www.pwc.com/oracle

September 2011

Minimum access, maximum SOD validation

How an integrated, automated segregation of duties solution can reduce risk and enhance compliance

Managing risk isn't getting any easier. Expanding government regulations, new anti-corruption laws, and sweeping reforms in the healthcare and financial industries have combined to make risk management more complex—and more compulsory—than ever

Today organizations struggle to comply with an avalanche of global mandates that include the US Sarbanes-Oxley (SOX) Act, as well as similar regulations as mandated by European and Japanese statutes. Many companies also must comply with regulations that include the Gramm-Leach-Bliley Act, Basel II, Payment Card Industry Data Security Standard, the Health Insurance Portability and Accountability Act (HIPAA), and the Foreign Corrupt Practices Act.

Appropriate, up-to-date user entitlements and segregation of duties (SOD) controls for corporate applications and data are critical to complying with these mandates. Yet many companies still employ manual methods to audit user access and implement controls, an approach that is time-consuming, costly, and—all too often—inaccurate. Even among organizations that have deployed automated solutions, the runaway complexity of IT infrastructure and the proliferation of applications combine to make monitoring and enforcing controls a daunting challenge.

And it comes at great cost. A Ponemon Institute study of 46 multinational organizations found that the average cost of compliance is $3.5 million a year.[1] The high price of compliance is due, in part, to the use of ineffective manual processes that involve too many people for segregation of duties reporting and exception management.

Many organizations are now turning to automated solutions to boost the efficiency and accuracy of compliance efforts. Governance, Risk, and Compliance (GRC) suites and Identity and Access Management (IAM) solutions are being widely seen as a means to improve compliance and manage risks.

[1] Ponemon Institute, The True Cost of Compliance, January 2011

GRC is a broad-based concept that delivers a consolidated view of compliance, risk, and internal controls across the enterprise. GRC suites typically provide a central repository and workflow capabilities to document business policies, risks, and controls—and help avoid overlaps, conflicts, and gaps. They also often include some level of built-in tools for monitoring and validation of SOD. GRC suites have typically been employed to manage this risk on the most sensitive business applications, including Enterprise Resource Planning (ERP) systems, making it possible to use the capabilities built into the GRC solutions for role-based SOD validation.

When compared with GRC, IAM solutions have a more straightforward mission: They administer user access privileges across a company's resources throughout an employee's tenure. IAM creates a central source of identity data that ensures user access rights to enterprise data and applications are appropriate, up to date, and in compliance. Identity management systems also create an audit trail for access privileges to regulated data.

GRC systems are designed to integrate the management of financial, operational, and IT risks. A foundational first step in an effective GRC strategy is integration of GRC and IAM systems. Forward-thinking organizations are beginning to embrace this approach a means to deliver more robust and seamless segregation of duties validation. When GRC and IAM are integrated, SOD capabilities are no longer isolated within the ERP application, enabling organizations to proactively assess SOD during the creation of access privileges and accounts, incorporate SOD monitoring into user access reviews, and monitor for SOD violations across business functions for the entire enterprise. In other words, segregation of duties management and validation extends to all points of access within all business applications.

SOD rises to the top of compliance concerns

In today's risk-intensive business environment, many organizations are enhancing their commitment to effective access control management by focusing on segregation of duties (also known as separation of duties) to help ensure compliance and prevent fraud.

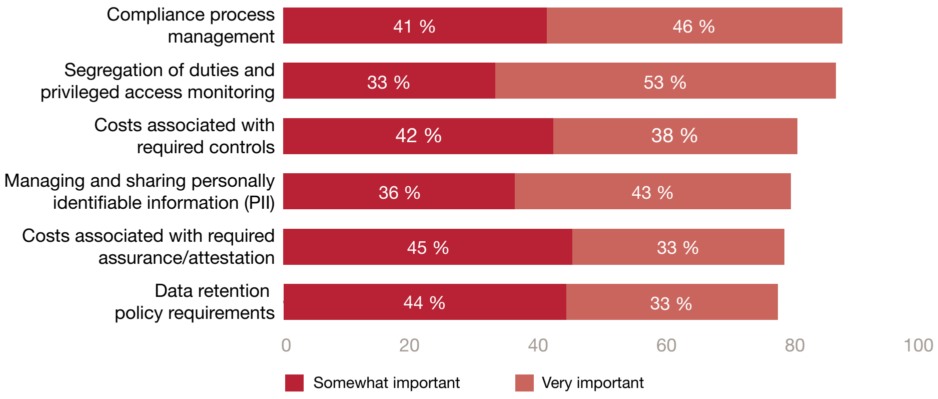
A recent survey by ISACA found that 53% of IT, security, and audit and assurance managers polled ranked segregation of duties and privileged access monitoring as "very important," putting it at the top of regulatory compliance concerns for the year.[2] (See Figure 1.)

