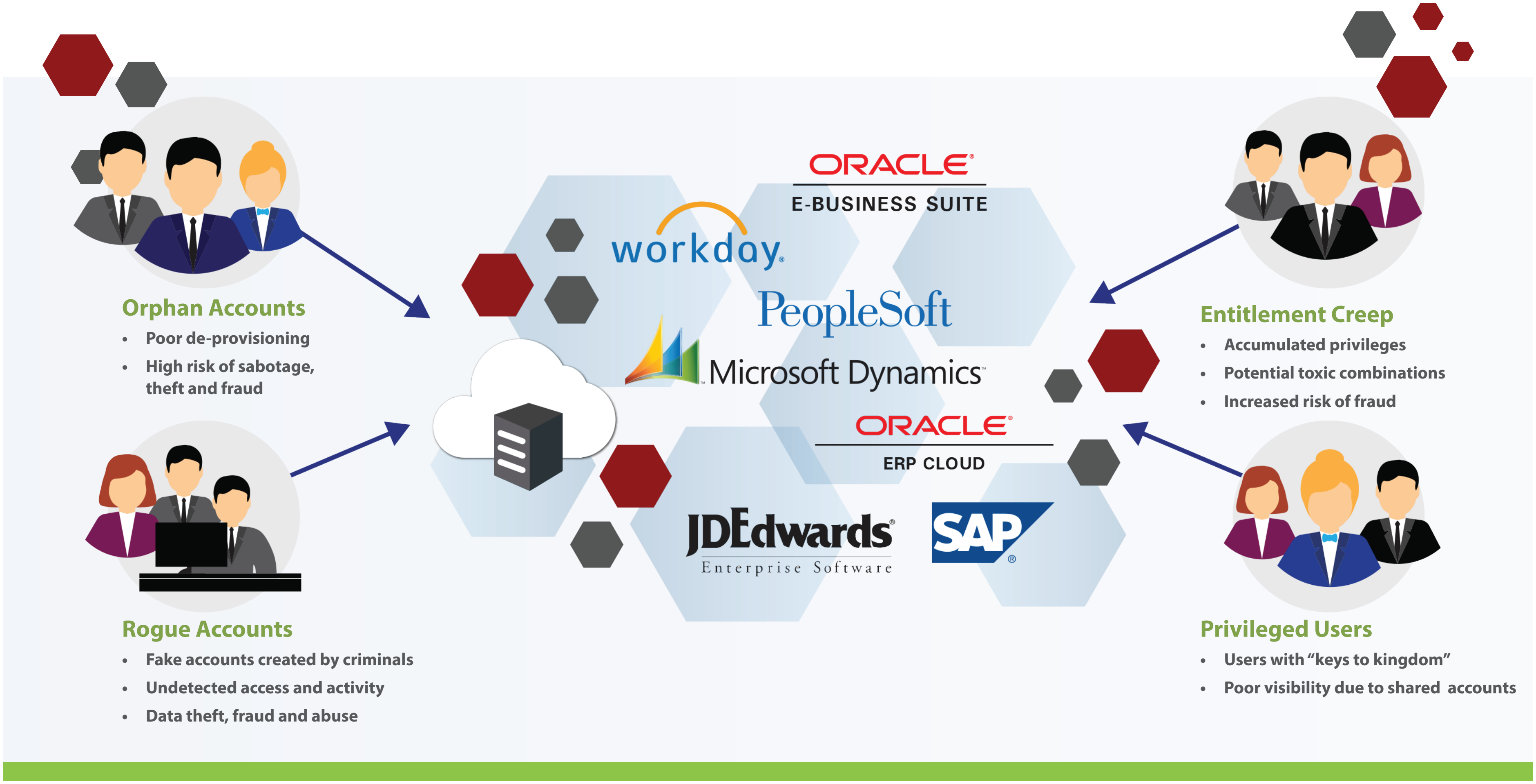
SafePaaS™

CISO's Guide to
Enterprise Application Access Governance

All product names, logos, and brands are property of their respective owners. Use of these names, logos, and brands does not imply affiliation.

