Gartner

Research

Publication Date: 9 February 2007 ID Number: G00145412

MarketScope for Segregation of Duties Controls Within ERP, 2007

Paul E. Proctor, Jay Heiser, Neil MacDonald

Segregation of duties controls for ERP systems will be an ongoing concern to auditors, particularly in the context of Section 404 of the Sarbanes-Oxley Act and similar legislation worldwide. A variety of stand-alone and embedded control capabilities are available from nine vendors.

WHAT YOU NEED TO KNOW

Segregation of duties (SOD) conflicts — and the controls to prevent them — will remain an area of audit findings for the foreseeable future. SOD violations are sometimes an indication of ongoing fraud, and they always represent an unnecessary vulnerability to unwanted financial activity. This risk can be reduced by managing SOD through preventive and detective controls. Control automation provides efficiency and defensible documentation on effectiveness, which ultimately reduces risks and costs. This MarketScope not only addresses technical controls for automation, but also provides guidance on process effectiveness.

Three primary techniques are used to address SOD issues in ERP systems (see expanded descriptions below):

- Technique 1: Static analysis — Identifying and reducing SOD conflicts within ERP application-level functional permissions.
- Technique 2: Provisioning support — Preventing new SOD conflicts through integration with the user provisioning (UP) and role management process. Today, privilege conflicts are typically addressed within a single ERP application, if at all, but increasingly, the need is to address conflicts across multiple application types simultaneously.
- Technique 3: Transaction monitoring — Identifying SOD violations by automatically monitoring for transactions that indicate inappropriate behavior.

Controls using Technique 1 are absolutely necessary to address auditor concerns and findings. Although controls using Techniques 2 and 3 are currently of less interest to external auditors, experience has shown that they are useful both in ensuring that SOD policies are met and in reducing operational costs, and best practice for SOD management is to use a combination of all three control techniques. Once a choice of control processes has been made, an organization can begin evaluating sources of automation technology. Historically, vendors have specialized in one subset of controls and expanded to provide others. Gartner does not recommend one subset of vendors above all others in the ERP SOD control market; however, organizations will typically be interested in a specific vendor subset:

- SAP ERP — Organizations that use primarily SAP should put ACL Services, Approva, CSI, Oversight Systems and SAP on their shortlist.
- Oracle ERP — Organizations that use primarily Oracle and/or PeopleSoft should put ACL, Applimation, Approva, LogicalApps, Oracle and Oversight on their shortlist.
- Multiple ERP — Organizations with multiple ERP instances from different vendors should put ACL, Approva and Oversight on their shortlist.
- Transaction monitoring — Organizations interested in primarily ERP transaction monitoring should put ACL and Oversight on their shortlist.

STRATEGIC PLANNING ASSUMPTIONS

By 2010, auditors will expect regulated organizations to detect fraud by performing transaction monitoring on a continuous basis, and 60% of regulated firms will have such an automated process in place (0.8 probability).

The broader market for GRC products will subsume this market by 2010, and SOD controls will be offered primarily as embedded capabilities in GRC products/suites (0.8 probability).

MARKETSCOPE

SOD controls within ERP systems will be an ongoing concern to auditors, particularly in the context of Section 404 of the Sarbanes-Oxley Act (SOX). This Research Note discusses nine vendors that address this need with a wide variety of stand-alone and embedded control capabilities. Some of the products support ERPs from multiple vendors, while others address only SAP or only Oracle. The choice of vendors is further limited by governance philosophy and the corresponding control types implemented by the various providers.

Managing SOD in the context of a complex and highly active ERP system is no simple task (see Note 1), and multiple types of controls should be used. As discussed earlier, technology can facilitate three different SOD control processes within an ERP system. The effectiveness of such tools in using these techniques to recognize and control duty conflicts is dependent on the breadth and depth of the accounting domain knowledge embedded within them.