Segregation of duties, simply put, requires more than one person to complete a task. In essence, SOD applies checks and balances to the activities of individuals. A basic tenet of SOD is that the employee (user) should not have access that entitles him or her to perform more than one function that could expose the organization to increased risk via errors or fraud.

The classic example of SOD: An employee who approves payments should never be allowed to issue them. The scope of segregation of duties is not limited to financial functions, however. In the IT department, for instance, a software programmer who has the authority to create code should not have authorization to move that code into production. Proper SOD calls for another employee to verify that the code is functional and not malicious before it goes live.

SOD is a critical component of compliance programs because organizations must be able to prove that anyone—employees, contractors, vendors, and suppliers—who has privileged access to their systems cannot use that access for malicious or fraudulent purposes. Since the enactment of SOX, compliance-sensitive organizations have developed comprehensive controls that require periodic validation of user access entitlements. They also have designed policies to ensure compliance with SOD controls and implemented mitigating controls to accommodate situations in which SOD conflicts cannot be avoided.

Figure 1: Regulatory compliance importance



Source: ISACA

[2] ISACA, Top Business/Technology Issues Survey Results, April 2011

Why manual SOD validation is disruptive—and often inaccurate

Despite advances in SOD validation technology, the processes for monitoring controls, managing exceptions, and implementing mitigating controls remains a largely manual exercise that is typically achieved via spreadsheets, e-mail, and human teamwork. This manual assessment, which compares all system users' access entitlements against identified "toxic" combinations of system access, is an arduous, resource-intensive process.

The review is typically carried out by IT employees, with the assistance of business-aligned support staff, who often lack expertise in SOD. They are required to develop reports, identify the appropriate manager for review, collect the responses, answer questions, and resolve issues raised by reviewers. They must then follow up on missing or delayed items and generate overall summaries of the report.

Managers and supervisors must review reports of any user access that presents an elevated risk or requires an exception. Circumstances that trigger an exception include resource constraints, employee vacations and leaves of absence, and gaps in skills of available staff. Exceptions must be evaluated from a risk perspective and mitigating controls must be identified before an exception can be allowed.

And it doesn't end there. After receiving feedback from managers, the review team begins the process of exception management, remediation, and root-cause analysis. New processes to sustain the mitigating controls must be developed and time-bound exceptions must be tracked.

A manual SOD review process drains the productivity of application owners, employees responsible for generating and distributing the reports, and managers and supervisors who must approve them. Hundreds of man-hours are squandered on generation and analysis of data, and managers must set aside their day-to-day responsibilities to perform the review and manage exceptions.

Given the unsystematic nature of the SOD validation process, it's not surprising that organizations report that review results are often unreliable. Any manual process introduces opportunity for human error, including inaccuracies and omissions. What's more, managers and supervisors often do not understand the technical wording and nondescript values associated with segregation of duties. And in the era of doing more with less, they are likely to be time-constrained and may not diligently follow up on questions or concerns.

Even organizations that implement an effective manual program often fail to maintain and update SOD processes and policies. And that's a mistake, because issues and processes evolve quickly, and the organization's SOD validation program must be continuously updated to ensure compliance and avoid risk.

