SailPoint

SOLUTION BRIEF

Fulfilling CDM Phase II with Identity Governance and Provisioning

SailPoint has been selected as a trusted vendor by the Continuous Diagnostics and Mitigation (CDM) and Continuous Monitoring as a Service (CMaaS) program Blanket Purchase Agreement (BPA) holders. Our partners provide government entities with solutions to support Phase 2 requirements which specifically provide capabilities that are intended to monitor and manage people-based accounts and services; TRUST, BEHAVE, CRED and PRIV.

The CDM\CMaaS program is designed to assist government entities with protecting their systems and networks from unauthorized access and bolstering their cyber defense posture. The goal of CDM is to continuously monitor and identify users' status, networked devices and systems and mitigate identified risk.

Phase 2 capabilities requirements include:

TRUST	**Manage Trust in Those Granted Access** Ensure only properly vetted users are given credentials and access to facilities, systems, data and privileged accounts.
BEHAVE	**Manage Security-Related Behavior** Ensure authorized users meet the security-related requirements for facilities, systems, information and privileged accounts to prevent insider attacks.
CRED	**Manage Credentials and Authentication** Ensure authorized users can be authenticated appropriately for access to facilities, systems and information. Establish whether authentication, reissuance and revocation policies are incurring more risk than deemed acceptable by enterprise policy.
PRIV	**Manage Account Access - Manage Privileges** Ensure that privileges for both physical and logical access are assigned to authorized people or accounts that require that access to perform authorized job responsibilities.

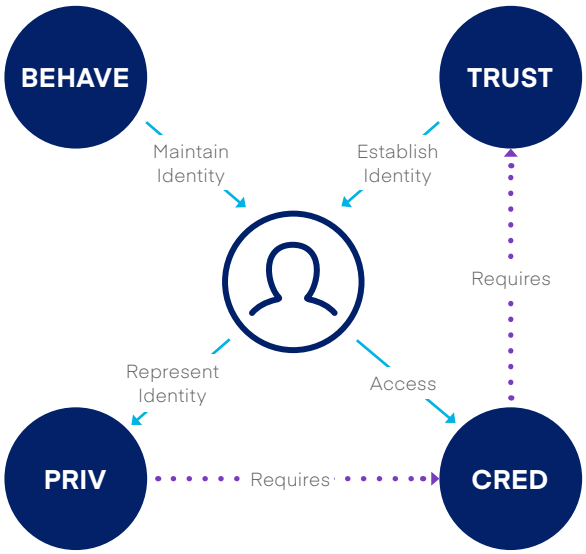
SailPoint's partners have selected the IdentityIQ solution for its unique industry-leading capabilities. SailPoint's governance-based approach centralizes visibility, improves compliance, and minimizes risk by uniformly applying controls across all identity governance and provisioning services. IdentityIQ is designed for the business user, translating complex identity data into actionable business information and processes.

Our partners provide full CDM\CMaaS dashboard development and integration, as well as full identity system integration and support, feasibility and capability studies of the SailPoint solution.

CDM Phase II: Manage Accounts for People and Services

The four capabilities; TRUST, BEHAVE, CRED and PRIV have significant interdependencies and CDM requires that each capability must be able to determine the Actual State and Desired State of the authorized user. As such, the TRUST, BEHAVE, CRED, and PRIV capabilities are dependent on the existence of a Master User Record (MUR) that identifies roles or characteristics that require specific trust levels, training, credentials and access rights.

These capabilities are closely related to the Federal Identity Credential and Access Management (FICAM) program which provides architecture and implementation guidance to address Identity, Credential and Access Management (ICAM) concerns. CDM extends government entities' cybersecurity postures by facilitating the gathering and reporting of metrics regarding critical security controls and objectives with the goal of identifying risks.



The CDM dashboard brings this data from ICAM together to create a single prioritized list providing a decision support tool for determining what mitigation actions to perform in what situation.