- Technique 1 (preventive): Static analysis to clean up the mess — Most organizations have not effectively addressed SOD conflicts and are saddled with thousands of conflicts throughout multiple ERP instantiations. These conflicts can be difficult to identify, and the identification process requires accounting knowledge and institutional knowledge of the specific ERP instance. Poorly conceived roles and ad hoc role management increase the complexity, making it difficult to identify user accounts with excessive levels of access. Static analysis of the current situation is used to identify and prioritize conflicts for cleaning up neglected ERP roles. Many organizations wince when first confronted with the volume and severity of discovered conflicts, but tackling them is becoming increasingly important to address auditor concerns and avoid qualified audits and audit findings. Organizations with manual SOD analysis processes for role creation and assignment may use these types of tools to automate the analysis.

- Technique 2 (preventive): SOD controls integrated with the ERP UP process — Once the permissions "mess" is cleaned up, organizations must put preventive controls within the ongoing user and role provisioning process to keep it that way. To be fully effective, this control technique requires workflow process elements, including request, review, signoff and attestation. Ongoing prevention of new SOD conflicts also requires an exception tracking process and the ability to measure and report on residual risk. Overlap exists with Technique 1 and longer term with the identity and access management (IAM) market (see Note 2).

- Technique 3 (reactive): Transaction monitoring — A central tenet of governance is that control effectiveness must be continuously monitored. The contribution of SOD controls can be verified by monitoring what happens, as expressed by a system's business transactions. Transaction monitoring also functions as an additional layer of reactive control that will detect failures in the two preventive controls (Techniques 1 and 2). This control is based on analysis of the transaction logs in a periodic or continuous manner. Relevant logs include those that reflect the activities of the ERP users. For example, if a user has the privilege to create and the privilege to pay a vendor, and subsequently took advantage of these conflicting permissions, the transaction log would reflect that the user had performed both of these actions. Inappropriate activity sequences such as these actions would be automatically identified through transaction monitoring.

Transaction monitoring can be used early in the cleanup process to detect the use of conflicting permissions and prioritize these conflicts for earlier remediation. It also can be used to monitor the use of risky, yet approved, permissions on the exceptions list. However, transaction monitoring is still in the early stages of use by Gartner clients. The tools and practices that support this control set continue to evolve, and we expect it to provide great value by 2008.

Overall, most of the market activity has followed a natural maturity model, with clients first focusing on the immediate need to identify and remediate issues cited by auditors using Technique 1, evolving their processes to prevent the reintroduction of SOD issues using Technique 2, and over time, ensuring the ongoing analysis of transactions using Technique 3. Market penetration reflects this trend: Approximately 10% of ERP-equipped organizations with more than 1,000 ERP users have adopted Technique 1, 5% to 7% are using Technique 2, and 3% to 5% are using Technique 3.

Market/Market Segment Description

The ERP SOD control market offers several good technology choices, appropriate for organizations of different sizes, capabilities and monitoring needs. Organizations should analyze their requirements along the following dimensions and choose the vendor most appropriate for their unique situation:

- Technique 1: Static analysis — Automated static analysis to help an organization identify and clean up existing SOD conflicts.

- Technique 2: Provisioning support — Functions embedded in provisioning workflow to evaluate proposed permission additions and changes to identify SOD conflicts. May include workflow support for approvals and exception management.

- Technique 2: Integrated provisioning workflow — Provisioning support can also be directly integrated within an ERP system or externally with IAM systems, preventing a user from being provisioned without appropriate approvals when SOD conflicts are identified.

- Technique 3: Transaction monitoring — Functions to analyze ERP transactions for SOD violations. Through 2007, these functions will be primarily enabled by batch processing daily, weekly, monthly or quarterly (depending on the organization's requirements and availability of transaction-level data for historical analysis). While analysis of transactions executed for a historical period can help to prioritize SOD remediation efforts, it should not be viewed as a substitute for static analysis of SOD issues that exist but were not exploited in the historical snapshot of transactions analyzed.

- SAP — Products appropriate for addressing SOD conflicts in the SAP ERP system.

- Oracle — Products appropriate for addressing SOD conflicts in the Oracle/PeopleSoft ERP systems. Ideally, this would include support for JD Edwards as well.

- Other ERP — Products appropriate for addressing SOD conflicts in other ERP systems (not Oracle or SAP).