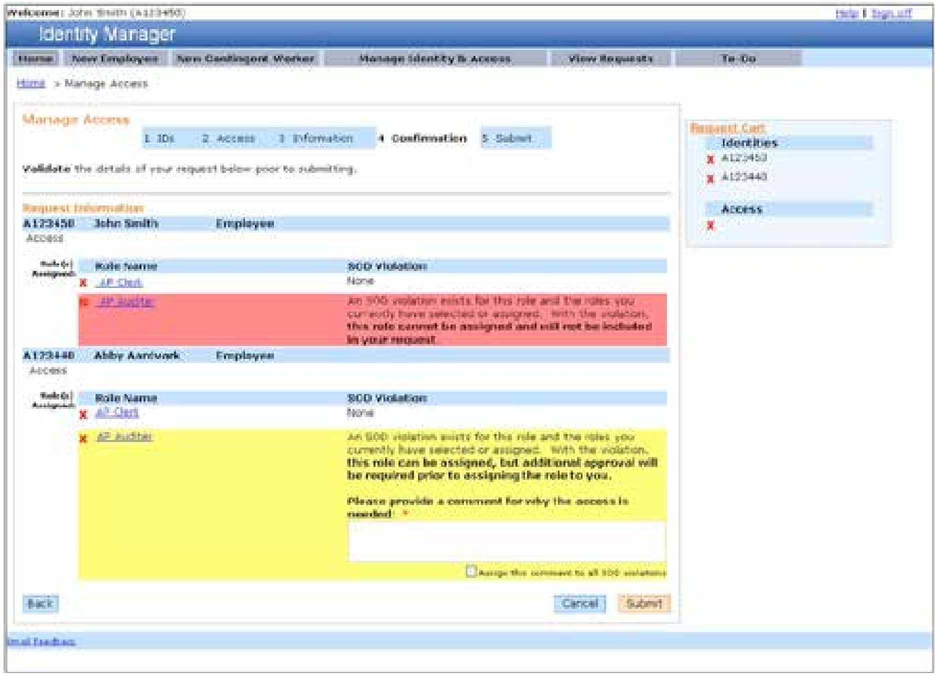
The current state of SOD reporting, validation, and exception management presents a Sisyphean challenge for a typical organization. In our experience, it is costly and disruptive to ongoing operations, and the results of reviews are often inaccurate and can increase risk to the business.

The case for convergence of enterprise solutions

Identity management and GRC solutions are evolving to a state of sensible, if somewhat clumsy, convergence. We believe the intersection of the two is logical since many governance and audit processes, including entitlement management, are based on identity and access management.

Vendors are beginning to offer end-to-end solutions that blend identity management functions with GRC-related features to support more powerful, centralized controls for access management, review processes, and SOD validation.

Figure 2: Segregation of duties capabilities are now integrated into some IAM tools.



Welcome: John Smith (A123450)

Identity Manager

Validate the details of your request below prior to submitting.

Request Information

A123450 John Smith Employee

Access

Role(s) Assigned: Role Name	SOD Violation
AP Clerk	None
AP Auditor	An SOD violation exists for this role and the roles you currently have selected or assigned. With the violation, **this role cannot be assigned and will not be included in your request**

A123440 Abby Aardvark Employee

Access

Role(s) Assigned: Role Name	SOD Violation
AP Clerk	None
AP Auditor	An SOD violation exists for this role and the roles you currently have selected or assigned. With the violation, **this role can be assigned, but additional approval will be required prior to assigning the role to you.** **Please provide a comment for why the access is needed:** *

□ Assign this comment to all SOD violations

These integrated solutions are built upon a centralized repository of entitlements and controls that can deliver enterprise-wide visibility into security and compliance management, and eliminate unnecessary costs that occur when different business units separately track and manage a single risk factor. Consequently, they can reduce the cost of managing access control and ensuring compliance while enhancing business efficiencies and security policies. What's more, integration of GRC suites with IAM systems eliminates information silos and provides a common user interface across the enterprise.

Organizations can further strengthen their compliance initiatives by leveraging SOD monitoring tools for systems beyond their ERP systems via the GRC suite. By housing enterprise SOD validation within the centralized repository for entitlements and controls, the organization can create a SOD validation system that is more accurate, efficient, and cost-effective.

SOD validation also will become cohesive across business units. In most organizations, there is no unified approach to validating, monitoring, and reporting of segregation of duties, and most businesses do not combine the validation they perform during IAM user access reviews with SOD management. The lack of integration is a technical, a process and people issue, since companies often appoint multiple compliance teams across departments to manage SOD.