SailPoint's identity governance and provisioning platform ensures that data attributes from a user's identity are accurate and up-to-date with the data from risk assessments and policy management on protected resources that are used to make an access decision.

The SailPoint Solution

IdentityIQ lays the foundation for effective identity governance and provisioning within the enterprise. It establishes a single framework that centralizes identity data, captures business policy, models roles and takes a risk-based, proactive approach to managing users and resources. The platform also offers extensive analytics that transform disparate, technical identity data into relevant business information. Additionally, robust resource connectivity is provided that allows organizations to directly connect to applications running in the datacenter or in the cloud.

This unified set of controls, policies and processes allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications both on-premises and in the cloud. SailPoint IdentityIQ applies consistent administration of compliance and provisioning processes, maximizing investment and eliminating the need to buy and integrate multiple products.

IdentityIQ Identity Intelligence

Transform technical identity data scattered across multiple enterprise systems into easily understood and business-relevant information through intuitive reporting and dashboards. With identity intelligence, organizations can more quickly identify risks, spot compliance issues and make the right decisions to improve effectiveness. SailPoint pioneered identity intelligence solutions and is the recognized industry leader in delivering business-relevant information for effective identity and access management.

IdentityIQ Compliance Manager

Automate access certifications, policy management and audit reporting through a unified governance framework. This allows enterprises to streamline compliance processes and improve the effectiveness of their identity program.

IdentityIQ Lifecycle Manager

Monitor changes to access through user-friendly self-service request and password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of organizations in a way that is both efficient and compliant.

IdentityIQ Integration Modules

- **Third-party provisioning and service desk:** enables multiple sources of fulfillment to access change.
- **Service catalog:** supports a unified service request experience with integrated governance and fulfillment.
- **Mobile device management:** mitigates risk posed by mobile devices through centralized visibility, control and automation.
- **Security:** leverages third-party security solutions to enhance responsiveness and controls within identity governance processes.

- **Privileged Access Management:** enables layered management to secure information and prevent data breaches while providing a centralized place for roles, processes and policies.

SecurityIQ - Data Access Governance

SecurityIQ reduces risk by identifying where sensitive data resides, determining who has access to it and how they are using it, and putting effective controls in place to secure it. SecurityIQ helps government entities meet security requirements by providing proof of compliance during audits and increases staff productivity by reducing time spent on diagnostics, forensics and data administration tasks. It also simplifies the ongoing challenge of managing how users are granted access to unstructured data throughout a user's lifecycle within the organization.

Key Capabilities:

- **Visibility:** discover and catalog sensitive data and analyze who has access to what
- **Control:** establish data ownership and define audit and alerting policies
- **Analysis:** identify overexposed data and understand effective access models
- **Remediation:** normalize access to data and identify and address stale data issues

SecurityIQ shares information with IdentityIQ to provide comprehensive control of access to unstructured data. By augmenting identity governance data from structured systems with permissions data from unstructured data targets, organizations can more quickly identify risks, spot compliance issues and make the right decisions to strengthen controls. SailPoint provides centralized visibility across structured and unstructured data in the enterprise – all applications, all data and all users. SecurityIQ adds unstructured data targets to preventive and detective controls, such as access certifications and separation-of-duty (SoD) policy enforcement and automates provisioning access to unstructured data repositories and revocation of inappropriate access. Additionally, input from SecurityIQ informs the larger identity governance system with real-time activity data to improve risk mitigation and understand appropriate use.

SecurityIQ automatically collects and analyzes effective permissions for unstructured data and provides full visibility across on-premises Windows file servers, NAS devices, SharePoint and Exchange, in addition to cloud-based portals such as Office 365, Box, Dropbox and Google Drive. Data owners may, from a single dashboard, then:

- Identify and remediate overexposing access to sensitive data (open shares, sites, mailboxes, etc.)
- Report and remediate unused entitlements by cross-checking effective access with activity monitoring
- Ensure access for unstructured data is aligned with best practices across the enterprise

SecurityIQ enables government entities to discover and classify sensitive information and put effective security controls in place. SecurityIQ analyzes data using keywords, wildcards and regular expressions and uses verification algorithms for common data types to improve accuracy and reduce false positives. SecurityIQ provides flexible methods for classifying sensitive data using content-based or behavior-based approaches.