- Cross-platform — Products that support multiple ERP systems simultaneously. A multiplatform approach not only identifies and remediates conflicts that exist across multiple instances of a single ERP technology, but it does this between ERP instances from different technology providers. For example, if the ERP infrastructure is such that a vendor could be created in one ERP instance, but payments to that vendor would be processed in another instance, SOD control mechanisms must operate across both instances, treating them as a single transactional system.

- 911 (emergency) access — Support for managing emergency privileged access to the ERP system. At a minimum, all activities of the administrative access — while it is active — should be logged and auditable. Ideally, such a capability provides a check-out/check-in system for administrative credentials, with the option for a workflow-enabled approval process.

Figure 1 provides summary guidance for product selection. These are Gartner recommendations and are not based solely on the presence of a function by a vendor.

Figure 1. Vendor Selection Guidance

	ACL Services	Applimation	Approva	Control Software International	D2C Solutions	LogicalApps	Oracle	Oversight Systems	SAP
Technique 1: Static Analysis	○	◑	◑	◑	◑	●	◑	◔	●
Technique 2: Provisioning Support	○	◑	◑	◔	◔	◑	◑	○	◑
Technique 2: Integrated Provisioning Workflow	○	◑	◔	○	◔	●	●	○	◑
Technique 3: Transaction Monitoring	●	◔	◑	◑	◔	◔	◔	●	◑
SAP	◑	○	◑	◑	◑	○	○	◑	●
Oracle	◑	●	◑	○	○	●	●	◑	◔
Other ERP	◑	◔	◑	○	○	○	◔	◑	◔
Cross-Platform	●	○	●	○	○	○	○	◑	◔
911 (Emergency) Access	○	○	◑	○	○	◑	○	○	◑

Key:

○ Gartner does not recommend if you have this requirement
◔ May meet requirement
◑ Gartner recommends for this requirement
● Gartner strongly recommends for this requirement

145412-1

Source: Gartner (February 2007)

Organizations looking for a technical solution to SOD risk can find a number of suitable products that not only will go far in "pleasing the auditor," but will also offer immediate risk reduction benefits. SOD is a well-proven concept, and Gartner expects that within a few years, technical mechanisms to enforce it will be considered virtually mandatory for ERP instances within regulated companies.

However, the strict maintenance of duty segregation cannot guarantee a risk-free ERP system. Although significant, SOD exposure and conflicts are certainly not the only areas of risk that are associated with ERP systems. Furthermore, SOD is not the exclusive ERP concern of government regulators, although it is currently an area receiving a great deal of attention from auditors. Highly regulated organizations should expect that once the auditors are satisfied with the SOD controls, other ERP risks will become areas of auditor attention. Effective risk management requires a broad visibility into all material exposures and a priority-driven approach. Too much focus on any single form of risk will inevitably mean that other forms of risk are gaining inappropriately low levels of attention. Thus, vendor road maps for ongoing evolution in ERP governance, risk and compliance (GRC) should be considered as organizations make tactical SOD tool decisions.

Inclusion and Exclusion Criteria

Products included in this MarketScope have at least one of the three SOD control techniques (static analysis, provisioning support or transaction monitoring) to address SOD issues. The included vendors had to provide at least three production references that are using their product primarily for SOD controls in ERP.

Only products that explicitly supported SOD control were included. For example, products that performed transaction monitoring — even toward the goals of detecting fraud, reducing waste or verifying the integrity of financial processes — did not qualify for this MarketScope if they did not directly support SOD control.

Rating for Overall Market/Market Segment

Overall Market Rating: Strong Positive

Market Summary

The demand for SOD functionality will grow through 2010 as organizations look to automate controls for efficiency and cost savings. The SOD for ERP market rating is positive and poised for growth in 2007. The market was about $150 million in 2006 and is forecast to grow to $200 million in 2007 and to more than $250 million by 2008. These are conservative numbers that are based on the product and service revenue of the companies in this document. However, convergence will make this market increasingly difficult to measure and define. Today, the SOD for ERP market can best be understood as a submarket within the larger finance and audit GRC market, which is sized at $604 million in 2008 and will grow to $855 million by 2010 (see "Finance and Audit GRC Software Market Is Expanding"). As SOD functions become embedded in broader GRC products, the stand-alone market will shrink and be subsumed by 2010.