User Provisioning Process: #1 area requiring remedial action

- User Access: Common Source of Internal Abuse is a Top Focus for IT Audits
- Gartner survey: 44% of IT audit deficiencies are IAM-related
- EY: 7 of Top 10 control deficiencies relate to user access control



Orphan Accounts

- Poor de-provisioning
- High risk of sabotage, theft and fraud

Rogue Accounts

- Fake accounts created by criminals
- Undetected access and activity
- Data theft, fraud and abuse

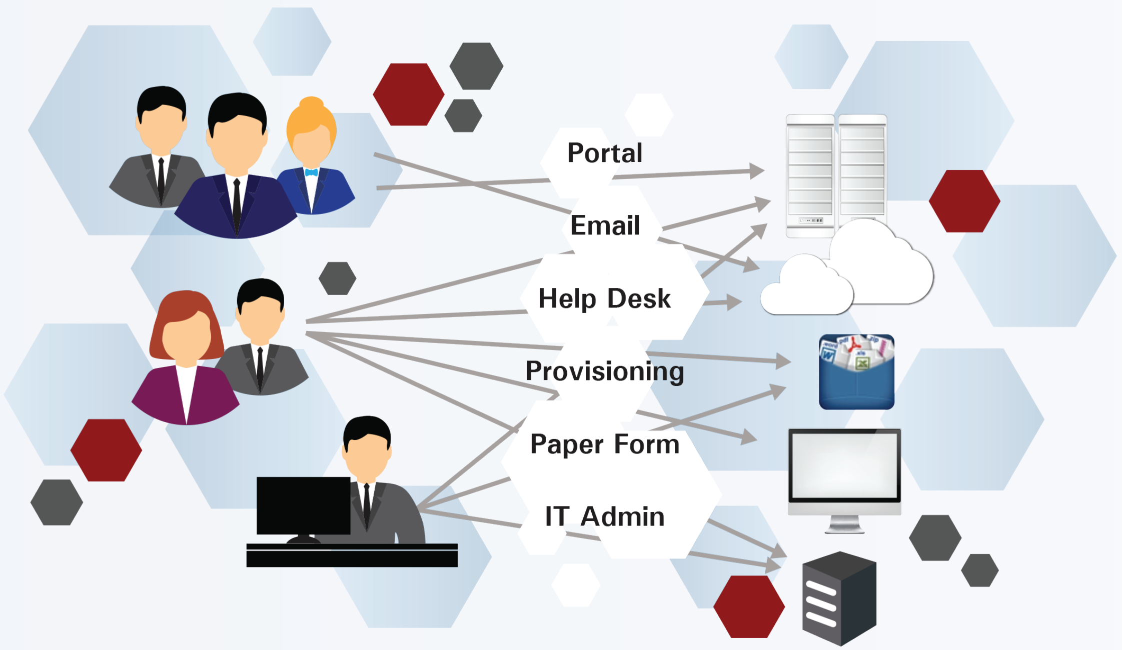
Entitlement Creep

- Accumulated privileges
- Potential toxic combinations
- Increased risk of fraud

Privileged Users

- Users with “keys to kingdom”
- Poor visibility due to shared accounts

User Provisioning Challenges with Traditional Access Management



Process

- Hundreds of user add, change, delete requests every day…
- Inconsistent, ad-hoc and manual processes – platform dependent…
- Disparate provisioning tools and workflows…
- Many human touch points: business managers, help desk, IT, etc…

