

IDENTITY ANALYTIC AND COMPLIANCE MANAGER (IACM)

Fálaina's Identity Analytics and Compliance Manager (IACM) is key for the next generation Identity Governance and Administration (IGA) solution that provide complete visibility on who's who, what's what and who have access to what for enterprises to address their audit and compliance requirements.

Fálaina's IACM is the foundation for Identity Lifecycle Manager and Privileged Access Manager, which is a powerful platform for enabling and improving compliance at a lower cost. A single integrated IGA platform that makes it possible to set a baseline for compliance and maintain that baseline to detect violations.

In addition, because the IGA process is intrinsically linked to the compliance process, a single integrated platform also makes it possible to consolidate all capabilities with compliance checking, thus enabling prevention and not just detection.

Fálaina's IACM key capabilities includes:

- Reconciliation process with automated discovery of account and access
- Complete visibility with comprehensive entitlement catalog
- Identity governance, risk and compliance management with Segregation of Duties (SoD) checks
- Access rights review with close-loop remediation
- Enterprise role management

Fálaina's next generation IACM also provides identity centric threat intelligence. Proactively enforcing access rights policies, monitoring of rogue user creations, access right changes, detection of dormant/inactive accounts, and segregation of duties (SoD) checks makes IACM as the utmost security defense platform.

Reconciliation process with automated discovery of account and access

Discovery of users (employees and non-employees) against their accounts in various target systems is key to detection process. IACM provides agent-less connectors for both authoritative source and target systems integration to enable enterprises to automate the reconciliation process.



The IACM discovery engine is distributed in nature and can be deployed both on-premise and on the cloud. IACM today has more than 40 out-of-the-box agent-less connectors that enable discovery of accounts, technical group/role and permission across operating systems, directory servers, databases, mainframes, enterprise applications, IoT platforms and Cloud/SaaS based applications.

IACM also supports the use of flat files/batch files to populate the employee identity data and access rights data. The data population of these data can be scheduled for periodic reconciliation.

Every target systems stores their Identity data differently. IACM provides a mechanism for not only aggregating identity and entitlement data, but storing the data in a normalised format in the identity repository.

Complete visibility with comprehensive entitlement catalog

Fálaina's IACM entitlement catalog displays the actual access rights granted to any individuals including employee and non-employees. Access rights granted also referred to as authorisations, privileges or permissions.

The initial access rights granted as part of the employee/non-employee on-boarding process with default access rights. As the individual journey continues with the enterprises, the access rights get updated or added.

The IACM entitlement catalog displays employee identity data along with their detailed access rights data which was discovered and reconciled as part of the discovery process. IACM's entitlement catalog gives the ability to drill-down access rights data across target systems specific login/account, technical group/role and permission details.

Identity governance, risk and compliance management with Segregation of Duties (SoD) checks

Fálaina's IACM provides cost effective GRC solution to address a wide range of compliance requirements such as segregation of duties (SoD) conflicts, sensitive access and other violations. It produces results for policy violations, reviews, risk scoring, reports and dashboards.

Assuming for ERP or CRM systems such as Oracle, Salesforce or SAP, users may have conflict of access rights at role or actual permissions. Such roles could be ability to create transactions and approval of payments.

The SoD rules and policies can be applied across multiple applications or across platforms to address conflicts that exist across systems.

As part of the compliance check for sensitive access, policies can be created to query set of users having set of sensitive access for any systems, and these can be used for reporting and access rights review process.

Access rights review with close-loop remediation

Fálaina's IACM automate access review and certification processes. The access review and certification use workflow processes and web portal to present identity data and entitlement data to reviewers.

The solution allows the reviewer to run certification campaign by resource, user, entitlement or by any attributes such as review of users leaving the organisation, inactive/dormant users, users transferred to other department or delta certification. Sensitive access and SoD compliance review is integrated as part of this review and certification process to allow seamless experience for the reviewer and approvers. Other capabilities include workflow integration and attachment management.

The IACM review and certification process includes close-loop remediation process via workflow process, provisioning event or email notifications.

Enterprise role management

Role management is the process of mining, modelling, defining and maintaining roles in the IGA implementation. Business roles are typically used to define individual job functions within an organization. IT roles on the other hand are created to provide valuable information to construct policies for administration of access, and enforcement of access within any applications.

Given the comprehensiveness of the connectors, Fálaina's IACM is able to mine access data all the way down to detailed entitlements, IACM automates the mining/discovery process and recommend candidate roles.

These informations are used in the downstream processes such as role-based provisioning, access review/certification, SoD checks, role-based access control across enterprises on-premise and cloud/SaaS applications.

About Fálaina

Fálaina is a technology provider of Identity and Access Management solutions. Fálaina enables enterprises to have visibility and secure their infrastructures, applications and data for private and public cloud. Fálaina comprehensive solution addresses today's requirements of an enterprise for:

- Identity Governance and Administration (IGA)
- Data Access Governance (DAG)
- Access Management (AM)

It provides businesses with the relevant reporting and analytics to improve IT security, maintain compliance and eventually minimise business risk.

To learn how Fálaina can help your business, visit www.falainacloud.com, or email us at sales@falainacloud.com.