Evaluation Criteria

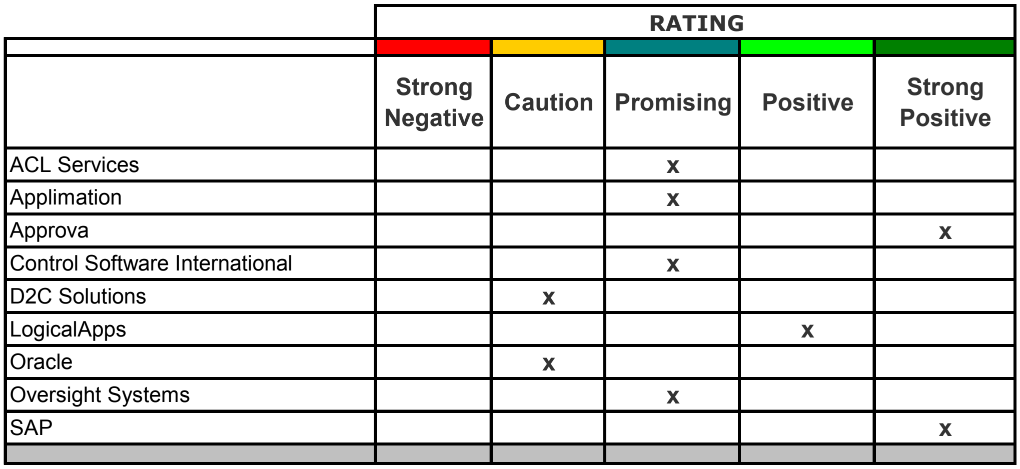
Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Market Understanding	The success and "mind share" of the product in the SOD market, including the installed base and market share, as well as the maturity and breadth of the organization's distribution channels. Also considered is the quality of customer case studies and references, and the level of interest from Gartner clients.	high

Evaluation Criteria	Comment	Weighting
Market Responsiveness and Track Record	Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customers' needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.	standard
Offering (Product) Strategy	The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map onto current and future requirements.	high
Product/Service	Breadth of the current feature set is a key evaluation criterion. We specifically evaluated the elements in Figure 1.	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	Viability includes an assessment of the overall financial health of the organization and its commitment to the SOD market, along with the financial and practical success of the business unit. Also included is the likelihood of the organization/business unit to continue investing in the market and to continue developing innovative products to meet the requirements of several different types of customer.	standard

Source: Gartner

Figure 2. MarketScope for Segregation of Duties Controls Within ERP, 2007



	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
ACL Services			x		
Applimation			x		
Approva					x
Control Software International			x		
D2C Solutions		x			
LogicalApps				x	
Oracle		x			
Oversight Systems			x		
SAP					x

As of 9 February 2007

Source: Gartner (February 2007)

Vendor Product/Service Analysis

ACL Services

Rating: Promising

Technique 3: Transaction Monitoring (Gartner Strongly Recommends)

ERP: SAP, Oracle, PeopleSoft and Others

Emphasizing almost two decades of in-depth experience with the external auditing community, ACL's Continuous Controls Monitoring (CCM) offering is based on the premise that detection is ultimately more important than prevention. Providing no proactive controls, ACL instead offers a business-process-oriented approach that is theoretically capable of detecting anomalous activity that would be invisible to products that provide control over one or more ERP instances. Unsurprisingly, SOD is not the primary emphasis of CCM, as it also addresses risks such as fraud, waste and abuse. The architecture is designed to accept a data feed from virtually any enterprise application, using it to monitor the integrity and acceptability of end-to-end business processes, without limitations on the number, type or brand of application platforms.

Shortlist: ACL should be on the shortlist of organizations that already have a solution for Technique 1 (static analysis) or that expect to eventually use a UP tool, and are looking for a multiproduct transaction analysis tool from an independent vendor.