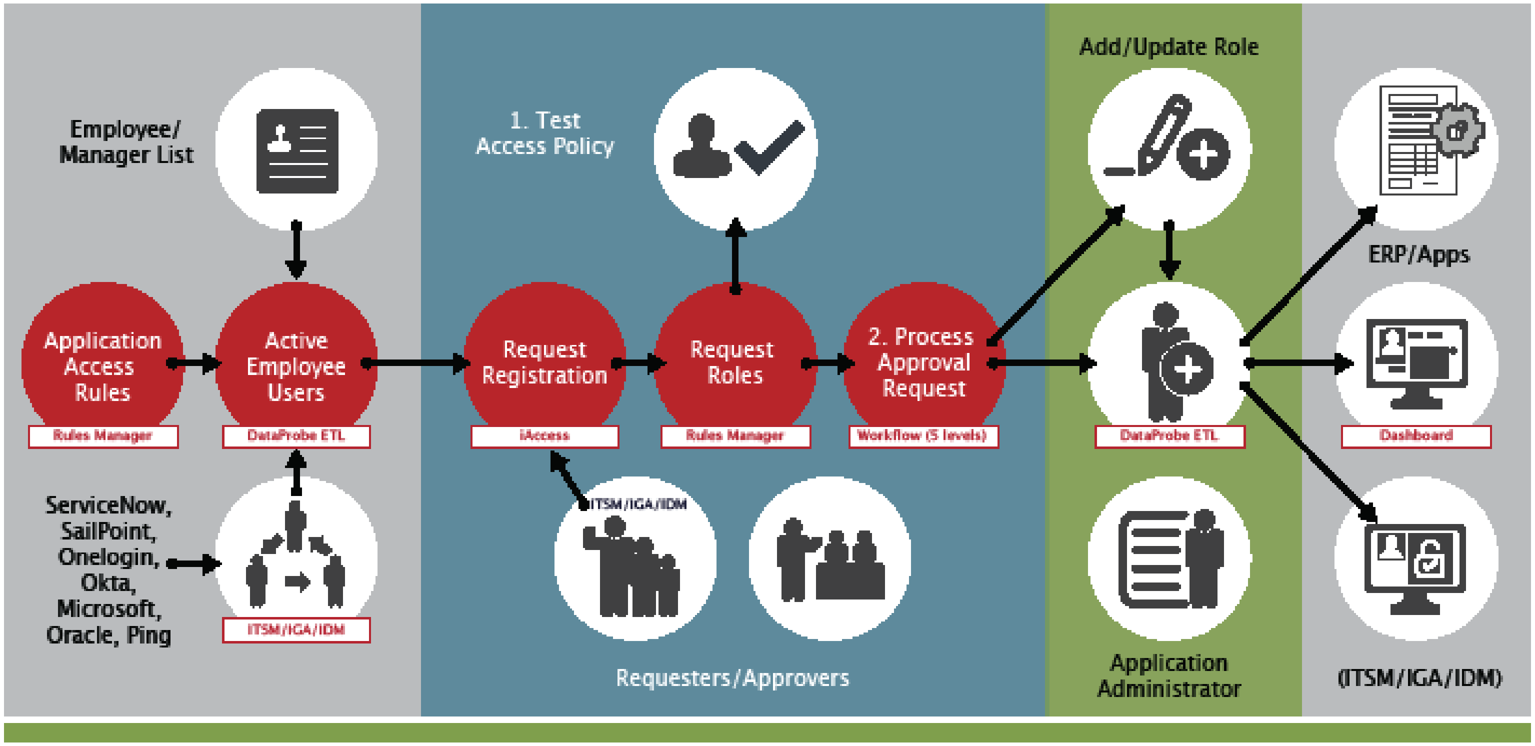
Challenges

- No consistent policy enforcement
- No common controls or audit trail
- Very difficult to ensure compliance and assess risk

Traditional Identity and Access Management (IAM) technologies control user access to enterprise systems by provisioning roles from a catalog of high level privileges, that do not prevent user ability to access sensitive data, privileges or functions, resulting in significant audit findings, increased risk of regulatory penalties and costly remediation effort. Unrestricted, widespread, or poorly monitored user access to sensitive data and transaction processing across an organization's enterprise applications not only violates the basic security policies for data protection and segregation of duties, but also severely limits the ability to establish individual accountability for privileged actions undertaken.

Risk-Based Approach for Application Access Governance

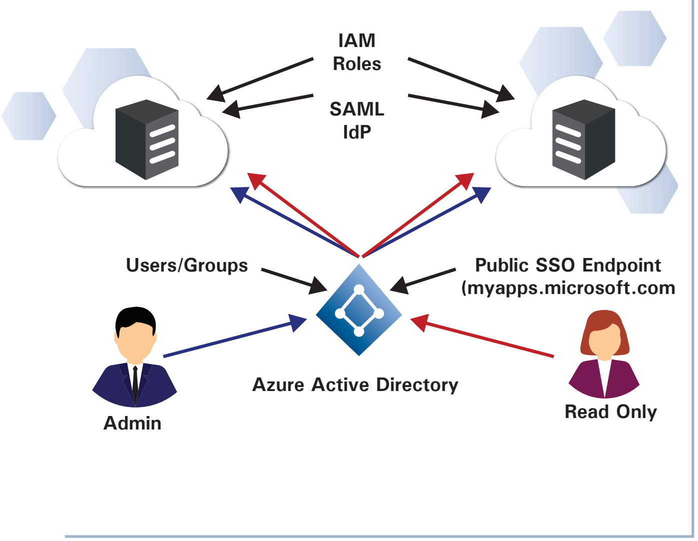
CISOs and risk management leaders accountable for enterprise security and access controls should take a risk-based approach based on special considerations, processes and tools to ensure that all user access requests to grant enterprise access privileges are processed in compliance with access governance policies by presenting any access control violations to the requesters, approvers and reviewers in the closed-loop workflow. The following approach will help streamline the mitigation of security, operational and business risks created by the inherent power of privileges granted to enterprise application users.



