Automate User Access Review and Certification

Control Access across the entire enterprise

User access is a common source of internal abuse and a top focus for IT Audits. It's key for organizations to not only know who has access to their systems but what they are doing.

The enterprise application landscape and data streaming from multiple sources is challenging. Rising cyber risks, insider threats and growing scrutiny from auditors is increasing the demand to streamline and automate the enterprise-wide user access certification process. Auditors are increasingly demanding complete, accurate and timely user access certification, a key control for financial risk and compliance management. In today's face-paced hybrid work environment, it's critical to have complete confidence that the access granted to users is limited to job roles and that privileges granted to the business applications are approved and periodically certified by the authorized management.

SafePaaS Enterprise Certification Manager™ makes it easy to manage and control access that meets the audit standards established and expected by major audit firms including the Big Four. Automating the process not only replaces a manual time-consuming task, often done via email and spreadsheets, but ensures timely, complete and accurate results ensuring compliance. **Automating access reviews saves organizations hundreds of hours each quarter**, which requires management review of access role assignments and privileges within business-critical applications.

Intuitive Review and Certification for Accurate Results

Certification Managers can easily complete the periodic certification survey by accessing a deep link to the certification page on SafePaaS that contains all the user-role access records assigned to the certifier. Users can start the certification using the Single-Sign-On (SSO) ID already assigned to them or receive a one-time Passkey to certify the users' roles. User information is augmented with information such as role usage frequency and provisioning records from business applications and ITSM systems to ensure that certifiers can perform this key control activity accurately.

Consolidated Controls Management and Administration for complete compliance

Certification Administrators have the ability to set up, initiate and monitor certifications for all business applications, databases, servers, and other data stores using a consolidated controls panel. Administrators can set up the survey by cross-linking user security information from multiple sources such as business applications, IT Services Management, Identity Management and Access Request Provisioning systems. The survey can be initiated using filters such as application environments, access risk levels, access groups, etc. to ensure complete compliance with policies while preventing time-consuming redundant activities. Analytics is available to monitor progress using dashboards, track completion status, send reminders to certifiers, and prepare audit reports.

Closed-loop User Access Change Management for timely remediation

Once the certification survey is completed, any access change requests to remove one or more role assignments for a user, expressed by the Certification Manager, are issued and monitored for timely risk remediation within SafePaaS as well as any integrated IT Service Management Systems such as ServiceNow.

Lower IT Costs with self-service integrated ITSM and IGA synchronizations

Enterprise IT leaders and service delivery managers responsible for access controls can lower IT cost of ownership by eliminating the manual activities frequently required to execute corrective actions after each certification. User access change requests can be synchronized with ITSM and IGA systems using self-service integration services on the platform.

Reduce Audit Burden with Risk-based Intelligent Certification Management

Intelligent Survey Initiation options can reduce the audit burden on management by eliminating redundant requests where the risk is lower than the threshold and accepted by management for user roles such as "birth-rights", fire-fighters, service-accounts, and robotic process automation (RPA) .