Applimation

Rating: Promising

Technique 1: Static Analysis (Gartner Recommends)

Technique 2: Provisioning Support (Gartner Recommends)

Technique 3: Transaction Monitoring (May Meet Requirement)

ERP: Oracle and PeopleSoft

Applimation Integra Access Segregation of Duties is available either stand-alone or bundled into the complete Integra suite. In contrast to the other vendors in this document, Applimation does not position itself as being primarily in the "compliance" business, but instead positions itself in the application life cycle management business. Offering a modular product approach that emphasizes data and change management, along with transaction monitoring, Applimation's SOD offering is not the best of breed.

Shortlist: Organizations that use Oracle and PeopleSoft, that are interested in broader application life cycle management, and that are looking for SOD controls should consider the Integra product.

Approva

Rating: Strong Positive

Technique 1: Static Analysis (Gartner Recommends)

Technique 2: Provisioning Support (Gartner Recommends)

Technique 3: Transaction Monitoring (Gartner Recommends)

ERP: SAP, Oracle, PeopleSoft and Cross-Platform

We rate Approva's BizRights suite as strong positive because of its breadth of capability in all three categories of SOD control. Although Approva is one of the more expensive products that we evaluated, it is the only product set that we recommend for cross-platform usage because of its application-independent design. It is the only three-technique product with substantial cross-platform production use. Approva's capabilities are comparable to SAP's in functionality, but because Approva is a relatively small company (slightly more than 200 people), it may be an acquisition target. Approva and SAP have the strongest teams in both size and experience to address SAP SOD issues. While SAP's Virsa acquisition makes SAP able to address cross-platform requirements, Approva has more production clients. In addition, Approva's neutral position makes its cross-platform capabilities more credible than SAP's in the long term.

Shortlist: Approva should be on the shortlist of every organization that needs strong support for all three techniques, especially those organizations that need to support multiple platforms or those that prefer an independent vendor.

Control Software International

Rating: Promising

Technique 1: Static Analysis (Gartner Recommends)

Technique 2: Provisioning Support (May Meet Requirement)

Technique 3: Transaction Monitoring (Gartner Recommends)

ERP: SAP Only

Control Software International is part of the CSI group, which is a 60-people consulting organization with a small dedicated team (five people) that has developed an inexpensive stand-alone toolset on top of Microsoft Access (MS Access) to address SOD issues. CSI Authorization Auditor is notable for its ability to download a transaction set that is integrated with the static permissions analysis making remediation easier. These products should be considered "low end" (technically oriented) expert applications for security administrators and auditors as a first step in SOD analysis automation. A new .NET-based product (launch planned in early 2007), called "CSI Accelerator," will provide greater GRC functionality, such as integrated provisioning workflow as well as documenting risks, control objectives and control measures, but it was not reviewed for this MarketScope. We rate them as “promising,” but the company will have to demonstrate a greater commitment to the software business to maintain or improve this rating.

Shortlist: Organizations outside North America or smaller organizations inside North America with technically capable security and audit professionals that are also interested in bundled services should put Control Software International on their shortlist.

D2C Solutions

Rating: Caution

Technique 1: Static Analysis (Gartner Recommends)

Technique 2: Provisioning Support (May Meet Requirement)

Technique 3: Transaction Monitoring (May Meet Requirement)

ERP: SAP Only

D2C Solutions has a small customer base with a unique analysis approach that is somewhat unproven. However, it is currently in the middle of an ambitious set of new product introductions, and its 2007 story is more compelling. The company employs a unique analysis method in which transactions are grouped into business activities that are then grouped into processes. D2C then analyzes risk at the intersection of the processes, ostensibly simplifying the analysis. C-Advisor also currently provides role modeling across multiple applications simultaneously, which is tantamount to a form of role management for enterprises (RME). The new C-Provision product adds role analysis, approval chaining and workflow, albeit only for SAP. Claiming efficiency and scalability concerns with competitive approaches, C-Advisor identifies not only SOD exposures in a risk-prioritized dashboard, but also non-SOD forms of unwanted access.

We rate D2C as "caution" because it is challenged in multiple ways: It is small, and it is offering what is purportedly a new, but mostly unproven, technical and process model. Compounding these two significant challenges is the company's ability to credibly explain to the market how its product functions without reliance on mechanisms — such as rules — used by the other vendors. D2C's approach may well turn out to be superior, but to succeed, it will need to provide both a competitive story and a larger body of practical customer evidence. We find D2C’s product road map interesting and recent customer wins a good sign, but organizations need to carefully compare their requirements to D2C capabilities based on their size and the maturity of their offerings. The RME market is heating up rapidly, and DC2 might have a play there, even if its SOD product doesn't gain traction in the next 12 months.

