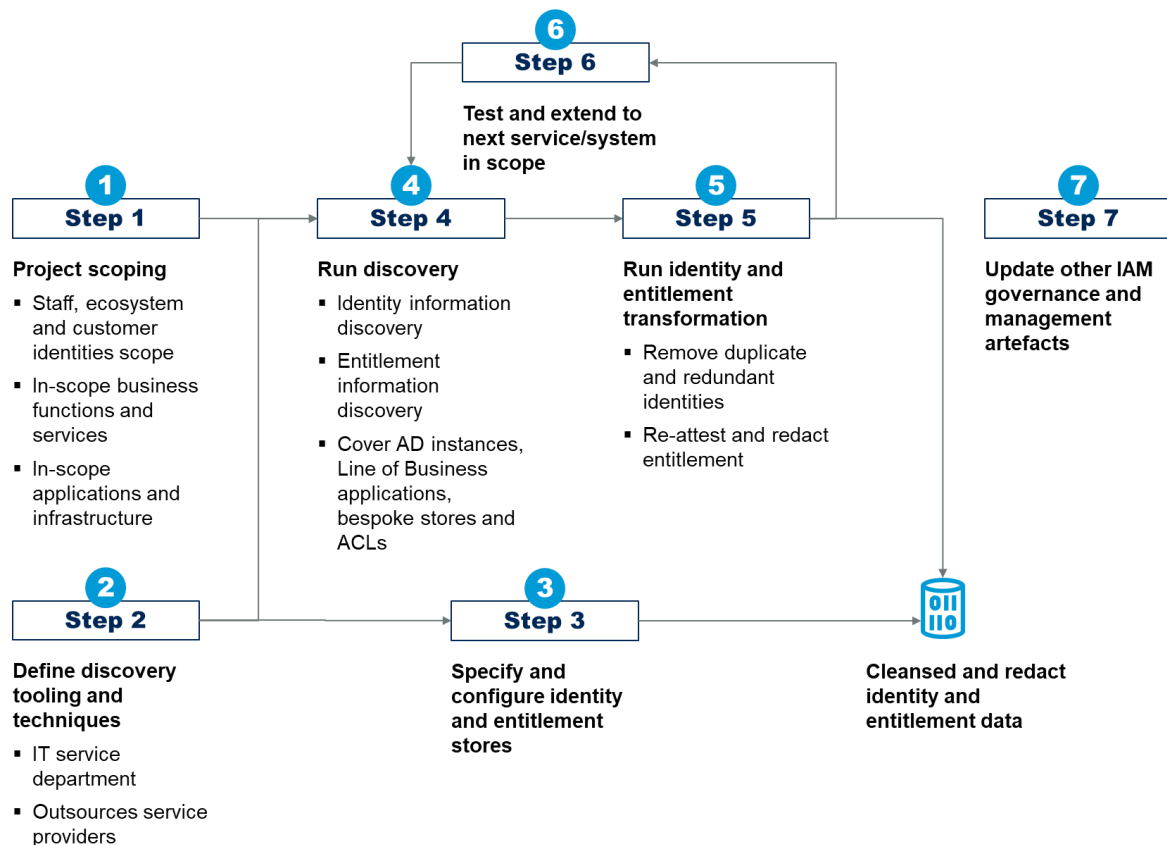
The output of this phase is a recommended set of revisions that represents a streamlined and improved operating model for the management and governance of identities and access entitlements.

Phase 3 — Fast track remediation of identities and entitlements

This phase requires technical discovery of identity and entitlement information across the subscribing organisation's IT services and infrastructure within the scope of the engagement. Its output is to cleanse and redact identity and entitlement information, providing a trusted subset of identity and entitlement information that substantially reduces the immediate IAM risk posed to the organisation. The following activities are included:

- Scoping of the internal staff ecosystem and customer identities, IT services, applications and infrastructure within the scope of the fast-track remediation
- Agreement of identity and entitlement discovery tooling and techniques. This is typically with the internal IT service department and outsourced service providers whose services are within the scope
- Specify the patterns for identity and entitlement information management and storage. Specify and configure target identity and access stores
- Run the discovery
- Redact duplicated and redundant identities, updating a new, clean identity store
- Revise entitlements, transforming and updating the access data
- Progressively run and test the transformation for selected business functions, services and applications
- Update the IAM strategy and IAM operating model — defined in Phases 1 and 2

The fast-track remediation phase is illustrated in Figure 1.