This inconsistent, decentralized approach results in an ill-defined strategy because segregation of duties is valued and managed differently by disparate business units. Every department has a different priority in managing risk, and elevated user access or the ability to perform multiple roles is not consistently monitored across business units. IT risk leaders, for instance, may have a very different view of SOD when compared with that of IT security teams. Similarly, the chief compliance officer will focus on ensuring that the organization's controls and audit capabilities comply with necessary regulatory mandates across the entire organization, rather than a single division.

Moving from manual to integrated solutions

PwC believes that the increasing complexity and diversity of IT business applications demand that segregation of duties validation be automated to effectively report, validate, and manage SOD. Yet, in our experience, we have seen that few organizations have adequate visibility into user access entitlements and SOD controls across applications and business divisions to design and deploy truly effective automated solutions.

To do so, we believe that organizations must evaluate their entire technology ecosystem and develop a strategy to eliminate silos of applications and information on user entitlements. Effective SOD validation requires that organizations have a precise understanding of individual application permissions and how those permissions, when combined for a single user, constitute a risk.

The key to effectively creating an automated SOD tool lies in policy-driven technology that can be seamlessly integrated with the organization's identity management and GRC systems. We believe that CIOs must take the lead in developing a comprehensive SOD roadmap that eliminates silos of information and integrates applications across the enterprise.

First, organizations must take a step back and carefully assess how existing technology and compliance programs manage separation of duties. The CIO must work with the CSO and business leaders to develop a strategy that incorporates the correct level of controls, SOD rules, and appropriate policies across applications.

Once a strategy is in place, IT leaders should determine the enterprise's current maturity of technology for identity and access management and SOD automation, as well as its ability to support the advances in the integration of the two technology stacks. To better ensure security and compliance, an integrated solution dictates that all user accounts reside into a single, common directory in order to enable proactive, continuous monitoring of access based on real-time data.

To be truly effective, we believe these integrated solutions must enable role management with fine-grained SOD capabilities that allow the organization to define specific access controls for users based on attributes of the user, the resource, and the context of the access request. We have helped organizations design controls that prevent potentially perilous combinations of access entitlements and create controls that track employee roles over time to identify job changes that may result in excessive access privileges. These automated SOD solutions also must track and log every action a user performs while logged on with privileged access; they must also report failed log-on attempts, a proven indicator of attempted misuse of resources.

Furthermore, we believe that organizations must design effective SOD controls that can pre-emptively block assignment of roles or responsibilities that would violate proper segregation of duties. Over the past few years we have seen leading vendors of SOD tools enable this capability by providing a library of thousands of best-practice controls and rules to identify, remediate, and mitigate risks. These best practices ensure accuracy by describing access and violations in nontechnical language that is easily understood by managers and supervisors. The tools provide automated simulation and remediation that enables the security team to preview the effects of a remediation in order to make the best decisions.

When effective automated reporting and management tools are deployed, we have routinely seen organizations eliminate much of the potential for human error. Reporting and validation of access is automated, and reports are generated and distributed with minimal manual intervention, significantly reducing cost and business disruption. The tools track and aggregate reviewer feedback using Web-based user interfaces that obviate the need for spreadsheets and e-mail.

While designing a comprehensive SOD management tool is not an uncomplicated project, when done correctly it enables organizations to significantly reduce the burden of reviewing SOD controls for compliance and provides a real-time view into the business's risk situation. Cost benefits are realized by an automated review process that involves fewer people and reduces the disruption to managers and supervisors. And increased accuracy helps ensure better control compliance while providing an audit trail for all privileged access users.

Automating SOD Analysis and Remediation with Oracle's Applications Access Control Governor

AACG alleviates the cost and inaccuracy of manually managing and maintaining users' access to ERP applications. AACG includes a delivered library of hundreds of application access policies. In addition, new policies can be easily configured and added to the library for deployment across multiple ERP instances. AACG automates the detection of SOD conflicts at a granular level of detail beginning with users and roles through menus and functions (or in the case of PeopleSoft, pages and permission lists).