Shortlist: Small-to-midsize SAP-based businesses looking for a right-size supplier, or other organizations looking for the potential ability to influence their supplier's feature set, may find that a smaller, less-established company such as D2C offers useful flexibility.

LogicalApps

Rating: Positive

Technique 1: Static Analysis (Gartner Strongly Recommends)

Technique 2: Provisioning Support (Gartner Strongly Recommends)

Technique 3: Transaction Monitoring (May Meet Requirement)

ERP: Oracle only

LogicalApps is focused on Oracle SOD issues, providing tightly integrated capabilities for the Oracle platform in all three process areas. Well-established within Fortune 100 organizations, LogicalApps uses embedded agents within the Oracle platform that are able to modify Oracle application behavior, thereby restricting the options visible to Oracle users, including administrators. For static analysis and detection (Technique 1), LogicalApps provides a comprehensive set of capabilities, including proactive "what if" modeling.

Where Oracle does not provide "out of the box" rule sets for Technique 1 SOD analysis, LogicalApps does. For organizations not wanting to use Oracle Internal Controls Manager (ICM) to document exceptions, LogicalApps provides its own capabilities. For Technique 2 compliant provisioning, LogicalApps provides tight integration with the native Oracle administration tools, and it can prevent the creation of a user that would violate SOD policy — one of the few products in this MarketScope that has this capability in the ERP platform's native provisioning system versus the use of an external Web-based tool. Integration outside of the Oracle platform is minimal and requires the future v.7.2 of ACTIVE Governance. This will provide the necessary application programming interfaces (APIs) for external third-party IAM platform integration, including connectors for Sun and Oracle for integration with third-party UP solutions.

LogicalApps added Technique 3 analysis in 2006 with its ACTIVE Governance platform. However, this capability is not used to identify SOD violations in a way that facilitates and prioritizes Technique 1 SOD remediation efforts.

Shortlist: Organizations looking for a tightly integrated Oracle solution from a vendor — complete with out-of-the-box pre-defined rule sets for SOD analysis — should consider LogicalApps.

Oracle

Rating: Caution

Technique 1: Static Analysis (Gartner Recommends)

Technique 2: Provisioning Support (Gartner Recommends)

Technique 3: Transaction Monitoring (May Meet Requirement)

ERP: Oracle Only

Oracle provides ERP SOD analysis as an integrated part of its ICM platform. Although ICM provides rich controls management capabilities, we are only evaluating its SOD capabilities for this MarketScope. Unlike most of the other vendors in this document, Oracle does not supply a pre-populated set of rules for SOD analysis. Oracle partners with audit firms and systems integrators to configure SOD rules in ICM, which means that Oracle customers either will take longer to implement a useful set of controls on their own or will increase costs by contracting a third party. Oracle states liability concerns as the reason for this; however, it is the only vendor, large or small, to take this position. A substantial part of the value of the other SOD analysis products lies in the intellectual property encapsulated in the pre-populated rule set, which Oracle lacks. For this reason, we rate ICM as "caution" until Oracle integrates SOD rule knowledge into the product.

ICM has no capabilities to perform cross-platform analysis outside of Oracle's own applications. For Technique 2 proactive SOD modeling and prevention, Oracle ICM has these capabilities and can perform compliant provisioning for Oracle users; however, although Oracle has UP capabilities in other platforms with its Oracle Identity Manager (acquired from Thor Technologies in November 2005) — it does not yet have the ability to perform compliant provisioning to these platforms. This is expected in Oracle Identity Manager 9.1, which is targeted for the second quarter of 2007. In general, we recommend organizations considering ICM wait for Oracle to step up to providing basic rule sets.

Shortlist: Oracle customers that have a good handle on their SOD processes and that have performed a cost analysis, which includes the required third-party configuration work to implement ICM for SOD, should consider Oracle.