To prevent security breaches and information theft, or to minimize the potential damage of this activity, organizations need real-time tracking of users that access sensitive files or change file permissions, as well as the ability to respond to violations in real-time. SecurityIQ captures events for all users on monitored resources and enriches these events with user and machine details gathered from directories, identity systems, HR applications or any other data source.

Through its intuitive graphical interface and reports, SecurityIQ allows detailed forensic analysis and data usage auditing, addressing questions such as:

- Who has accessed this folder?
- What data has this user been accessing?
- Who accessed mailboxes not self-owned?
- Who changed this group's membership?
- What data is stale and for how long?

SecurityIQ can either stand alone or be integrated with other solutions from SailPoint.

Key Features for CDM

The SailPoint solution provides a single view of a user and his accounts, entitlements and associated risk across all applications, as well as structured and unstructured resources for "big picture" visibility and control. It also transforms technical identity data scattered across multiple enterprise systems into easily-understood and business-relevant information through intuitive reporting and dashboards. With the SailPoint platform, organizations can more quickly identify risks, spot compliance issues and make the right decisions to strengthen controls.

Identity Data Aggregation & Correlation

IdentityIQ aggregates technical identity data scattered across multiple enterprise systems and transforms it into a centralized, easily understood and business-relevant format that is accessible and actionable. User identities across enterprise systems and applications are correlated using rule-based algorithms, linking individual accounts and entitlements to create a holistic view of an identity and create an Identity Cube. This Identity Cube is a multi-dimensional view of each individual and their associated access, giving the enterprise more information and visibility into who has access to what.

Reporting & Logging

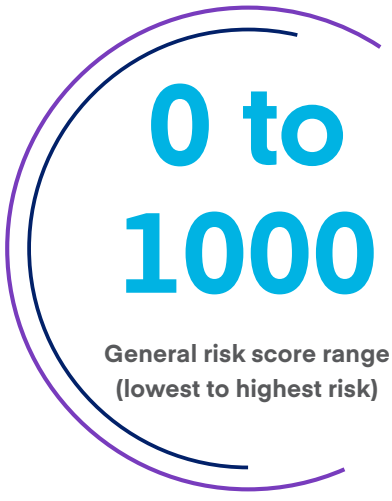
IdentityIQ and SecurityIQ include a reporting architecture that greatly simplifies the process of creating custom reports. Reports provide an at-a-glance view of the enterprise data which helps the organization manage system access and the compliance process. Basic reports can be created very quickly through an XML specification, and a variety of hooks are available for introducing more complex logic where it is needed to produce the desired report output. The standard report templates that are part of the product are modeled with this same XML specification structure, and are helpful examples of how custom reports should be structured.

All events and activities within IdentityIQ are recorded and can be accessed through the analytical real-time query engine and logging utility to monitor for security incidents, service levels and other key performance metrics.

Additionally, out-of-the-box support for common industry reporting standards, protocols and SIEM and DLP solutions enable real-time visibility for external enterprise security, reporting and forensic solutions.

Risk Model

IdentityIQ uses a combination of base access risk and compensated scoring methods to determine the overall Identity Risk Scores or Composite Risk Score to establish whether authentication, reissuance and revocation policies are incurring more risk than deemed acceptable enterprise policy (CRED).



Base access risk is a measure of inherent user access risk. Base risk scores are set on each role, entitlement and policy that are defined. The account weight attached to any additional entitlements that are assigned to an identity also has an impact on base risk scores. Account weights are factored into the entitlement baseline access risk scores.