A visual analysis traverses users application security and identifies access paths that have the potential of resulting in transactions with SOD violations. Security Administrators simulate the changes to a user's role, menu or submenu access and can test the results before deploying to operations. Furthermore, AACG provides the multi-user workflow and remediation tracking to audit where SOD violations have occurred and what steps have been taken to resolve them.

AACG can either be deployed as a standalone GRC application or rolled out as part of the GRC Controls Suite, including Enterprise Transaction Controls Governor for monitoring potential transactions as compensating controls to AACG security policies.

AACG also can be part of the user provisioning process. When new users are granted user and role access to an application, AACG can operate as a fine-grain user access provisioning engine, identifying SOD conflicts at the menu, submenu and function levels.

Automating SOD analysis and remediation results in a much faster and accurate assessment of SOD conflicts than can be achieved with manual steps.

Sustaining Compliance with Oracle Identity Governance

Organizations need to ensure users have sufficient access privileges to perform their job functions, but for compliance and security reasons it's also important to constrain such access. Accordingly, enterprises must make it easy for users to acquire access, and also easy for managers, resource owners, and system administrators to automatically review and revoke access. By streamlining the management of user identities and access rights, automating enforcement of SOD policies, and automating time-consuming audits and reports, Oracle Identity Governance solutions can help support strong security policies across the enterprise, while reducing the overall cost of compliance.

Oracle Identity Governance which includes solutions for user provisioning, identity governance, and privileged account management is a closed loop governance platform. By linking provisioning and auditing at the business role level, Oracle Identity Governance solutions can prevent, detect, and resolve access rights conflicts to reduce the likelihood that individuals can act in a fraudulent or negligent manner. It can further automatically detect violations and initiate the notification and remediation steps, based on corporate policies.

"By delivering a comprehensive platform for access request, role lifecycle management, access certification, segregation of duties, closed loop remediation and privileged account management, Oracle delivers an integrated Identity Governance solution set that enables organizations to efficiently balance the objectives of access, security, and compliance, while reducing total cost of ownership."

Chris Leone—Oracle Senior Vice President, Applications Development

How PwC can help

In today's heightened compliance and regulatory environment, segregation of duties matters more than ever. Fraud, compliance violations, and theft of sensitive data are just a few of the potential negative impacts of an ineffective SOD strategy.

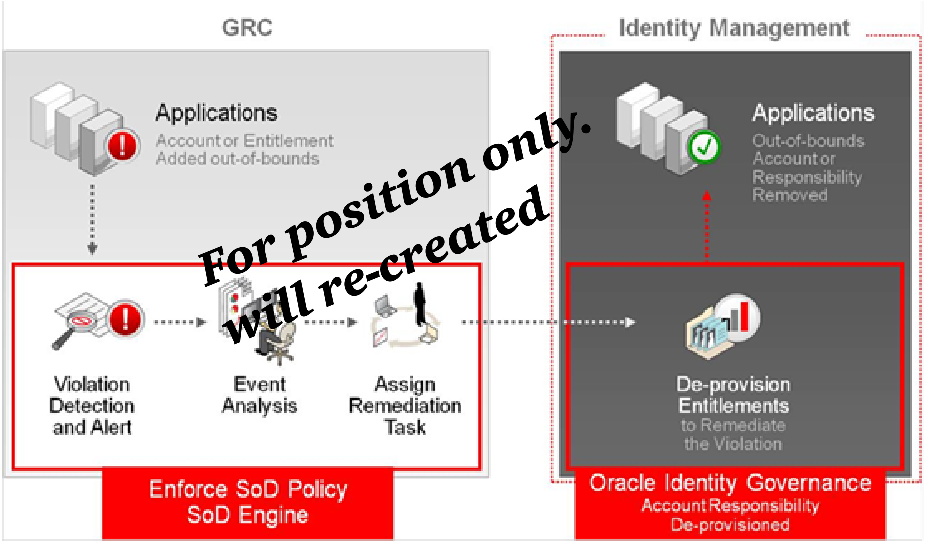
Implementation of an automated segregation of duties system requires that key stakeholders take a step back and carefully assess current roles, responsibilities, and access entitlements across the business. Only then can they design a holistic approach, based on proactive and preventative controls, to manage, monitor, and report segregation of duties violations.