Oversight Systems

Rating: Promising

Technique 1: Static Analysis (May Meet Requirement)

Technique 3: Transaction Monitoring (Gartner Strongly Recommends)

ERP: SAP, Oracle, PeopleSoft and Others

Oversight Systems' historical strength has been in the after-the-fact analysis of ERP transactions (Technique 3 analysis) across multiple heterogeneous platforms, primarily for North America-based companies. Oversight's analysis of transactions goes beyond SOD analysis (for example, fraud, duplicate payments, collusion and so on). Oversight's core intellectual property lies in its ability to convert transactions from heterogeneous systems into a "common ontology" for cross-platform analysis. The ability to analyze executed transactions for SOD violations and use that as a starting point for SOD remediation is a pragmatic and desirable characteristic for any SOD analysis tool. However, auditors will want to see that organizations have put in place a process to address potential SOD violations, not just those that have been seen in actual transactions.

Oversight first introduced static SOD analysis capabilities in 2006, so its technology doesn't have the broad customer adoption that earlier entrants have. However, Oversight prices its static analysis capabilities aggressively, using static SOD analysis as an evolutionary stepping stone to broader transaction analysis. Oversight has no capabilities for Technique 2 compliant provisioning, characterizing it as a distraction from its core capabilities. Even so, we feel that Oversight should provide out-of-the-box capabilities for organizations to integrate with their incumbent UP systems.

Shortlist: Organizations looking for broad transaction analysis capabilities in addition to SOD analysis should consider Oversight.

SAP

Rating: Strong Positive

Technique 1: Static Analysis (Gartner Strongly Recommends)

Technique 2: Provisioning Support (Gartner Recommends)

Technique 3: Transaction Monitoring (Gartner Recommends)

ERP: SAP (Strong); Partial Support for Oracle, JD Edwards and Other ERP

Originally very weak in this area, SAP acquired Virsa Systems on 12 May 2006, and now offers one of the strongest product sets in our analysis, comprehensively addressing all SOD issues across multiple SAP instances. Products include Virsa Compliance Calibrator, Virsa Firefighter for SAP, Virsa Role Expert and Virsa Access Enforcer. SAP has one of the most robust client bases, but it also has one of the most expensive product sets. Compliance Calibrator is capable of running on multiple ERP platforms, and customers have reported that it is flexible on non-SAP systems. However, it is not recommended at this time for multiplatform use, as we find few organizations that are doing so in production use. Organizations with ERP systems from multiple vendors should carefully analyze their requirements and SAP's offering before choosing it, especially if SAP is not their primary ERP system.

SAP's long-term credibility for addressing SOD issues on the Oracle platform is questionable. SAP's SOD functionality has been completely subsumed by its GRC positioning and direction. This broad GRC vision encompasses multiple elements of enterprise risk, beyond just those represented by the ERP system. Although SOD functionality represents the core of the current GRC product offering, it is not SAP's focus. Gartner clients should evaluate the relevance of SAP's full GRC functionality to their requirements as part of their selection process.

Shortlist: SAP-centric organizations willing to pay for one of the best and most comprehensive capabilities and/or are interested in pursuing SAP's developing GRC functionality should put the SAP offerings on their shortlist.

RECOMMENDED READING

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Best Practices for Role-Based Separation of Duties in ERP"

"Select and Implement Appropriate Controls for Regulatory Compliance"

"Implement 10 Elements of a Good Control Environment to Address Compliance"

"Magic Quadrant for Finance Governance, Risk and Compliance Management Software, 2007"

Note 1
Reasonable and Appropriate Controls to Address SOD Conflicts in ERP Systems

Very few "governance" regulations include specific guidance as to exactly what practices must be followed to be considered compliant. Organizations are forced to use their own criteria to select reasonable and appropriate controls to protect against reasonably anticipated risks, and document their decision process adequately to make a defensible case that they selected appropriate controls (see "Select and Implement Appropriate Controls for Regulatory Compliance"). A good example of this is the response to Section 404 of SOX. Requiring organizations to address reasonably anticipated risks that may result in a material impact on their financial reporting is encouraging auditors to increasingly focus on SOD in ERP systems.

