

WHITE PAPER

# A HOLISTIC APPROACH TO MANAGING RISK AND ADDRESSING COMPLIANCE IN CRITICAL APPLICATIONS



# CONTENTS

page 03 INTRODUCTION

page 04 RISE OF CRITICAL APPLICATIONS IN THE CLOUD

THE HOLISTIC APPROACH

page 05 SOD ANALYSIS AND REMEDIATION

page 06 EMERGENCY ACCESS MANAGEMENT

TRANSACTION MONITORING

CONFIGURATION AND SECURITY CONTROLS MONITORING

page 07 RISK-BASED ACCESS REVIEW

ROLE DESIGN AND MANAGEMENT

page 08 COMPLIANT PROVISIONING

CONCLUSION

# INTRODUCTION

Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Supply Chain Management (SCM) and Human Capital Management (HCM) applications provide organizations with the ability to seamlessly integrate their most business-critical operations. These applications manage an organization's most critical processes and contain sensitive information. Continuous availability and integrity of such applications are vital to the successful execution of a company's core business and for its employee's ability to perform their day-to-day operations. If these applications are compromised due to badly designed and ineffective security controls, the impact can be catastrophic. Organizations aren't merely at risk for failing to meet regulatory and compliance requirements, but they risk undermining the trust of their employees, shareholders and ultimately their very existence (as was the case for many companies at the beginning of the century). Costs to recover from data breaches, fraudulent activities and reputational damage can be significant.

*Applications with complex authorization models are among the most common places where frauds are hidden. It remains difficult to analyze these applications for access, Segregation of Duties (SOD) and other policy violations without specialized software.*

Adequately assessing risk, as well as designing and operating effective controls within an ever changing and expanding threat landscape, is a challenge for most organizations. In a recent survey, it was found that almost 75% of fraud committed of over \$1M or more had some internal involvement; weak internal controls were the main contributor towards the facilitation of the fraud. One of the most critical areas within the various domains of information security has been and will continue to be access controls. As companies continue to struggle with it, the key contributor to these organizations' ineffectual grasp of implementing adequate access controls is the lack of unified access governance, as well as the use of point solutions to solve every problem in the organization. The left arm is doing one thing and the right arm is doing something else and when something goes awry, both arms are there pointing at the other as the guilty party. In result, companies fail to have a strong unified and centralized access governance program.

*Occupational fraud is a problem that costs the typical organization about 5% of revenue (according to Association of Certified Fraud Examiners [ACFE]).*

The use of manual, spreadsheet-based controls are ineffective. Manual spreadsheet controls as it pertains to adequately assessing sensitive access and Segregation of Duties (SOD) consistently break down. Point solutions for every ERP in the enterprise is very expensive and highly ineffective in achieving a centralized access governance program. For example, a company has something effective for SAP but it doesn't integrate with Workday. Similarly, one may have something effective for Oracle EBS but can't implement those controls to ensure Segregation of Duties across Salesforce or Hyperion. Buying solutions for every application in your enterprise becomes rather costly.

Further, the coordination of efforts for those managing the point solutions for all the different applications and systems is disjointed. There will be no unified access governance program, platform or approach for ensuring the organization is secure and access controls are operating effectively. Network security professionals may relate; the only solution that makes sense today is the unified threat management.

Why buy separate antivirus, anti-spyware, anti-spam, network firewalling, web app firewalling, IDS and IDP, content filtering and leak prevention technologies when you can get them in one appliance managed and supported by the same company? This is true in the case of access governance as well, and you will find a solution in subsequent sections of this paper.

## RISE OF CRITICAL APPLICATIONS IN THE CLOUD

The most significant game changer for business-critical applications in the past five years has been heavy adoption of Software-as-a-Service (SaaS) aka “Cloud.” Gartner predicts that by 2019, approximately 28% of installed HRMS systems globally will be SaaS-based, up from 13% in 2014. The prediction extends to convey that, by 2020, about a quarter of organizations in emerging regions will run their core CRM systems in the cloud, up from around 10% in 2012. The most popular SaaS applications used worldwide today are Workday, Salesforce, SAP HANA and Oracle ERP Cloud. The larger SaaS data solutions include SharePoint, Box, Google Drive, Office 365 and Dropbox. The larger Infrastructure-as-a-Service (IaaS) solutions include AWS, Azure, Google Cloud Platform and Oracle. Any organization most likely utilizes at least two of these. However, how many access governance solutions need to be maintained for these solutions? Most cloud providers themselves can’t even provide comprehensive access governance for their own solution and only address certain aspects of what is required.