Given the proliferation of IT systems, applications, and processes across the enterprise, that's no easy task. An automated SOD solution requires expertise in designing effective SOD controls, integrating technology stacks across the enterprise, and understanding compliance requirements and processes.

That's where PwC can help. We can assist you in transforming your manual segregation of duties program into an automated system that is streamlined, accurate, and cost effective. We have extensive knowledge and expertise in helping a wide variety of companies—across industries and around the globe—reduce risk and achieve compliance. Drawing upon our expertise in access management and role engineering, our team of professionals can design and implement a segregation of duties framework that fully meets your business needs. Leveraging our expertise in security, our deep knowledge of business processes, and proficiency in solutions integration, we help you take the lead in confidently managing SOD validation.

Figure 3: SOD detection and remediation

Detective simulation

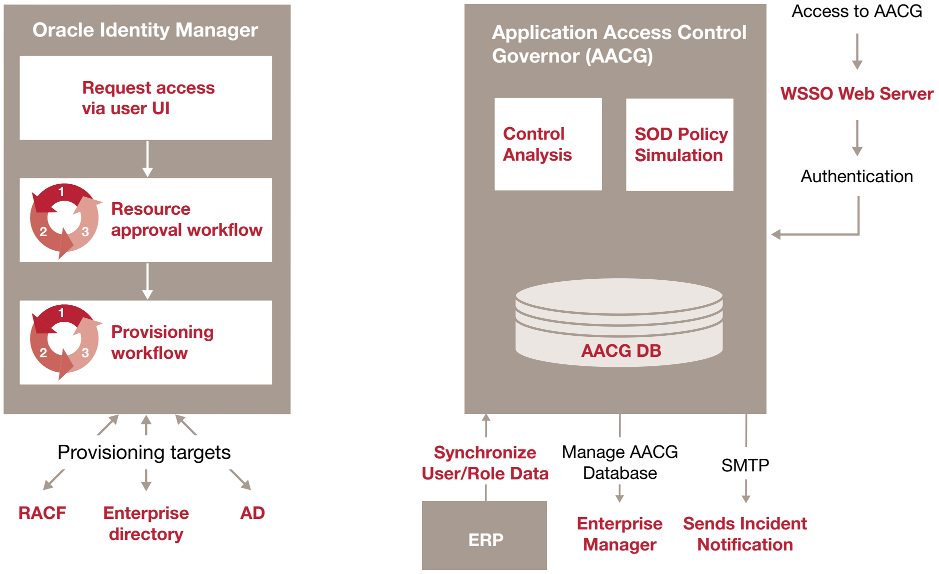

GRC
Identity Management
Applications
Account or Entitlement Added out-of-bounds
Applications
Out-of-bounds Account or Responsibility Removed
Violation Detection and Alert
Event Analysis
Assign Remediation Task
De-provision Entitlements to Remediate the Violation
Enforce SoD Policy SoD Engine
Oracle Identity Governance
Account Responsibility De-provisioned
For position only.
will re-created

Case study: A healthcare organization modernizes segregation of duties

A large nonprofit provider of healthcare services faced an increasingly common challenge: Ensuring appropriate segregation of duties to meet SOX compliance was becoming overly complex and arduous. The company was using manual processes for segregation of duties validation that were inefficient, costly to maintain, and did not support a strategy for future growth.

The healthcare organization knew that it needed an integrated, end-to-end solution that would automatically check access for potential SOD dutiesviolations during user access request and approval. The company had previously worked with PwC to implement an identity and access management strategy comprising Oracle Identity Governance solutions for identity governance and user provisioning. To capitalize on the inherent benefits of a single-vendor platform, the company identified Oracle GRC Manager, combined with Oracle Application Access Controls Governor (AACG), as the best tool to automate its SOD monitoring and validation.

Figure 4: IT architecture before automating SOD



The healthcare provider knew integrating the new solutions with its existing infrastructure would be complex and challenging; it also understood that it needed help improving its SOD controls and designing a strategy that would fully align with its SOX compliance needs. Our team of security experts had worked with the company to design and implement previous security solutions, and the company selected PwC to help with its SOD initiative because of our deep knowledge of its technology and processes, as well as our global security and compliance expertise.

