IAM CATALYST

Overview

Our IAM Catalyst program is a detailed assessment of your organization's current state business processes and desired IAM direction. This assessment starts with detailed discovery sessions with various members of the organization to dig into the details of your organization's process to get a full current state picture. The end result is actionable insights and a recommended roadmap to help achieve your goals. Zirous' team of a senior-level IAM Business Analyst and a senior-level IAM technical resource will identify areas of improvement, blockers to future state goals, and recommendations to overcome them. Based on your organization's priorities and immediate needs, the IAM Catalyst can be tailored to meet the exact need of your organization.

Catalyst Modules

Identity and Access Management covers a wide breadth of areas within the business. Our Catalyst Assessment is fully customizable to only address the area's that matter most to your organization. Each assessment starts with the Organization Identity and Access Management Assessment, then you can choose which modules to include. Our team of Identity experts will work with you to define the right list of topics for your organization.

Organization Identity and Access Management Assessment 3 weeks			
Identity Governance 4 Weeks	**Workforce Access Management** 2 week	**Customer Access Management** 2 week	**Privileged Access Management** 2 week

Organization Identity and Access Management Assessment

- ☐ **Key High-Level Business Drivers** *(business requirements, used by management, to determine success of the IAM program)*
- ☐ **Replaced System Functionality**
- ☐ **Architecture and Design**
- ☐ **User Communities** *(who will use the system and in what capacity)*

- [ ] **Application Inventory** *(application types and entry points, identity store, authentication/authorization, provisioning/deprovisioning)*
- [ ] **API Inventory** *(expected clients, authentication, authorization, security policies)*
- [ ] **Self-Service Flows** *(registration, password management, preferences management, application requests)*
- [ ] **Service Desk Flows** *(ticketing, account/password/preferences management, session management)*
- [ ] **Account Management** *(how accounts get created, updated, disabled, deleted, etc.)*

Identity Governance

- [ ] **User Identity Lifecycle Management** *(Authoritative Sources for onboarding, offboarding, transfers, etc.)*
- [ ] **Password Management** *(policies, password propagation and self service)*
- [ ] **Role Based Access Control** *(application/business roles, role membership rules)*
- [ ] **Access Requests and Approval Workflows**
- [ ] **Fulfillment of Access** *(automated or manual workflow to provision and deprovision to target systems)*
- [ ] **Reconciliation with Target Systems** *(ensuring governance system matches what is actually in the target to catch out of band access)*
- [ ] **Compliance** *(reporting, auditing, certification of access, segregation of duties)*

Workforce Access Management

- [ ] **Identity Stores and Federations** (*where user accounts are stored, what data is stored, and authentication relationships between stores)*
- [ ] **Connectivity** *(data flows, downstream processes)*
- [ ] **Lifecycle Management** *(Account activation and deactivation for onboarding, offboarding, transfers, etc.)*
- [ ] **Password Management & Authentication** *(Single Sign-On, Multi-Factor Authentication, password & lockout policies)*
- [ ] **Security Monitoring** *(identity proofing, fraud detection, threat analytics)*

Customer Access Management

- [ ] **Identity Stores and Federations** (*where user accounts are stored, what data is stored, and authentication relationships between stores)*
- [ ] **Connectivity** *(data flows, downstream processes)*
- [ ] **Lifecycle Management** *(Account activation and deactivation for onboarding, offboarding, transfers, etc.)*
- [ ] **Password Management & Authentication** *(Single Sign-On, Multi-Factor Authentication, password & lockout policies)*
- [ ] **Data & Privacy Rights** *(customer data integration, regulations, PII flows)*
- [ ] **Security Monitoring** *(identity proofing, fraud detection, threat analytics)*

Privileged Access Management

- ☐ **Identity Stores and Federations** (*where user accounts are stored, what data is stored, and authentication relationships between stores)*
- ☐ **Connectivity** *(data flows, downstream processes)*
- ☐ **Lifecycle Management** *(Account activation and deactivation for onboarding, offboarding, transfers, etc.)*
- ☐ **Credential Vaulting & Secrets Management** *(types of credentials, rotating credentials, how users obtain access to shared credentials)*
- ☐ **Provisioning** *(session management & isolation, just-in-time privilege, zero-standing privilege, endpoint control)*
- ☐ **Service Accounts** *(account creation processes, provisioning processes, what user have access)*
- ☐ **Security Monitoring** *(identity proofing, fraud detection, threat analytics)*

Actionable Insights

All of the deliverables can be customized to your expected outcome. Regardless of what you chose, the insights gained will help you make decisions for the future of your Identity and Access Management practice area

- ☐ Current state IAM Architecture diagrams
- ☐ Current state Business Process documentation
- ☐ Analysis and Recommendations, including:
    - Business needs and opportunities
    - Current gaps and pain points
    - Recommended security policy changes
    - Recommended business process changes
    - Recommended tooling and technical integrations
- ☐ Candidate Vendor/Tool Evaluations - Zirous will use your functional needs and priorities to evaluate software that best fits your organization's needs
- ☐ Technical Roadmap for implementing recommended changes - Zirous will provide a phased approach for implementing changes while balancing resource constraints and user impacts

Example 6-Week Plan

WEEK	ACTIVITY	OVERVIEW
Week 1	Detailed IAM Catalyst Plan	• Compile questions specific to your organization's use cases and current and future-state processes related to enterprise-wide and application specific requirements • Plan will define duration needed for each IAM Catalyst session and the target audience needed to participate

		• Coordinate/schedule meetings
Week 2	IAM Catalyst Meetings	• Execute IAM Catalyst Plan
Week 3 & Week 4	Follow-up meetings as needed Documentation	• Lead follow-up meetings necessary to obtain further details or get clarification • Document assessment from IAM Catalyst sessions
Week 5	Finalize Deliverables	• Finalize Assessment deliverables
Week 6	Onsite Review Sessions	• Review Recommended IAM Program Approach & Business Justification, update as appropriate and deliver

Resource Needs

These needs will vary depending on which modules are selected.

- The IAM Program Team, consisting of IAM leadership and decision makers
- The IAM Core Team, consisting of IAM Administrators and process SMEs
- The IT Security Team, consisting of Security and Compliance personnel responsible for defining organizational security policies, administering security controls, and monitoring threats within applications and systems
- The IT Privacy Team, consisting of those who define organizational privacy policies, processes and tools regarding the collection, processing, and storage of PII, whether of customers or of employees, as well as Privacy Rights request and fulfillment
- The Human Resources, consisting of those who understand the lifecycle of workforce users and administer HR data/processes like hires, job changes, leaves of absence, and terminations
- The Customer Resources, consisting of those who understand the lifecycle of customer business identities, and customer data integrations with other systems, including marketing and security systems
- The Workforce Service, typically consisting of those who understand and administer ITSM solutions for internal help desk purposes related to terminations, access requests, password resets, etc.
- The Customer Service, typically consisting of those who understand and administer call center and help desk solutions for supporting customers during account registration, login, update, and recovery.
- Various Application and System SMEs that own and administer key applications, systems, and infrastructure of interest