

# Access management and segregation of duties: solving the conundrum



Total plug-and-play solutions for access management and segregation of duties aren't here yet, according to the findings of an exclusive BearingPoint benchmarking survey. Instead, most solutions today focus on either identity software or business rules. For now, the leading solutions will combine the best of both approaches.

## In this white paper

Introduction	2
Benchmarking the current state	2
Focus areas and leading practices: study decoded	3
The state of software today	6
Road map for the future	8
How BearingPoint can help	8

Access management and segregation of duties solutions can help streamline both audit preparations and audit cycles. They also can help organizations lower their costs—an important benefit in today's turbulent economy—and support zero-day provisioning and deprovisioning, which can lead to increased efficiency.

## Introduction

Access management (AM) and segregation of duties (SoD) controls have become increasingly important to executives and corporate managers responsible for preventing fraud, ensuring the security of enterprise information systems, and complying with the Sarbanes-Oxley Act and other regulations. Although AM and SoD controls have always been required, they were often viewed as part of regulatory compliance and, thus, frequently overlooked. This is changing as auditors—and the companies they audit—focus increasingly on compliance. AM and SoD solutions can help organizations streamline their audit preparations and audit cycles, lower costs—an important benefit in today's turbulent economy—and support zero-day provisioning and deprovisioning, which can lead to increased efficiency.

AM and SoD controls serve separate yet interrelated functions. AM controls are designed to prevent violations from occurring. On the other hand, SoD controls help organizations reduce risk of fraud associated with conflicting user access to enterprise resource planning (ERP) and other distributed information systems. They also help auditors monitor and control functional responsibilities within an enterprise. Executed through the provisioning process, AM controls support and augment SoD controls. SoD controls work largely after the fact by appearing in audits that seek possible violations. Using both AM and SoD controls creates a balance of proactive and reactive mechanisms within organizations.

Software companies offering AM and SoD solutions have developed their products largely as extensions of current applications. This has resulted in the development of two main approaches to AM and SoD solutions. One approach, developed by identity and role management software suppliers, is identity-centric; it mainly extends the capabilities of identity and role management software. The other approach, developed by ERP vendors, centers on business rules; it extends the capabilities of ERP and other process-based add-ons.

However, neither means alone is sufficient to meet the needs of today's demanding and security-conscious audit environment. Instead, companies need a broad AM and SoD approach, one that encompasses the concepts of both identity roles and business rules. This hybrid method can offer controls that are suited for today's stringent requirements.

## Benchmarking the current state

Before organizations select and implement AM and SoD controls, it's helpful for them to first obtain a clear view of the current marketplace. To help a major client gain just such a view, BearingPoint recently worked with research firm Corporate Integrity to conduct a joint benchmarking study. The study surveyed the AM and SoD control programs of several large, well-known multinational corporations operating in a range of industries, including energy, financial services, manufacturing, retail, shipping/transportation and telecommunications. These companies were selected for their use of legacy and open source systems, recent merger and acquisition activities, broad customer and supplier bases, and constantly changing user populations.

During this benchmarking study, BearingPoint learned that these companies viewed AM and SoD controls primarily as business projects, not information technology (IT) projects. What's more, these companies tended to view IT solely as an enabler. As a result, many of their current projects merely aimed to automate AM controls and improve overall SoD processes.

The study also revealed that a limited enterprise view of both AM and SoD controls is common among large corporations. Full-fledged enterprise approaches typically are not on

these companies' agendas. Instead, corporate AM and SoD projects are generally conducted in functional silos. For example, the corporate IT organization may approach AM and SoD initiatives from an identity and access management perspective. At the same time, the finance and audit groups routinely approach projects—especially SoD implementations—from a rules-based process perspective.

A tendency to adopt a minimalist, decentralized approach to AM and SoD reviews—common at many organizations—was another benchmarking discovery. In most cases, this means companies perform only those tasks necessary to meet regulatory compliance. While this minimalist approach appears to work in the short run, no company surveyed in the study was happy with its current environment.

Similarly, control environments at many companies are manually governed and overly focused on process, according to our survey. This approach should change, thanks to Auditing Standard No. 5.<sup>1</sup> So far, this change has been slow to arrive.

