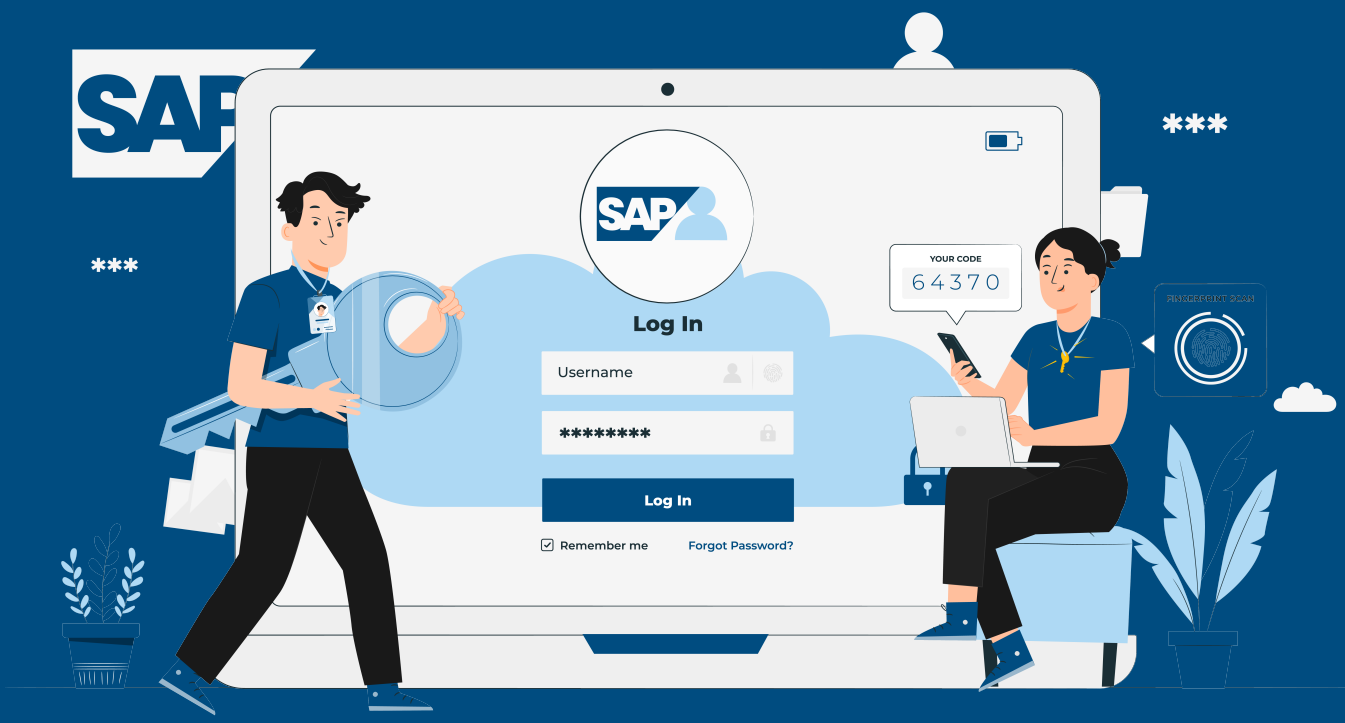
fálaina

Fálaina Access Governance & Privileged Access Management for SAP



Importance of Access Governance for SAP Systems

There were more data breaches last year than ever before, and the cost of breaches have never been higher. Time and time again, we see breaches occur as a result of compromised or stolen employee credentials, or a malicious insider with excessive privilege, including the large-scale data breach where hackers gained access to critical data through credentials stolen via excessive access or privileged access belonging to employees. Such breaches cost millions - and continue to cost even more - and we continue to see similar repercussions from large- scale data breaches around the world.

Unfortunately, hearing about another company's misfortunes may not be enough to get management buy-in for an IAMS program at your company. Selling IT programs to management can be difficult, especially when the programs don't tie directly to the bottom line. However, just as identity-related breaches can cost millions, strategic IAMS programs can - and do - provide measurable ROI.

IAMS projects are primarily driven by challenges in three areas: security, compliance, and user productivity. Building a business case for identity management involves demonstrating how identity management systems can effectively address these challenges and then justifying the cost based on the business benefits that result.

The following describes some of the typical challenges that drive organisations to pursue identity management projects:

1. Ensuring security and managing risk

The risk of a breach has been a security issue for as long as companies have been doing business online. Unfortunately, this is an issue that only seems to be getting worse. Organisations can take steps that range from implementing identity and access management, including privileged access management, systems at the most basic level (i.e., making sure that the right people have the right access to the right applications and data), to implementing sophisticated identity-based frameworks to control and prevent the misuse of access to data, or fraudulent use of corporate data.