## THE HOLISTIC APPROACH

Automated solutions that provide organizations with the means to analyze and manage risks associated with SoD conflicts, sensitive access and other types of policy violations for applications with complex, role-based authorization models and multi-level hierarchical entitlements are essential. These solutions will enable companies to nearly eliminate SOD conflicts and meet increased audit and regulatory requirements. Gartner estimates that in 2015, only 30% of companies with complex business applications requiring enforcement of SOD controls made use of automated SOD controls monitoring solutions. But by 2019, it is estimated this number will grow to 50%. The reason being that no matter what manual controls a company implements, it could take one exception for the auditor to cite a deficiency. If the same exceptions keep occurring, that deficiency soon becomes a significant deficiency; if the failures are significant enough, those failures can become a material weakness.

Many enterprises have adopted Saviynt Application Access Governance that simplifies Application Governance Risk and Compliance (GRC), as well as brings together security management of critical applications into a single platform, such as:

- On-premises ERP applications: SAP, Oracle eBusiness Suite (EBS), Oracle PeopleSoft, Oracle JD Edwards, Microsoft Dynamics GP (Great Plains)
- Cloud ERP applications: SAP HANA Cloud Platform, Oracle ERP Cloud, Workday, NetSuite, Salesforce, etc.
- Healthcare applications: Epic, Cerner, McKesson, MEDITECH, GE, etc.

### *Saviynt Application Access Governance*

*Saviynt Application Access Governance is based on a cloud-architected, Next-Generation Identity Governance and Administration (IGA 2.0) platform. The solution is strongly risk-aware, empowered by Intelligence and Analytics. Its availability as a cloud offering, enabling enterprises with minimal Total Cost of Operation (TCO) and high implementation agility.*

## **SOD ANALYSIS AND REMEDIATION**

Saviynt's platform offers out-of-the-box rulesets that analyze SOD risks across key financial, supply chain and human capital management processes. Entitlement hierarchies are included that show role relationships to entitlement permissions. The rulesets have been specifically designed to analyze access to ERP-specific permissions. The solution can also consume rulesets for applications the organization may have developed in-house. Rules are mapped to various industry regulations such as PCI-DSS, NIST, ISO, HIPAA and CoBIT.

*SOD is an essential control over financial and other sensitive transactions to combat internal fraud (see Note 1). For example, it is a typical interpretation of Section 404 of the Sarbanes-Oxley Act in the U.S. not only to require SOD controls for financial transactions and reporting, but also to require ongoing monitoring and validation of such controls.*

Another salient feature is that Saviynt isn't confined to two-way SOD relationships. The solution can provide up to five functions to analyze for analysis and ruleset definitions and can accommodate complex SOD analysis that require AND, OR, and NOT conditions. It is also capable to analyze SOD violations that may exist across-applications and provide integrated usage analytics and transaction monitoring. The solution provides relevant insights such as SOD violations that are potential risks and which of those risks have been violated. Before provisioning roles to users, Saviynt simulates access and can provide "what-if" scenarios to help ensure provisioning access does not cause violations. If violations exist, the system also generates automatic remediation recommendations. The solution also provides integrated mitigating controls management for SOD violations that need to be accepted based on business reasons.

## EMERGENCY ACCESS MANAGEMENT

Privileged Access Management keeps the organization safe from accidental or deliberate misuse of privileged access. One of the core concerns of auditors in today's regulatory environment is the use of Privileged IDs. Shared privileged accounts tend to violate the principle of least privilege and SOD. Moreover, the risk increases as the password can be "leaky" as it has more than one owner. Therefore, a shared account provides limited or no accountability.

One of the key benefits of using Saviynt is that companies can manage emergency, break-glass procedures to provide time-bound, privileged access on demand without having to add yet another point solution to satisfy their requirements. Additionally, with Saviynt's in-depth ERP expertise (i.e. when privileged access is granted), Saviynt can provide visibility into transacted activities to provide assurance that nothing inappropriate was transacted, as well as alert control owners in case of failure so that process is not reactive and evaluated months later. The solution can perform behavior-based anomaly detection, leveraging user behavior analytics while the privileged ID is being accessed. While the Integrated workflow exists for privileged access requests and approvals, multiple levels of approvals can be implemented before privileged IDs are provisioned.

## TRANSACTION MONITORING

Data analytics have been a key component to assessing fraud risk in organizations for decades. The problem has been that these analytical assessments took place months, quarters or even years after the transactions occurred. Saviynt's library of analytics can be monitored as these transactions take place and can provide alerts to the process owners of anomalies as they occur in real time. Transactions can also be mined to provide valuable business intelligence. The capabilities for Saviynt to provide business-relevant insight is customizable and isn't limited to those analytics that come out-of-the-box.

