

■ SERVICE BRIEF

Identity & Access Management (IAM) *Assessment*





re

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Identity & Access Management (IAM) Assessment.

This point-in-time assessment evaluates the Customer's current-state IAM practices, policies, and tooling to identify gaps, risks, and opportunities for improvement in identity governance and access control.

This service engagement is governed by this Service Brief and associated with SKU: SEC-IAM-ASSESS. The quantity defined in the quote determines the number of identity systems and accounts to be reviewed under this engagement

The FUTURE BELONGS
to the CURIOUS.

Table of Contents

01. Services Overview

02. Offer Structure

03. Project Scope

04. Quantity & Effort Model

05. Services & Key Activities

06. Deliverables

07. Services Scope Changes

08. Services Scope Exclusions

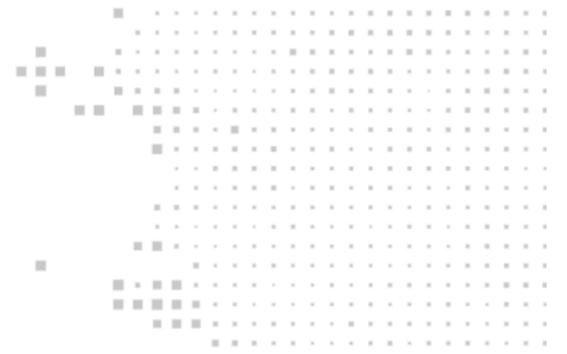
09. Customer Responsibilities

10. Services Schedule

11. Terms and Conditions

01. Services Overview

Redesign's IAM Assessment Service provides a structured, vendor-agnostic review of the Customer's identity and access management ecosystem. The service focuses on authentication methods, user provisioning/deprovisioning, privileged access, federation, and directory integrations to evaluate current-state maturity and provide prioritized recommendations.



02. Offer Structure

PRIMARY SERVICES

- Assessment of IAM controls, practices, and architecture across defined system.

Including:

- Documentation review
- Stakeholder interviews
- Gap analysis

OPTIONAL ADD-ONS

Separate SOW

- Implementation of IAM solutions
- Remediation work
- Identity lifecycle automation
- Privileged access management (PAM)
- Or conditional access policy deployment

03. Project Scope

This engagement includes a review of the IAM strategy, systems, policies, and user access patterns across a defined quantity of systems or platforms (e.g., Azure AD, Okta, Active Directory, Google Workspace, AWS IAM, etc.).

In-Scope Activities

- Review of identity sources (directories, HRIS, etc.)
- Authentication and MFA methods in use
- Role-based access control (RBAC) or group-based entitlement structure
- User lifecycle processes (provisioning, deprovisioning, transfers)
- Privileged access handling (admin accounts, break-glass, etc.)
- Federation and SSO configuration review
- Audit of identity governance or review practices
- Alignment with security and compliance frameworks (optional)
- Host reboots and post-upgrade health checks

04. Quantity & Effort Model

- **Service SKU: SEC-IAM-ASSESS**
- **Quantity: Number of identity systems and accounts**
- **Work per Unit Includes:**
 - System documentation and policy review
 - Stakeholder interviews (up to 2 per platform)
 - Configuration analysis and risk identification
 - Recommendations tailored to platform and risk profile

05. Services & Key Activities

Stage	Key Activities
 Discovery & Planning	<ul style="list-style-type: none">▪ Kickoff call and scope validation▪ Request and review IAM documentation (architecture, policies, diagrams)▪ Schedule stakeholder interviews with IT, security, and HR/business stakeholders
 Assessment & Analysis	<ul style="list-style-type: none">▪ Evaluate authentication flows, MFA enforcement, and federation▪ Identify privilege escalation risks and inactive/overprovisioned accounts▪ Review identity audit/logging capabilities
 Post-Engagement	<ul style="list-style-type: none">▪ Deliver written assessment including current-state observations▪ Identify gaps and maturity deficiencies▪ Provide actionable remediation guidance and IAM roadmap▪ Host review session with stakeholders

06. Deliverables



IAM
Assessment
Report



Prioritized
Recommendations



Virtual
Stakeholder
Review Session
(1 hour)

07. Services Scope Changes

Changes to the number of platforms, stakeholder access, or security domains assessed may require a revised SOW or quote. Expansion beyond current-state assessment into implementation will require a separate engagement.

08. Services Scope Exclusions

Unless explicitly stated, this assessment does not include:

- **Deployment or configuration of IAM tools or policies**
 - **Automation of identity lifecycle management**
 - **Real-time access or entitlements cleanup**
 - **Federation with third-party SAML/OIDC providers**
 - **Full security audit or penetration testing**
-

09. Customer Responsibilities

- **Access:** Provide documentation and access to IAM platforms or admin consoles (read-only if applicable)
- **Staff Availability:** Make stakeholders available for interviews and reviews
- **Inventory:** Provide a list of identity-connected systems and applications
- **Policy Sharing:** Share identity-related policies and control documentation (e.g., access review, admin control)

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:**
Upon quote acceptance and access provisioning
- **Completion:**
Final report and review session delivered within 10 business days of discovery completion

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

ⓘ SERVICES WILL NOT BEGIN UNTIL THE FOLLOWING PREREQUISITES ARE MET:

- Signed quote referencing SKU: SEC-IAM-ASSESS and quantity
- Access to IAM platforms granted
- Stakeholder availability confirmed

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

redesign

The FUTURE BELONGS
to the CURIOUS.