2. Meeting compliance demands through Identity Governance

Organisations continue to work to improve their overall compliance with regulations that govern data privacy and integrity - while at the same time controlling the cost of that compliance. This becomes increasingly challenging as the number of regulations increase, the amount of data to be maintained grows, and operations become more complex in light of emerging trends such as cloud computing. Governance-focused identity management projects are designed to deliver end-to-end visibility and automate controls across an organisation's systems and applications. They make it easier and more cost-efficient to establish an organisation-wide desired-state model for compliance, enforce conformance to the model, and attest to the effectiveness of internal controls. Ongoing access certifications become both more effective and less resource-intensive through the strategic use of automated identity controls such as policy enforcement and role-based access models.

3. Streamlining delivery of access to the business

The original intention of streamlining the IT process of delivering access to critical business information has been to make it more efficient, minimise help desk costs, and speed up time to user productivity. Today, that vision remains compelling for many organisations as they continue to respond to pressure to increase operational effectiveness without increasing operating costs. Identity management addresses the need for efficiency with a variety of capabilities. These include the automation of time-consuming, error-prone manual processes for provisioning user access, as well as the creation of self-service environments in which users can directly manage their access without having to rely on assistance from the help desk.

The requirement for SAP Systems access governance is to improve SAP access management and to establish a structure for governance that standardises the management process and helps minimise access control risks for the long term. With this Access Governance for SAP Systems, organisations may yield many benefits, including:

- Access analysis by building detailed entitlement catalogue to understand who has access to what in SAP Systems
- Reducing unauthorised access, which may inherently become a risk across the organisation, with regular access review and certification process
- Limiting the risk of departing employees and time lost when employee access is changed
- Ensuring privileged access to SAP Systems are controlled and audited at all times
- Increasing efficiency of security and provisioning audits
- Streamlining the day-to-day management of access rights
- Helping organisations to meet overall regulatory and audit requirements

How Fálaina Technology Helps

The access governance for SAP Systems is based on Fálaina's next generation Identity Governance and Administration (IGA) solution that provides complete visibility on who's who, what's what and who has access to what for enterprises to address their audit and compliance requirements.

Fálaina's solution is a foundation that includes Identity Analytics and Compliance Manager (IACM), Identity Lifecycle Manager (ILM) and Privileged Access Manager (PAM), which is a powerful platform for enabling and improving compliance at a lower cost. This single integrated platform makes it possible to set a baseline for compliance and maintain that baseline to detect violations.

In addition, a single integrated platform also makes it possible to consolidate all capabilities with compliance checking, thus enabling prevention and not just detection.

Identity Analytic & Compliance Manager (IACM)

Fálaina, with its next generation IACM, also provides identity centric threat intelligence. By proactively enforcing access rights policies, monitoring rogue user creations, access right changes, detection of dormant/ inactive accounts, and segregation of duties (SoD) checks, IACM performs as a comprehensive security defence platform.

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

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

The compliant user provisioning is integrated with on-line user access request. It automatically notifies the user if there are conflicts identified. If the user's requests are required to be approved by the next level approver, the risk identified in the user's request will also be displayed to the approver. It will keep a record of all activities and their related risk for reporting purposes.

Identity Lifecycle Manager (ILM)

Fálaina's ILM is the industry's most lightweight solution that provides a "layered" approach to identity administration. This is an add-on component to Fálaina IACM and shares the same repository. Fálaina ILM and IACM share the same connectors to manage user identity lifecycle, and their access within enterprises applications and systems. Fálaina ILM enables enterprises to have complete administrative capabilities.

The IACM access right review process, along with close-loop remediation, are automated using integrated workflow.

Privileged Access Manager (PAM)

Fálaina's Privileged Access Manager (PAM) is designed to secure privileged users (identity) and accounts, while enabling practical session management from a single, integrated portal. This portal enables centralised authentication that is integrated with Multi-factor Authentication (MFA)

Fálaina PAM supports real time session monitoring and remote session termination where the authorised user can perform real time session monitoring and remote session termination from any popular web browser. Further, Fálaina PAM supports video log and keystroke log for every user session. This is to secure, control, manage, and monitor privileged sessions to enterprise critical assets like SAP system. PAM also keep your organisation safe from accidental or deliberate misuse of privileged access.

Fálaina's 3-Step Approach

Several approaches may be used to remediate security exposures. Fálaina provides the following 3-Step approach that effectively integrates traditional remediation steps with automation using Fálaina technologies, quickly yielding substantial results.

Step 1: Visibility into SAP Systems

Firstly, an organisation needs to gain visibility into their security environment within SAP Systems. This process involves deployment of Fálaina IACM to extract and correlate the data.