Saviynt mines transactions and master data to discover suspicious activities that may be difficult to otherwise discover (e.g., duplicate payments to the same vendor, payments for more than the purchase order or contract amount, sequential invoices from the same vendor or vendors with addresses identical to employees). Saviynt provides transaction analytics for Vendors and AP, General Ledger, Sales, Procurement, as well as many others.

## CONFIGURATION & SECURITY CONTROLS MONITORING

Saviynt provides a framework with out-of-the-box controls to meet different compliance mandates, as well as rich analytics dashboards with security controls that includes configuration monitoring to identify potential security risks in critical applications as they occur in real time. There are over 150 out-of-the-box IT General Controls that include access, passwords, usage and many others. Saviynt



can automate the import of key application security configurations (e.g. 3-Way Match), for any application. It also provides for the ability to set up whitelists and take relevant 'action' on specific controls (e.g. quarantine files uploaded from Salesforce that contain credit card numbers). Organizations also can define or request their own controls in which to monitor.

## RISK-BASED ACCESS REVIEW

Saviynt allows full automation of access certification processes (e.g., scheduling certifications, detecting policy violations, reporting on the status of ongoing certifications, archiving previous certification data, and revocation of excessive access rights).

To avoid uncovering issues with excessive or unauthorized access during the certification process, Saviynt supports event-based certifications that are triggered due to changes in user attributes (e.g., department transfers, role changes, long absence, etc.).

By supporting micro-certifications and limiting the certification scope, Saviynt enables organizations to increase efficiency and reduce rubber stamping. During access review, Saviynt consumes audit and usage logs from managed systems to further drive intelligence and to provide insight into how often access was requested by the user.

## ROLE DESIGN AND MANAGEMENT

Role-Based Access Controls (RBAC) provide the ability to increase efficiency, reduce costs, and meet compliance requirements. However, organizations have struggled over the years to leverage the potential of a role-based framework.

Saviynt offers a comprehensive solution that combines top-down and bottom-up techniques and has the unique ability to define roles according to business functions. This ensures effective SOD validation by identifying the permissions that fall outside the role framework and applying those controls for exception access. The solution offers techniques to ensure that roles are accurate by incorporating usage analysis and impact analysis, maintaining history, and versioning a fully integrated workbench to formalize and manage roles.

The solution enables organizations to strike the right balance between RBAC and ABAC for provisioning access. Saviynt utilizes this hybrid approach where a user's HR attributes and usage information are factored in while designing roles. It further extends the traditional RBAC model with rule mining to create rules for dynamic assignment based on attributes.

## COMPLIANT PROVISIONING

When designing roles, Saviynt helps internal security teams and auditors to define SOD rules, determine SOD conflicts, monitor critical transactions, and remediate violations by using an intuitive approach where a user's HR attributes and usage information are factored in. It further extends the traditional RBAC model with rule mining to create rules for dynamic assignment based on attributes.

After the data is ingested, organizations can drive automated provisioning-based roles on Attribute-Based Access Control (ABAC)/Role-Based Access Control (RBAC) policies. Users can add or remove granular access, modify attributes, and change passwords through an intuitive web or mobile interface.

Organizations can further automate lifecycle management processes as employees change jobs, locations, and/or roles (i.e., when an employee is transferred); Saviynt detects the change from an authoritative source, initiates access review and re-evaluates access rules. Similarly, when an employee is terminated, the solution triggers the account/access clean-up immediately. The solution also provides managers the option to disable all user accounts with a click of a button.

### Conclusion

*Organizations are going through significant transformation and revamping their application portfolio to meet the current business needs and to stay ahead of the competition. At the same time, the regulatory environment is constantly changing and the need for continuous compliance is imminent now more than ever. Organizations would benefit from taking an integrated approach by incorporating all crown jewel applications and move towards a unified platform to address risk management and fraud prevention.*



## LEARN MORE

### FIND OUT!

Why Saviynt received the highest product score for Midsize or Large Enterprise and Governance-Focused use cases in Gartner's 2018 Critical Capabilities for Identity Governance and Administration.

### CONTACT US

[info@saviynt.com](mailto:info@saviynt.com)

### START A FREE TRIAL

Saviynt's Enterprise Solution

### TRY A DEMO

Saviynt IGA Platform

## ABOUT SAVIYNT

Saviynt is a leading provider of next generation **Identity Governance and Administration solution for Data, Infrastructure and Critical Applications in the Cloud and Enterprise**. Saviynt combines traditional IGA features with advanced usage analytics, data or infrastructure access governance, behavior analytics, real-time threat detection and compliance controls to secure organization's critical assets.