Our team of identity management and compliance experts worked with multiple stakeholders to develop and build consensus on an integrated strategy and roadmap. We researched the healthcare organization's IT systems to fully assess management processes, technology infrastructure,

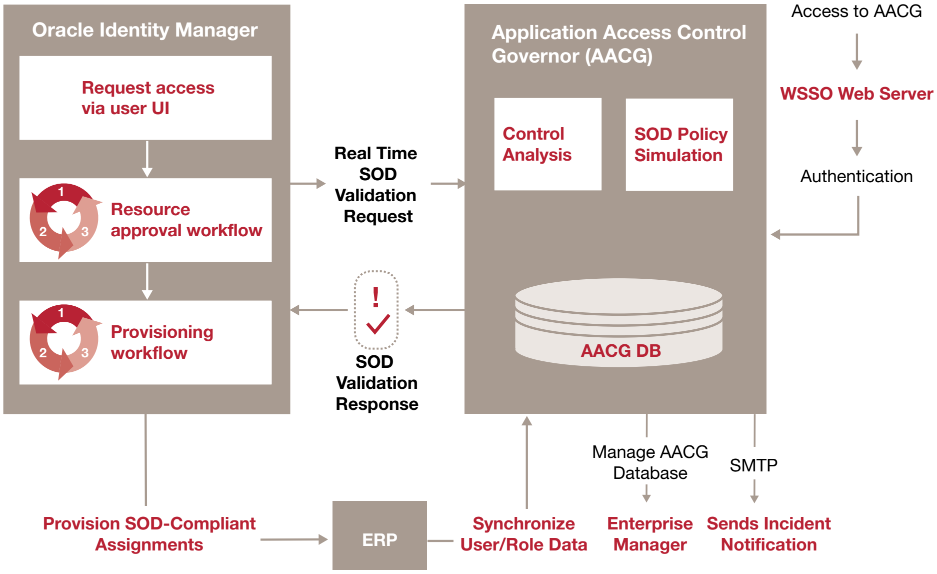
and compliance responsibilities. Our team integrated GRC Manager and AACG, Oracle's application for SOD management, with the company's existing identity and access management solutions. We helped the organization design and deploy a phased implementation that integrated GRC, identity management, and SOD capabilities.

The result? Today, application owners can automatically check for potential SOD violations during the access request and approval processes, and are informed in real time when access requests violate defined access controls. Reports are generated and distributed with minimal manual intervention, and reviewer feedback is efficiently tracked and aggregated using web-based user interfaces that do not require managers to pore over inscrutable spreadsheets and e-mail messages.

A centralized repository of SOD rules allows for automatic modeling of access changes due to business changes, and preauthorized exceptions to SOD rules and automated mitigating and monitoring controls now result in early identification and resolution of SOX exceptions.

Together, PwC and Oracle helped the healthcare provider create a single point of entry for IAM services and segregation of duties validation. The ability to audit SOD through the GRC module has reduced SOX exceptions and also reduced the audit demands on the security team. The healthcare provider now has automated processes for SOD management that are consistent across all divisions, helping reduce costs and inefficiencies while increasing accuracy.

Figure 5: IT architecture after implementing SOD



Oracle Identity Manager
Request access via user UI
Resource approval workflow
Provisioning workflow
1
2
3
Real Time SOD Validation Request
SOD Validation Response
Application Access Control Governor (AACG)
Control Analysis
SOD Policy Simulation
AACG DB
Access to AACG
WSSO Web Server
Authentication
Manage AACG Database
SMTP
Provision SOD-Compliant Assignments
ERP
Synchronize User/Role Data
Enterprise Manager
Sends Incident Notification

Contacts

To have a deeper conversation about how this subject may affect your business, please contact:

Gary Loveland
Principal, National Security Leader
(949) 437-5380
gary.loveland@us.pwc.com

Joe DeVita
Partner, GRC Technology Leader
(203) 539-4186
joseph.devita@us.pwc.com

www.pwc.com