Fálaina Identity Analytic & Compliance Manager (IACM) functionalities will be deployed to perform the following functions to gain visibility into SAP Systems access information.

A. Discover and correlate SAP System accounts and employees

The automation can be performed end-to-end from Authoritative Sources (e.g. HRMS system or batch import of identity data) to SAP Systems. Fálaina IACM can detect identity lifecycle events as they occur in an authoritative source and transform them into add, modify, or delete events for purposes of processing.

This is performed as part of periodic discovery and reconciliation activities. Fálaina IACM can detect events that need to be executed in the future (e.g., effective date of user's joining). Further, it can support sunrise and sunset dating. The IGA solution supports multiple types of users: SAP Privileged Users (SAP Administrator), Employees (regular staff) and Non-Employees (e.g. contractors, consultants, etc.). As part of discovery logs, during each event the logs will be updated in Triggers and Request which is related to the users and in Services logs which is related to Service.

B. Aggregate entitlements/ permission for all application/ system users

Fálaina IACM provides a comprehensive Entitlement Catalogue which includes details such as user profile (personnel and employment) attributes (e.g. employee ID, mobile phone number, department, manager etc.;). The Entitlement Catalogue gives a comprehensive information on users' access down to 'n' level supported by the target application (e.g. SAP users' access till T code level, authorisation objects and so on).

C. Integration with HR Systems

Fálaina IACM also integrates with HR systems using comprehensive connectors, which helps to discover users' profile information where personnel and employment attributes (e.g. first name, last name, unique ID, mobile number, department, role, manager etc.;) are retrieved. The IDMS can detect identity lifecycle events as they occur in HR systems and transform them into add, modify, or delete events for the purposes of processing. This is performed as part of periodic discovery and reconciliation activities. The IGA comprehensive connectors allow connection to both HR and target systems, enabling organisations to automate the reconciliation process and provide details across different layers of access. Organisations are able to tag sensitive and hidden attributes from trusted sources and target systems so that they can be managed within permissible means to meet regulatory requirements for data privacy such as PDPA, PII etc.

Step 2: Reporting Exposures and Risks

Once all data been discovered and updated in IACM, rules and policies are created to define and report the sensitive access and SoD conflicts information. Rules can also be created to report dormant accounts, roles, and other attributes. This data then will be used to generate reports and highlight potential security exposures, and known false positives can be removed as part of the reporting process.

Once rule sets are refined, Fálaina IACM can provide an insightful summary and detailed reporting that enables organisations to focus their efforts on their greatest areas of risk.

Organisations have the flexibility to add/ customise reports, and below are list of out of the box reports available for SAP Systems:

- Users by SAP Applications/Module
- Users by Department/Location
- Dormant/in-active Users
- Roles by SAP Applications/Module
- Roles by Department/Location
- Dormant/in-active Roles
- Users with sensitive access
- Users with segregation of duties conflict
- Detailed Roles and associated TCODEs
- Detailed TCODE and associated Authorisation Objects

And many more

Step 3: Execute Remediation

With Access Review (Access Certification) campaign run based on organisation inputs - the exposures are quantified, and requirements determined, and a plan may be formed to prioritise remediation efforts. After prioritising remediation areas, the following activities may be undertaken:

Clean up – Clean-up efforts primarily entail the removal of unnecessary access or excessive access rights. Users often have SAP privileges that relate to a past project, not their current function. For example, a system administrator responsible for implementing the finance module during an implementation should be restricted to system administration functions after the application is implemented.

Assess and restrict sensitive access – Organization business owners should determine who should have access to sensitive functions and data, such as banking information. If an analysis indicates that 20 people have access but only 5 need that access, the remaining 15 users should have the privilege removed. Conducting this analysis before focusing on SoD reduces the number of SoD conflicts up front, if it is determined that users should retain some sensitive access.

Assess and restrict segregation of duties (SoD) – In this phase, companies may consider removing privileges from users or redesigning privileges and/ or employee functions. If it is determined that several SAP privileges need to be redesigned, the organization can embark on this role re-design process.

Emergency Privilege Access – Emergency Privilege Access allows normal users to be granted with temporary or ad-hoc privilege access so that users can perform set of tasks outside their normal roles. These Emergency Privilege Accesses are granted using pre-defined SAP accounts with complete audit trail and reporting enabled at SAP level. Users will be using the integrated workflow and Access Request facility to request for Emergency Privilege Access and this access is granted based on approvals along with validity of the access.

Fálaina Identity Analytic & Compliance Manager (IACM), Identity Lifecycle Manager (ILM), and Privilege Access Manager (PAM) functionalities will be deployed to perform the following functions to execute Step 3.