Figure 1. Fast Track Remediation Phase

Phase 4 — IAM Market and Solution Evaluation

The work in the preceding phases is likely to have identified the need to review and potentially revise the tools and technologies required to enable improved processes for managing identities and entitlements. Identity Governance and Administration (IGA) technology often consumes more of an identity and access management (IAM) programme's capital expenditure/operating expenditure budget than all other IAM investments combined.

This phase undertakes the following:

- Specification of the requirements for improved IAM tooling and technology
- Identification and evaluation of identity governance and administration products that best meet the specified requirements and other buying criteria, including whole life cost, implementation/deployment risk, operational support and service management considerations
- Production of solution architectures and procurement considerations to meet the IAM tooling and technology needs

Service Benefits

- Early ROI through reduced service management costs
- Low-cost and risk approach for rapid IAM improvements
- Reduced risk of unauthorised access
- Risk associated with privileged accounts substantially reduced
- Implementation of regulatory controls, including for GDPR requirements
- Reduced risk from insider threat

- IAM policy breaches identified and rectified
- Clear target architecture and plan for full IAM remediation
- Evaluation of technologies/solutions for target IAM architecture

Service Features

- Industry-leading IAM research informs the Gartner analysis
- Modular service permits combination of any/all phases/components
- Flexible scope for alignment with specific areas of the business
- Short-duration yields early operational improvements
- Coverage of digital platforms/services, including cloud, OT and IoT
- Customer, supply-chain and digital ecosystem IAM coverage
- Scope can be fine-tuned for areas of business operation
- Accelerates delivery of actionable insights through proven analytical capabilities
- AI-powered analysis that augments Gartner's Insights and SME delivery experience

Full List of Service Features

Gartner's IAM Fast Track Acceleration Service will be delivered against an agreed scope of applications and business units. As part of the in-scope activities, Gartner will:

- Develop an IAM strategy that is suitable for the organisation and its threat profile
- Reconcile all users and entities within scope to a single identity store
- Develop the complete portfolio of IAM-related policies and processes
- Remediate gaps in policies and processes
- Address any user account anomalies
- Identify all privileged access users along with justification for privilege access
- Selected features related to each phase of the service are listed below

Project Approach

Phase 0: Project initiation

- Conduct a kick-off meeting to ensure an understanding of the project objectives, scope, schedule, milestones, roles, responsibilities and required resources
- Discuss and identify any anticipated risks and mitigation plans based on lessons learned from experience
- Identify key people and stakeholders required for the discovery and analysis phase

Phase 1: IAM strategy and target service architecture definition

- Conduct a rapid assessment of the current state of IAM within the organisation
- Understand the client's wider strategy (e.g., business strategy, IT strategy, etc.) to help inform the IAM strategy direction
- Develop the IAM strategy and define the target architecture for the IAM service required

- Identify the gaps between the current state and the target state of IAM

Phase 2: IAM governance and life cycle processes

- Leverage the outputs from Phase 1 to identify what IAM governance and life cycle process that need to be updated or developed
- Develop/update the IAM policies and processes, including J/M/L, recertification, privilege access, separation of duties
- Assign business owners for each of the processes (e.g., HR for J/M/L, business owners for the recertification of the applications they own)
- Identify all types of users within the organisation, including FTE, contractors and service providers

Phase 3: Fast-track remediation

- Establish a single identify for each user within the organisation and reconcile user access to the respective single identity
- Conduct discovery of all user access anomalies, such as duplicate accounts, orphaned accounts, etc. and resolve all user account anomalies
- Reconcile all users to the correct user groups defined within the organisation
- Identify all privileged users and document privilege access justification. Remove any privilege access which cannot be justified
- Conduct an analysis of the separation of duties and remove any user access that breaches the separation of duties policies

Phase 4: IAM solution evaluation

- Evaluate and specify the components that map to the defined target IAM architecture (See Phase 1)
- Leverage Gartner Research to conduct an evaluation of in-scope IAM products and services
- Map the target component architecture to available products and services
- Undertake a solution evaluation to identify the most suitable products and services to implement the target IAM architecture
- Develop a “pros and cons” report for each shortlisted IAM product and solution

Project Schedule

The estimated schedule is based on a 10-week engagement, but is subject to change based on the scope of activities agreed upon engagement.