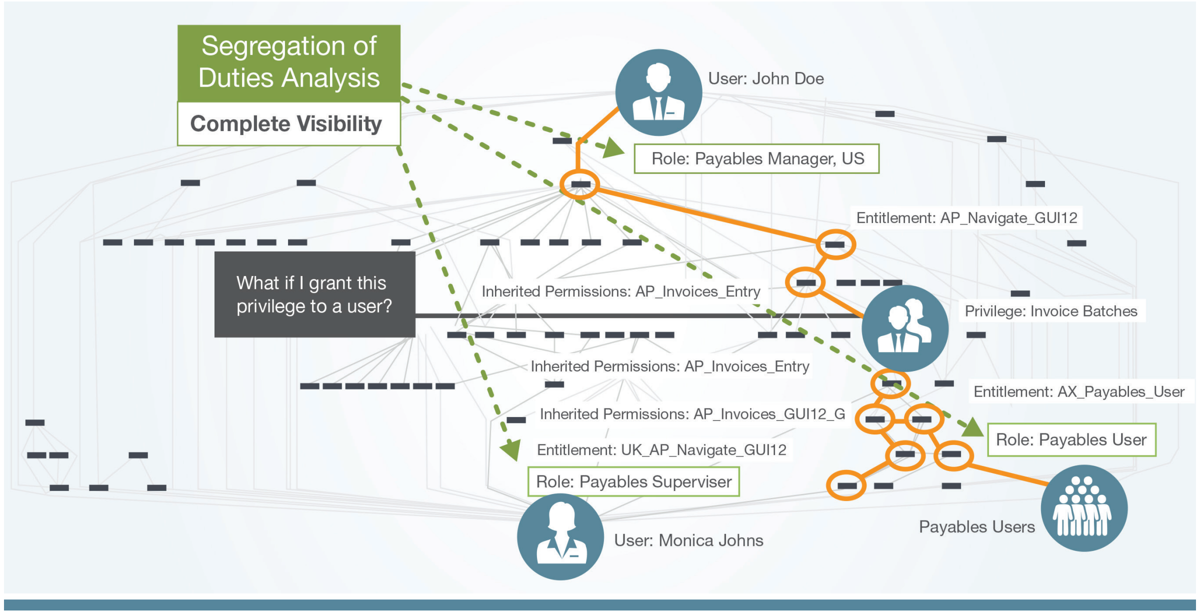
Fine-Grained Identity Governance and Administration

Effective enterprise access controls require fine-grained enterprise Identity Governance and Administration (IGA) to manage user privileges in enterprise applications that enable significant business processes, manage sensitive data, and report critical information for decision support. Unlike the traditional Identity and Access Management (IAM) and IT Service Management (ITSM) tools that manage user access requests at the "groups" or roles level in a software system, fine-grained IGA manages users access requests for enterprise applications and data at the "privilege" level to perform functions on that data, as shown below:

Traditional IAM



IAM with Fine Grained IGA



Segregation of
Duties Analysis
Complete Visibility
User: John Doe
Role: Payables Manager, US
Entitlement: AP_Navigate_GUI12
What if I grant this
privilege to a user?
Inherited Permissions: AP_Invoices_Entry
Privilege: Invoice Batches
Inherited Permissions: AP_Invoices_Entry
Entitlement: AX_Payables_User
Inherited Permissions: AP_Invoices_GUI12_G
Role: Payables User
Entitlement: UK_AP_Navigate_GUI12
Role: Payables Superviser
Payables Users
User: Monica Johns

CISOs and IT security leaders accountable for enterprise IAM should consider integrating fine-grained application access controls in the IDM and ITSM systems used to provision users in enterprise applications. Fine-grained identity governance is required to prevent security threats, and streamline operations to mitigate inherent risks in thousands of available privileges in enterprise applications.