The study also found that maintaining proper access as employees move into, around and out of companies remains a challenge. One requirement for this level of access control is technology that provides each employee with a single digital identity enterprisewide. Unfortunately, this technology automation and implementation is still evolving. As a result, managing access recertification remains a manual process, one that can involve multiple systems and is often overly technical and labor-intensive, adding costs to the process.

One risky result: While companies should investigate every pair of conflicting transactions for possible intrusions, few actually do. Instead, sampling is the norm. Few company managers are satisfied with this practice. Most would prefer to use technology-based solutions that prevent these conflicts and then automatically provide complete, validated reports—if such solutions were available. While centralized AM and SoD management tools do exist, they are not mature enough to satisfy the needs of global corporations.

In response, many companies are creating centralized identity repositories, a key finding of the study. But progress has been slow here, too. The challenges of building such repositories are immense, transcending the scope of individual business units and existing IT implementations.

## Focus areas and leading practices: study decoded

As a result of our AM and SoD benchmarking study, BearingPoint has identified leading, common and deficient practices for seven focus areas (Figure 1). These should be addressed by any organization seeking to develop comprehensive AM and SoD solutions:

**Enterprise strategy.** AM and SoD solutions should be leveraged at every level of the enterprise. A leading practice considers AM initiatives as part of an enterprise program driven by factors that include requirements for business, risk, compliance, security and auditing processes. For example, such requirements might include compliance-based SoD controls, IT security risks and organizational restructuring. An AM strategy should involve a carefully orchestrated deployment of policies, procedures and technologies that affect enterprise users, including employees, contractors, dealers, suppliers and other business partners. Ideally, all related communications will be coordinated around an organization's AM strategy, implementation and operation.

<sup>1</sup>Auditing Standard No. 5 is a 2007 provision of the Sarbanes-Oxley Act that governs audits of internal controls over financial reporting.

Figure 1. Summary of access management (AM) and segregation of duties (SoD) focus areas and leading practices

Focus area	Leading practice
Enterprise strategy	AM and SoD solutions should be leveraged at every level of an enterprise.
Business and information technology process alignment	Robust support from business managers will facilitate an AM implementation.
Role engineering and management	Role management, which includes role mining, role engineering and role definition, should touch and influence every structural aspect of an organization.
Entitlement and access management	Leading practices focus on entitlements and privileges of user accounts and managing them solely with roles and responsibilities.
User and transaction monitoring	This includes monitoring activities and supporting technologies for creating, classifying, managing and provisioning/deprovisioning identities in an enterprise.
Reporting and metrics	Leading practices include using processes that monitor and report on user behaviors in enterprise applications and business processes.
Technology implementation	One leading practice is to establish dedicated AM and SoD technology teams. Specific experience may be needed in areas such as role engineering and identity/entitlement provisioning.

As a result of our access management (AM) and segregation of duties (SoD) benchmarking study, BearingPoint has identified leading, common and deficient practices for seven focus areas. These should be addressed by any organization seeking to develop comprehensive AM and SoD solutions.

In comparison, common practices in this focus area include some collaboration between IT and the business, even as strategies remain focused on risk and compliance silos. At some common-practice companies, the focus is almost solely on compliance and barely on risk. Deficient-practice companies take an inconsistent approach to their AM and SoD strategies. For example, at one telecommunications company, risk management falls to the director of IT or chief security officer rather than on the business as a whole.

**Business and IT process alignment.** Success of AM and SoD solutions depends on the alignment of IT and the business. Robust support from business managers will facilitate any AM implementation. Similarly, it's a leading practice to have dedicated project management teams and project management offices (PMOs) at the head of effective deployments, especially because these implementations frequently involve multiple work streams. For example, a single enterprise installation could include work streams for user-community definition and coverage, digital identification definition, record consolidation, and storage and distribution requirements. These teams should be governed by charters from the executive management team.

Common practices in this area include rudimentary alignment between IT and the business. For example, some companies use exception management but not consistently. And deficient practices in this area include a major retailer whose IT department and business units are only beginning to collaborate.

**Role engineering and management.** This focus area verifies that user accounts are aligned with well-defined, well-engineered roles. This helps organizations understand the rules around access and entitlement management. Role management, which includes role mining, role engineering and role definition, should touch and influence every structural aspect of an organization. It's a leading practice to foster close interaction among IT groups, the business, application owners and PMOs. For example, one retail bank enforces its classification policy across all systems.