A. Automated Access Certifications

Access Certification capability with workflow integration to automate the Access Certification processes. The Access Certification will be fully configured and performed using web interface. The access review or certification process includes Segregation of Duties (SoD) and Sensitive Access (SA).

The Access Review/Certification can be configured to support the following:

- Define the scope of the access review process, e.g. an account, a list of user role and associated access permission, individual, a department, a division, company-wide, or specific group of users, etc.;
- Define type of review like review for accounts and access rights, staff accounts who have left the organization, role change, deactivated accounts and so on, level of reviewers, reviewers for each type of review, systems for review etc.;
- Scheduler: Manual and Auto trigger the access certification, e.g. ad-hoc, monthly, quarterly, yearly, etc.;
- Configure multi-tiered authorisation certification – display different levels of authorisation data (e.g. accounts, roles, group, transaction, object, etc.) for each application;
- Reviewers to indicate the outcome of reviews like approve and revoke;
- Send reminders to the reviewers and escalated parties if the review is outstanding for a defined period;
- Attach description and documents as part of the access certification process;
- Provide visibility on the status of access certification activities like completion to relevant users;
- Delta certification – highlight users or entitlement data that have changed since the last certification;
- Changes in access rights as part of review exercise will trigger tasks to the respective account administrators for action;
- Highlight out-of-policy and high-risk accounts and entitlements including SoD conflicts;
- Close-loop Remediation – If a reviewer determines that an entitlement is inappropriate, the solution can kick off a provisioning event;
- Central access rights listing will be updated according to the completion of update/tasks;

Once the Access Review/ Certification campaign has been configured and initiated, an Access Review task will be created. The reviewers and approvers will receive a notification (e.g. through email) and they will be able to access the access certification work-list items from the Self-Service dashboard (web-based interface). The IdMS solution also provides access certification reports and dashboards that allow administrators/ account reviewers to track the status of an access certification campaign.

The organisation's SAP Systems business and applications owners can then perform complete remediation and role redesign/re-engineering process using Fálaina IACM and ILM technologies.

B. Privilege Access Management (SAP Systems)

Privilege Access Manager provides the capabilities listed below for privilege access management process to enhance organisations' IT security and enable organisations to meet regulatory requirements, while practically enabling users to perform their day-to-day privileged activities in SAP System.

- Privileged access request management and approval workflow
- Privileged session - SAP Admin Application access (via SAP Client Application or HTTPS-Based for SAP HANA)
- Session recording and keystrokes logging
- Real-time session monitoring and access termination

Privilege Access Management will ensure SAP Privileged users can request for access to any privileged account on any critical asset based on the policies and rules created. These rules could limit the requestor to request only accounts within the group or set of servers the requestor is allowed to see and request. Other rules include day and time of access, especially after office hours access or location of access.

Fálaina's PAM is also able to log SAP Privilege user session with video recording for all SAP privileged sessions. These videos are encrypted and securely stored in the PAM server, and can only be viewed by authorised personnel based on RBAC security policies, via the administration web interface.

Fálaina's PAM provides real-time session monitoring and access termination. The session is made available for remote monitoring via video streaming and only viewing is allowed. This feature enables SAP systems owner to monitor vendor (who access SAP for system administration/maintenance work) session remotely instead of having to be physically present.

Business Benefits

Access governance require a strong foundation, including a robust user access administration and control for all access including sensitive access and SoD conflict. A centralised and automated provisioning process, Fálaina provides the right SAP security role architecture that fits current and future organisational needs, with controlled and monitored access. Ongoing input and commitment from all stakeholders involved, such as business users, IT, internal audit and regulatory requirement are also essential. Once the groundwork is done and a successful program is in place, an organization can realise many benefits, such as:

- Streamlined, enterprise-wide processes for managing access that result in cost savings
- Formalised risk management processes that identify high-risk exposures and mitigate them
- Better business results, as controls are driven more by business than by governance needs
- Greater efficiencies and cost savings due to effectively defined SAP security roles
- Enhanced protection of corporate data and assets
- Simplified compliance, improved governance, and easier auditing
- Maintain complete end-to-end audit trails/ records of who did what using the SAP Privileged Accounts
- Prevent unauthorised access and sharing of SAP Privileged Accounts and their passwords
- Precisely fix the accountability on SAP Privilege Accounts usage

Access control violations are inevitable. However, with an efficient and effective access management program that includes the foundational elements to get SAP Systems security right, and the correct structure to make processes sustainable, a company's ability to minimise, monitor and mitigate access control risks will be greatly enhanced, even as the organization changes and grows.

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's comprehensive solution addresses today's requirements of an enterprise for:

- Get visibility of who has access to what
- Automate and secure access to regular users and privileged users
- Centralise and unify access governance process

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

Visit us at falainacloud.com