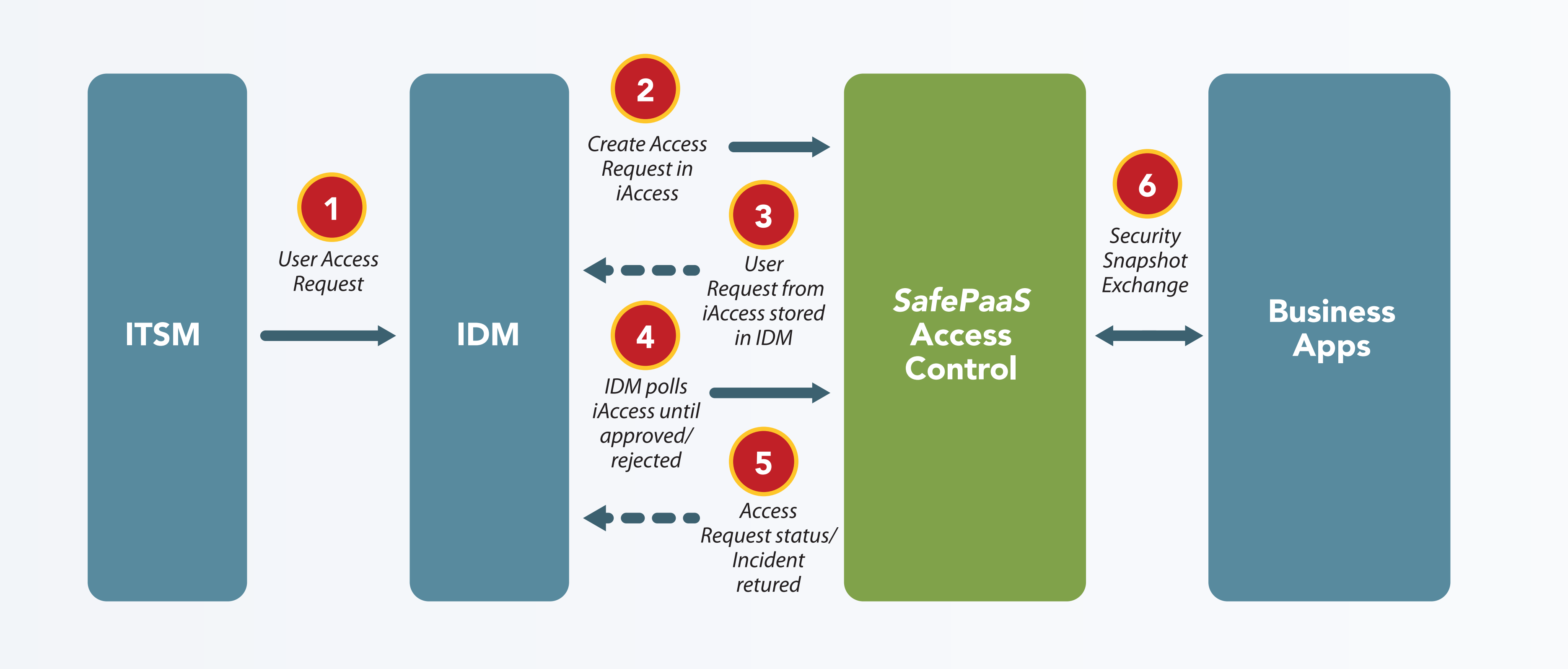
Access Control Capabilities for ID Governance & Administration

An Effective Identity Governance and Administration platform must manage all application access controls by monitoring privileges granted to user and role life cycles across multiple systems. The core IGA capabilities provide access controls management to automate provisioning of user accounts among heterogeneous systems, fulfil self-service access requests, enable password policy management, enable governance over user access to target systems via policy based automated workflows, and manage access certification processes. Access Control over enterprise applications must be able to rate risk in user access requests by applying intelligent rules logic based on a user's combined entitlements, segregation of duties enforcement policies, and inherent role risks. Security and Audit Managers should be able to use advanced analytics for role mining and audit incident management to maintain evidence of access controls effectiveness. The following criteria should be considered in IGA platform selection:

- **Access Policy Management:** Ability to establish effective access controls over critical enterprise applications by configuring policies in terms of the most granular attribute within the application security model that can be granted to a user through a role assignment, while filtering any over-riding attributes that may generate false positives.
- **Enterprise Security Modeling:** Ability to extract, translate and load (ETL) enterprise level security model for critical business applications that execute significant business processes such as record-to-report, procure-to-pay, order-to-cash, hire-to-retire, etc.
- **Continuous Access Monitoring:** Ability to test all user provisioning requests by applying the fine-grained access rules against the enterprise application security model to identify violations and report to requester, reviewer(s) and approver(s) roles in the request workflow.
- **API Services for IDM and ITSM Workflow:** Ability to extend, augment or replace self-service user request initiated in IDM and ITSM workflows with multilevel approval management that includes real-time fine-grained violation analysis.
- **Risk Mitigation:** Ability to assign corrective actions where the risk is above the acceptable access risk or assign one or more compensating control(s) where a business constraint requires waiver to the access risk in the application privilege requested by the user
- **Roles Management:** Ability to ensure that the roles catalog defined in IDM, ITSM and enterprise application do not contain inherent risk due to conflicting privileges. Ensure that all changes to roles due to change in business process or technical updates do not introduce inherent access risks.

Access Governance Options for Identity Management

There are several options to consider when enabling access controls for Identity Governance and Administration (IGA) based on the web-services supported by enterprise applications and IDM/ITSM systems. The optimal solution should provide real time fine-grained violation analysis to prevent user security risks in centralized authentication, single sign-on (SSO), session management and privilege authorization for enterprise applications. The Access controls engine should include multi-platform options to control enterprise application access in modern cloud applications as well as traditional on-premises applications accessed via web browsers or client-server architecture. Access control API services should allow multi-level workflow message integration options for on-premises, native cloud or hybrid cloud IDM systems where the user security request is initiated. Increasingly, enterprise applications also require access control options to include smart or constrained devices with or without human operators and IoT applications


ITSM
1
User Access Request
IDM
2
Create Access Request in iAccess
3
User Request from iAccess stored in IDM
4
IDM polls iAccess until approved/ rejected
5
Access Request status/ Incident retured
SafePaaS Access Control
6
Security Snapshot Exchange
Business Apps

Conclusion

An Identity Governance and Administration (IGA) platform enables organizations to mitigate cyber threats that make their way inside to attack the heart of the enterprise. CISOs can deploy advanced application access controls to prevent cyber threats and ensure that user access to enterprise data and process complies with company policies and regulatory mandates. Advanced application access controls can manage user access requests, roles design, and entitlement configurations by detecting as well as preventing access risks based on fine-grained rules logic. Fine-grained access rules can be configured in the IGA platform that supports meta-data for the enterprise wide application security model.

Identity and Access Management (IAM) tools do not meet enterprise application access governance needs because:

- Inability to configure access rules in terms of fine-grained privileges in the enterprise application security model.
- IAM focuses on "birthright" access for all user rights, whereas IGA requires risk management for enterprise access users with hundreds of privileges to sensitive data, transactions, and functions.
- Lack of support for short-lived, just-in-time elevated access required for emergency support – privileged access management (PAM). The life cycle between regular access and privileged access is just not the same.
- Single Sign-on to business applications for "birthright" users do not control provisioning fined-grained privileges that violate company policies such as Segregation-of-Duties or Data Privacy.
- IAM tools do not monitor or manage user activity in enterprise applications required for "lookback" analysis when a risk is materialized.
- Unable to support business process owner and control owner need to certify user access or activity log to support periodic access certification.
- IAM tools do not support security and application administrators needs to maintain role design and update entitlement to remediate inherent risks in thousands of privileges available in enterprise applications.

CISOs and risk management leaders responsible for identity and access management should evaluate critical capabilities during IGA platform selection. An effective IGA tool should help organizations provide secure, privileged access to critical assets and meet compliance requirements by securing, managing, and monitoring fine-grained privileges in user access requests across all enterprise applications in scope for compliance.

To learn more about Enterprise Access Controls contact:

✉ Emma.kelly@safepaas.com
C https://www.safepaas.com/contact
W https://www.safepaas.com/

SafePaaS™