Common practices include using ad hoc processes and greater reliance on rules management than on roles. Deficient practices were observed at one auto manufacturer, which has no strategy for roles, and at an insurer that has only limited and variable approaches to role management.

**Entitlement and access management.** Leading practices focus on entitlements and privileges of user accounts and managing them solely with roles and responsibilities. Roles become the foundation of every function that users can access in an organization's business processes and IT environment. For example, one technology manufacturer's ERP system maintains approximately 100 roles. AM solutions can be used to verify user accounts with appropriate permissions and help the company avoid SoD conflicts.

Common practices include AM implementations that do not cover the universe of systems within an organization. For example, at one automaker, only a quarter of the systems are fully utilizing the identities provided by its AM implementation. Deficient practices are characterized by using duplicate roles for accesses, blindly copying privileges among users and consolidating access reports with laborious manual processes.

**User and transaction monitoring.** One leading practice involves scrutinizing the enforcement of privileges, restrictions and controls around business transactions in real time. This includes monitoring activities and supporting technologies for creating, classifying, managing and provisioning/deprovisioning identities in an enterprise. Benefits include streamlined, consistent and compliant management of the identity life cycle, including identity recertifications.

Common practices include manual audit systems, partial technology integration — when automated systems are used — and limited monitoring of select applications. Deficient practices include variable and poorly defined audit processes.

**Reporting and metrics.** Leading practices include using processes that monitor and report on user behaviors in enterprise applications and business processes. This lets a company report a user's access privileges and behaviors based on roles and responsibilities and then identify SoD violations and deviations from prescribed behaviors.

Common practices include relying on manual processes. For example, one retail bank conducts both annual and quarterly reporting on identity and access but with largely manual processes. Deficient practices include decentralized processes, little or no automation and variable, inconsistent reporting processes.

**Technology implementation.** Because AM and SoD systems touch every aspect of the business and its associated processes, specific skills are needed to implement and interpret AM and SoD strategies. For this reason, one leading practice is to establish dedicated AM and SoD technology teams. Specific experience may be needed in areas such as role engineering and identity/entitlement provisioning. Another leading practice is to select AM and SoD tools only after a careful review of their capabilities to support a common infrastructure across enterprise processes and applications. A third leading practice involves custom enhancements or applications that augment shortcomings, if any, of selected commercial- off-the-shelf tools.

One common practice is the use of manual processes supported by islands of technology. For example, a retail bank enjoys a nearly complete view of identities through a directory, but it still scatters its AM controls. A deficient practice uses little to no technology. This results in both low levels of consistency and a decentralized approach.

## The state of software today

In today's AM and SoD marketplace, no single solution can adequately meet every need of global corporations. While complete solutions do exist, they tend to be overly based on either identity roles or business rules. Instead, a leading solution will involve adopting a hybrid approach that combines the best of these two approaches.

Each of the two main types of AM and SoD solutions displays both strengths and weaknesses. Rules-based tools enjoy several strengths: They can be deployed relatively simply, understood easily by business managers and integrated effectively with existing ERP systems. But their provisioning and role-engineering capabilities — and integratability with heterogeneous applications — are weak, often requiring customization. Also, because these tools are focused on a particular ERP system or application, using them may promote the creation of functional silos when an enterprisewide approach is needed.

By contrast, identity-centric, identity-based tools handle heterogeneous systems and applications well. But they lack prebuilt SoD rules and controls and cannot be the sole solution for complex enterprises.

Since neither approach is complete—and because no plug-and-play tool is available—a solution must offer interoperability to permit the creation of hybrid systems. It's also important that a solution offer the ability to assign a single identity to each user and implement proper AM controls, which prevents SoD conflicts from occurring in multiple locations.

Any hybrid approach should include at least one identity-based solution and one or more business process, rules-based tools. Role management should play a part in any approach as well. Furthermore, role management should be looked at two ways: top-down, aligned with the organizational hierarchy, and bottom-up, based on access controls in each application.