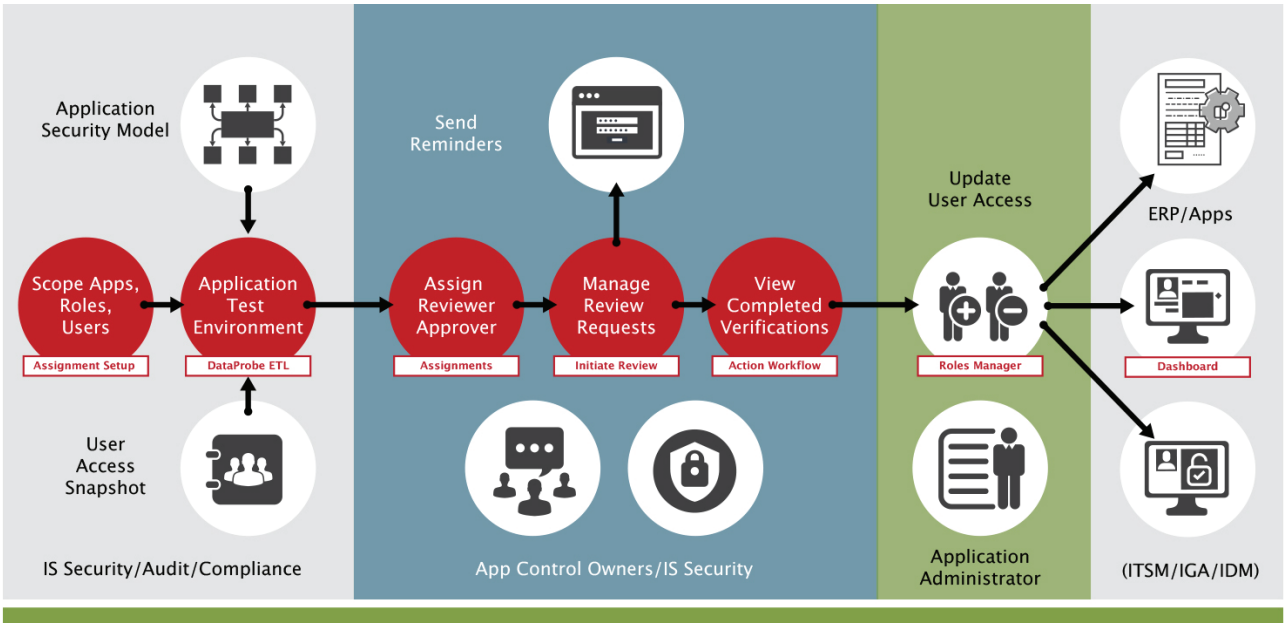
Prevent ITGC Control Failure with Fine-Grained Role-Entitlement Controls

Certification Survey displays the fine-grained entitlement details to prevent common sources of ITGC control failure where the provisioned roles are only abstracted at the job level – as often is the practice in configuring a roles catalog in ITSM, IDM and IGA systems. The lack of accurate representation of user privileges within entitlements granted by roles can result in a control failure where the privileges granted in the business applications are elevated due to security configuration changes e.g. ,"Payable Inquiry" role that allows the application user to create a supplier, or approve payments.

Rapid deployment with configuration integration protocols for on-premise and cloud applications

Whether your identity access certification includes applications in the cloud or on-premise, you can rapidly deploy certifications by choosing from a wide range of industry standard protocols for integration such as JDBC, REST and SOAP as well as formats including CSV, XML and JSON allowing you an easy, quick, and secure way of scoping the applications and data sources for the certification.

Automated Access Certification Process in SafePaaS



Best Practices to ensure Security and Compliance and seamless integrations

- **Scope Applications and Users to create a Central Controls Environment:** Security, Audit and Compliance departments collaborate to select the applications, users, identities, roles and entitlements in scope for certification. Your governance data is then extracted into the access identity governance hub.
- **Assign Reviewer and Approver:** Once your governance 'hub' is established, the business decides who's going to certify. (SafePaaS also offers an auto configure option to save time and certify quickly.)
- **Monitor Activity:** Continuously monitoring the applications provides evidence to stakeholders and external audit that your controls are operating effectively.
- **Manage Certification:** Set frequencies for high, medium and low risk for a risk-based certification process based on industry, business units and localization. Passkeys are provided for authorized certifiers for reliability and increased security lowering the burden on the business. Flexible options are offered to select users on your network and authorized in ID Management such as Azure, Okta, etc..
- **Dashboard capabilities:** Dashboards provide detailed, easy to read analytics and summary reports for efficiency and improved decision making. The automated process allows the Certification Manager to maintain these dashboards.

Seamless integrations with IDM and ITSM (Microsoft Azure, Okta, SailPoint, ServiceNow…) allowing for proactive continuous monitoring as well as a complete audit trail on ALL user access requests.

Azure
SailPoint
okta
servicenow