SOD is a control concept that essentially means the "fox should be explicitly prevented from watching the henhouse." A traditional application of this control is requiring the audit department to report outside the chain of people it is auditing to reduce conflict of interest. In the context of an ERP tool, it is expressed in controls over finance activities, typically preventing a single person from having the permission to both create and pay a vendor. Arguably, SOX requires organizations to control such conflicts to a defensible level (see "Best Practices for Role-Based Separation of Duties in ERP").

Note 2
IAM and SOD for ERP

Gartner includes the SOD for ERP market as a component of the overall IAM solution (see "Hype Cycle for Identity and Access Management Technologies, 2006") set, because the products provide SOD (entitlements management and enforcement from an access control perspective), automated provisioning of user access and role management capabilities for the ERP application set. However, two other components in the IAM solution — UP and RME — provide similar capabilities, albeit not at the depth of knowledge required for the ERP application space.

Today, all three product markets — UP, RME and SOD for ERP — are complementary; and all three are needed to address the complete identity management needs of the enterprise that has an ERP application (many don't). Individually, these different product types handle provisioning, roles and SOD at different levels of granularity, but none currently address transaction-level knowledge of ERP systems that the tools in this MarketScope address:

- UP — Some of the SOD for ERP tools can provision within the ERP application, but few vendors are addressing the full UP needs of the enterprise, which include provisioning to the network, e-mail systems, nonmaterial business applications and associated infrastructure, and so on. UP products do just that.
- Role management — UP and RME tools handle enterprise roles from a security administration perspective. SOD for ERP tools handle roles that are specific to the ERP application — they don't even address all the roles that are needed on the host running the ERP system (for example, system administrator, database administrator, manager, and so forth)
- SOD management — SOD for ERP tools focus on preventing conflicts of SOD at the transaction level within the ERP application; UP and RME tools handle SOD conflicts from an access assignment perspective.

Role management for systems and applications is not a precise science. The understanding of what maximum set of privilege should be granted to any particular functional role varies greatly from one organization and situation to another. While some roles are clearly understood, and conflicts are easy to identify, most are not. For example: In the case of an extension of financial controls, a purchasing manager should not have the same access to certain systems such as the accounts payable application.

ERP UP and SOD situations are more easily defined. The roles have clearly defined tasks and a finite, well-understood set of transactions. Most ERP SOD conflicts can be defined within about 400 to 600 rules based on accounting principles. If defining SOD issues within enterprise applications and systems is still an art, it is close to a science within the rigid ERP environment.

Overlap already exists between the SOD for ERP market and the RME market for role management. However, SOD for ERP products dive very deep into the transaction processing and monitoring level of the ERP application; RME products do not. Gartner does not expect RME products to provide transaction-level capabilities. Therefore, Gartner expects that the UP and RME markets will be the likely convergence point — providing the ERP application role management capabilities — and leaving the SOD for ERP market to focus on the transaction processing and monitoring side of SOD management and compliance reporting.

For more information, see "Magic Quadrant for User Provisioning, 1H06," "SunTrust Implements Role-Based Provisioning to a Successful Conclusion" and "Principal Financial Group Successfully Implements Role Management."

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

In the below table, the various ratings are defined:

MarketScope Rating Framework

Strong Positive
Is a solid provider of strategic products, services or solutions.

- *Customers:* Continue investments.
- *Potential customers:* Consider this vendor a strong strategic choice.

Positive
Demonstrates strength in specific areas, but is largely opportunistic.

- *Customers:* Continue incremental investments.
- *Potential customers*: Put this vendor on a shortlist of tactical alternatives.

Promising
Shows potential in specific areas; however, initiative or vendor has not fully evolved or matured.

- *Customers:* Watch for a change in status and consider scenarios for short- and long-term impact.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this initiative or vendor.

Caution
Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas; assess short- and long-term benefit/risk to determine if contingency plans are needed.
- *Potential customers:* Note the vendor's challenges as part of due diligence.

Strong Negative
Has difficulty responding to problems in multiple areas.

- *Customers:* Exit immediately.
- *Potential customers:* Consider this vendor only if there are no alternatives.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509