Hybrid solutions also need to meet the separate—and often, but not always—contradictory goals of infrastructure architects and business/application owners. Typically, infrastructure architects want seamless, unified solutions that employ a single:

- **Directory service**—to manage users' identities and profiles
- **Set of roles**—to allow roles to be interpreted uniformly by all applications and services for access control
- **Set of entitlement rules**—to determine whether a user should be given access to specific applications and services
- **Authentication service**—to authenticate users, which should be used by all applications and services
- **Authorization service**—to decide access control, which also should be used by all applications and services
- **Reporting service**—to provide accounting and auditing capabilities to all applications and business/application owners

In contrast, business/application owners usually select AM and SoD tools for their ease of use and deployment. They prefer tools that can be deployed and implemented with minimal configuration, customization, integration or development. Business/application owners also favor tools with SoD rules that they can use to jump-start discovery and easy-to-configure reporting templates for generating reports on risk, compliance and security.

To reduce the silo effect of individual business-based tools, identity-based AM and SoD solutions can serve as the foundation. Then a rules-based solution can more easily tie into heterogeneous systems and legacy applications, providing a base set of roles that can be reused by ERP and other enterprise systems.

In today's access management and segregation of duties marketplace, no single solution can adequately meet every need of global corporations. Instead, a leading solution will involve adopting a hybrid approach that combines the best of these two approaches.

Developing a strategy and outline for the desired future state often requires preliminary planning and creating additional definitions.

## Road map for the future

For organizations that want to move toward this hybrid approach with their AM and SoD solutions, an incremental, phased process is highly recommended. Developing a strategy and outline for the desired future state often requires preliminary planning and creating additional definitions. Managers also need a detailed understanding of their current state and a clear vision for their future state.

This means understanding current and prospective application environments in light of the adequacy of role management, centralization of access management and approach for SoD controls. First, create a detailed requirements list. This list can then be used to develop required process and organizational changes followed by an architectural and technical solution. In this way, managers can address AM and SoD controls at the enterprise level. To address all areas critical to AM and SoD controls, BearingPoint recommends that any solution methodology feature three work streams:

- **Business process**—this work stream begins with a business vision and then moves to strategy, business and functional requirements, risk assessment, and business case and return on investment.
- **Data analysis**—this work stream begins by first inventorying data and then aligning it. Next, it proceeds to metadata and taxonomy models, rules and role engineering, and end-to-end data integration. It ends with a pilot project.
- **Technology analysis**—this work stream begins with a current-state technology assessment. Then it proceeds to the architecture for identity and access management, technology infrastructure evaluation and selection, proof-of-concept (PoC) and implementation plan, and staging and quality assurance. Its final step is production.

Collectively, the various stages of these work streams can be thought of as a sequence, one that starts with the strategy and then proceeds through the design, build, deploy and operate phases. During the strategy phase, the organization creates the business strategy, develops the business case, analyzes and plans its AM and SoD solutions, and gathers requirements. During the design and build phases, the organization designs and conducts the PoC, obtains needed technology, develops implementation plans, and then constructs and deploys the solutions. In the final deploy and operate stages, the organization deploys infrastructure, supports applications and conducts knowledge transfer.

When considering this phased approach, managers should understand how other organizations—especially others in their industry—have implemented AM and SoD solutions. BearingPoint recently created a 36-month, phased, plateau-based road map for a major client planning to implement AM and SoD solutions at the enterprise level. While every enterprise is unique, commonalities do exist. A sample phased, plateau-based road map is provided in Figure 2.

## How BearingPoint can help

As illustrated in this white paper, many different types of organizations are challenged by AM and SoD control processes and implementations. In the past, many organizations took a minimalist, decentralized approach to compliance, simply doing whatever was needed to “just get by” for compliance requirements related to AM and SoD controls. But now, as overall Sarbanes-Oxley compliance becomes routine, that is changing. Auditors are focusing

Figure 2. Sample road map for the incremental, phased implementation of access management (AM) and segregation of duties (SoD) controls