IdentityIQ applies a series of compensating factors to each base risk score to calculate scores. These compensated scores are then weighted using a maximum contribution percentage and combined to form an overall Composite Risk Score for each user. The compensating factors and weighted values enable IdentityIQ to accurately identify high-risk users based on more than just the roles they are assigned within your enterprise.

For example, a user assigned only low risk roles might be considered high risk if they have never been included in a certification process. Alternatively, the identity may be considered high risk if the roles they have are in violation of separation-of-duty policies. Risk scores can be used to determine if a user has been granted or assumed excess or inappropriate access. (CRED)

Integration with PAM Solutions
Privileged Access Management (PAM) and Identity Governance can be implemented together to layer protection to prevent security breaches and information theft. IdentityIQ links the native capabilities of PAM solutions to extend access governance to privileged entitlements. An integrated solution with a PAM appliance\software application allows government entities to centralize on a single, unified set of roles, workflows, certification activities, policies, and rules for access for the target system.

Access Certifications
The Access Certification process ensures only properly vetted users have been given credentials and granted access (TRUST) that meet the security-related requirements (BEHAVE) and the correct privileges are assigned to authorized people or accounts that require that access to perform authorized job responsibilities (PRIV) without incurring more risk than deemed acceptable enterprise policy (CRED).

IdentityIQ enables automated reviews and approvals of identity access privileges, where each review can be annotated with descriptive business language that highlights changes, flags anomalies and highlights where violations appear. This process enables reviewers to:

- Approve access for identities
- Approve account group permissions and membership
- Approve role composition and membership
- Take corrective actions, such as revoking entitlements that violate policy

Certifications can be scheduled to run periodically or continuously – where certifications focus on the frequency that individual items need to be certified – and certifications can be configured to run based on events that occur within IdentityIQ. For example, IdentityIQ can be configured to automatically generate a certification when a user's manager changes.

Access Certifications for unstructured data can be integrated with SecurityIQ. When deployed as a standalone solution, SecurityIQ has built-in role-based and usage-aware access certification processes.

Provisioning
The IdentityIQ provisioning capabilities help government entities manage system access for their personnel. Provisioning requests can be created and processed in several ways in IdentityIQ, based on the needs and configuration of the installation. In many cases, modifications to access or entitlements requested in IdentityIQ can be automatically reflected in the associated native applications.

IdentityIQ can integrate with provisioning providers to automate access management. Provisioning providers can communicate user and account information and automatically add or revoke access. IdentityIQ can also enable automatic remediation for applications associated with direct connectors.

Policy Model

Policies defined in IdentityIQ enable the system to evaluate an identity's access or activities and report any inconsistencies with the desired state of the Master User Record (MUR). Violations are reported to the violation owner (often the identity's manager) or the appropriate application owner. They can then permit an exception or initiate a remediation. The Policy Rule can be initiated at any time to prevent a violation from occurring prior to a request being made or after the fact if access has been obtained out-of-band.

One type of supported policy, SOD, ensures more access is not granted to authorized users than is allowed by business or security policy (PRIV) and enforces the enterprise risk policy (CRED).

Policy violations generate a provisioning request to revoke the invalid access. For example, when a manager evaluates an identity's SOD violations and determines that one of the accesses for the identity must be removed, the manager can then request the revocation of the invalid access.

Access Policies for unstructured data can be integrated with SecurityIQ. When deployed as a standalone solution, SecurityIQ performs real-time monitoring and policy evaluation of sensitive data and continuous review of normal users' behavior to detect anomalous activity.

Data Access Governance

Data Governance can be implemented within an identity governance framework to centralize a single, unified set of roles, workflows, certification activities, policies and rules for access for the target system. With input of real-time activity data and behavioral data from SecurityIQ, government entities can improve risk mitigation and understand appropriate use of unstructured data and prevent future insider threat, security breaches and data leakages.