Plateau level	Timing	Activities	Relative business value
0	Now	<ul style="list-style-type: none"> <li>• Create identity management and SoD plan and charter</li> <li>• Set AM and SoD strategy</li> <li>• Assess current-state readiness</li> <li>• Define future state</li> <li>• Set business case and return on investment</li> <li>• Analyze organizational effect</li> </ul>	Low
1	0 to 3 months	<ul style="list-style-type: none"> <li>• Create role-engineering strategy</li> <li>• Classify and prioritize applications</li> <li>• Inventory and align data</li> <li>• Verify and validate digital identities</li> <li>• Gather requirements</li> <li>• Create metadata and taxonomy models</li> <li>• Analyze current-state technology</li> </ul>	Low-medium
2	3 to 9 months	<ul style="list-style-type: none"> <li>• Reference technology</li> <li>• Evaluate and select technology</li> <li>• Conduct proof-of-concept pilot project, including:                             <ul style="list-style-type: none"> <li>– Rules and role engineering</li> <li>– Development of SoD analysis and controls</li> <li>– Rollout and implementation planning</li> <li>– Data migration</li> <li>– Staging and quality assurance</li> <li>– Pilot project to go-live</li> </ul> </li> </ul>	Medium-high
3-plus	9 to 36 months	<ul style="list-style-type: none"> <li>• Reiterate plateaus 1 and 2 with expanded scope</li> <li>• Convert to service</li> <li>• Define and roll out identity management services</li> <li>• Begin production support</li> </ul>	High

The road to hybrid access management and segregation of duties solutions is not short. But the benefits can be worth the journey.

on previously overlooked areas, and just getting by is no longer considered a viable option. As a result, organizations are moving toward a proactive approach that involves changes to process and technology, as well as the leading practices discussed in this white paper.

From a technology solution perspective, most software suppliers approach AM and SoD initiatives in one of two ways. If they are identity and role management software suppliers, their approach is likely to be identity-based. If they are ERP suppliers, they will tend to focus on business rules. While both types of suppliers offer effective AM and SoD tools, their products are not mature enough to accomplish everything needed by large, complex multinational organizations.

As a result, the leading solutions for enterprises today involve hybrid approaches that combine the best of solutions focused on both IT and business rules. BearingPoint can help C-level executives plan, design and implement this kind of hybrid approach, taking into consideration business process requirements and aligning them with technology solutions. We have worked with a variety of organizations engaged in various approaches to building AM and SoD capabilities. Specifically, BearingPoint can help:

- Benchmark your organization's AM and SoD solutions against other companies', whether or not they're in your industry
- Align your organization's business and IT strategies
- Teach your managers to understand the current business and corresponding application environment
- Create a detailed AM and SoD requirements list
- Develop role management strategies and engineering solutions to reduce the proliferation of roles
- Set an AM and SoD strategy and create a road map for systems implementation
- Evaluate and select appropriate solutions and applications from a range of software suppliers
- Activate PoC and pilot project deployments
- Lead a phased implementation of AM and SoD solutions across business units on a prioritized application basis

The road to hybrid AM and SoD solutions is not short. But the benefits can be worth the journey.

## About the authors

**Tony Klimas** is a managing director in BearingPoint's World Class Finance practice. He is responsible for the company's Commercial Services Risk and Compliance solution. Tony is also a frequent speaker and author on enterprise risk strategy, enterprise risk management and compliance.

**Hitesh A. Anklesaria** is a senior manager in BearingPoint's Risk, Compliance and Security practice. He is responsible for and involved with a range of consulting assignments, including risk and compliance management, IT governance, security architectures, certification and accreditation, and strategic alliances. While Hitesh's experience crosses numerous industries, his focus has been on clients in financial and commercial services.

**Michael Rasmussen** is president of Corporate Integrity LLC, which specializes in conducting research and analysis in corporate governance, risk and compliance efforts. His company has collaborated previously with BearingPoint in the risk, compliance and security space.





Management  
& Technology  
Consultants

## Helping our clients get sustainable, measurable results

BearingPoint is a leading management and technology consulting company serving the *Forbes* Global 2000 and many of the world's largest public services organizations. Our thousands of passionate, experienced consultants help organizations around the world solve their most pressing challenges, day in and day out. Through our collaborative and flexible approach, we help our clients get practical, sustainable, measurable results, make the right strategic decisions and implement the right solutions.

**We are BearingPoint, management and technology consultants.**

To learn more, contact us at 1 866 BRNGPNT (+1) 508 216 2523 from outside the United States and Canada), or visit our Web site at [www.bearingpoint.com](http://www.bearingpoint.com).

BearingPoint, Inc.  
1676 International Drive  
McLean, VA 22102

[www.bearingpoint.com](http://www.bearingpoint.com)

© 2009 BearingPoint, Inc. All rights reserved. Printed in the U.S.  
BearingPoint® is a registered trademark of BearingPoint, Inc. or its affiliates in the United States and other countries. Any other marks are the property of their respective owners. C4755-0309-01-USNY