Market Guide for SOD Controls Monitoring Tools

Published: 28 August 2017 **ID:** G00293793

Analyst(s): Anmol Singh, Brian Iverson

The shift to postmodern ERP and multienterprise business applications with complex authorizations introduces new risks that challenge conventional SOD controls. Security and risk management leaders must consider automated solutions to enhance control over fraud and security risks.

Key Findings

- Effective segregation of duties (SOD) controls can reduce the risk of internal fraud by up to 60% through early detection of internal process failures in key business systems.
- An integral part of broader identity analytics functions, SOD risk analysis and controls monitoring is difficult to achieve without a specialized commercially supported software.
- Incumbent spreadsheet-based and consultant-led practices for SOD risk management fail as topology shifts to post-modern ERP with functions sourced from multiple ERP vendors.
- The high cost of traditional ERP platforms, combined with low perceptions of value and lack of support alternatives, makes it difficult for security and risk management leaders to justify buy-in for an SOD controls monitoring product.

Recommendations

To deliver effective identity and access management (IAM) capabilities:

- Review existing SOD controls to identify key SOD issues and challenges that drive process inefficiency and noncompliance.
- Seek automation of SOD controls monitoring through use of commercially supported software to achieve enhanced control, process efficiency and cost reduction.
- Consider integrating and centralizing SOD controls for a hybrid application environment as enterprises increasingly adopt a fragmented ERP model.
- Make cost-benefit, control-value decisions based on realistic assessments of SOD risks and resulting business impacts when choosing SOD controls.

- Recognize and quantify process efficiency and operational gains for a strong buy-in justification, in addition to demonstrating the anti-fraud, auditing and compliance benefits.

Strategic Planning Assumptions

By 2020, more than 60% of organizations will make use of commercialized products or services to implement SOD control monitoring for complex business applications in addition to ERP.

By 2022, more than 30% of SOD vendors will extend SOD CM capabilities to other non-ERP applications and IT assets toward convergence with identity governance and administration (IGA) products, up from less than 10% today.

Market Definition

SOD controls monitoring tools are products that provide organizations with the means to detect, analyze and manage risks associated with SOD conflicts, sensitive access and other types of policy violations for applications with complex, role-based authorization models. These applications include ERP components sourced from vendors such as SAP, Oracle, Salesforce, Workday, Concur, etc., and play critical roles in support of key business processes.

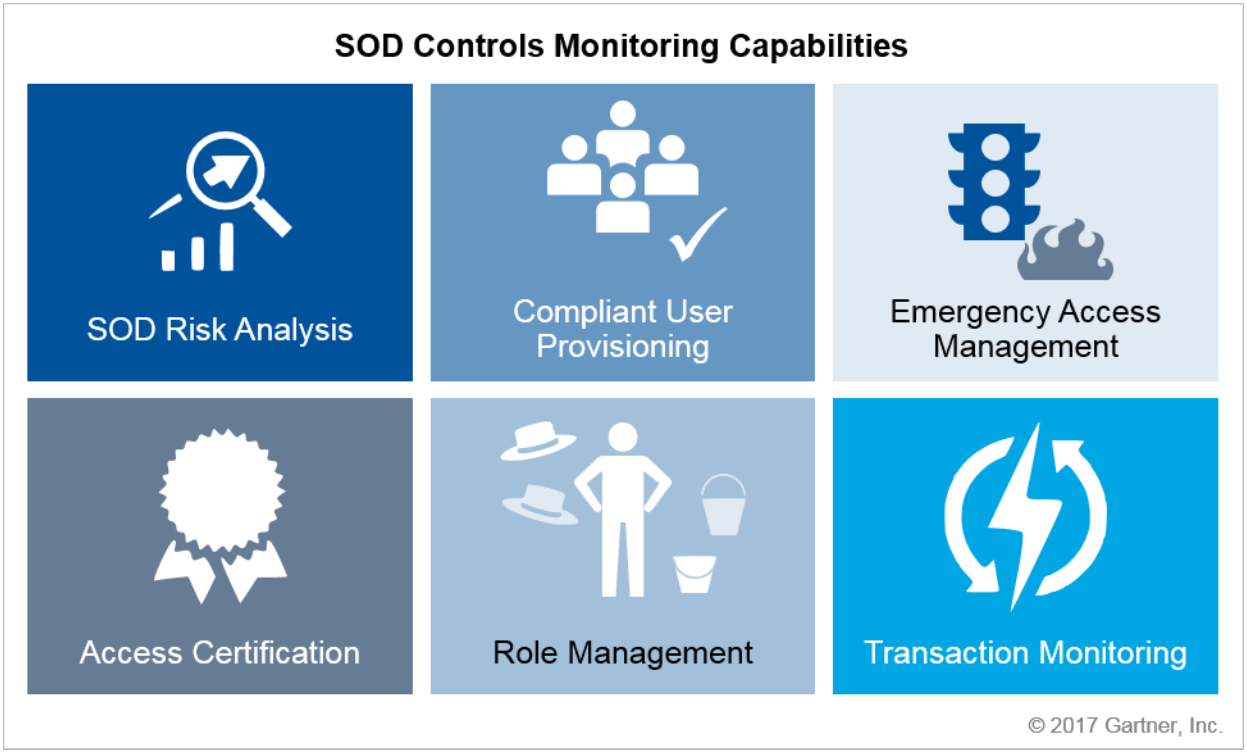
SOD controls increase the reliability of transactions, improve auditor trust and increase the effectiveness of anti-fraud controls. By detecting and preventing these violations of business rules, SOD controls greatly enhance the integrity of key financial processes and increase the availability of working capital.

When faced with audit and regulatory compliance requirements for enforcing SOD and other types of policies in complex organizations, most start with spreadsheet-based or consultant-driven processes for risk analysis and remediation. When such processes become too labor-intensive or too expensive to satisfy an organization's requirements, SOD controls monitoring tools can be used to automate the processes to provide more comprehensive coverage of risks, produce more timely reporting and enforce preventive controls (see "Detect and Prevent Internal Fraud With Effective SOD Controls").

Publicly held and other regulated organizations not only are accountable to their stakeholders to keep them informed of relative risk situation, but also must be prepared to defend their risk reporting through documentary evidence. In today's compliance-driven enterprise, this is frequently justification enough to undertake some level of SOD risks. However, most organizations that attempt to consistently and comprehensively manage SOD risks through controls automation also experience process and performance improvement. Ideally, SOD controls offer the compelling potential to treat occupational fraud risks, enabling business to reduce overall risk by offsetting access and authorization conflicts, and minimizing policy violations.

Modern-day SOD controls monitoring tools mainly offer six key capabilities (see Figure 1).

Figure 1. Key SOD Controls Monitoring Capabilities



Source: Gartner (August 2017)

1. **SOD risk analysis:** Detects SOD conflicts, sensitive access and potential policy violations for existing users through the use of business-oriented rules that are mapped to specific applications' authorization models. This extends beyond static rules built-in to preconfigured control libraries toward a dynamic modeling and analysis of SOD risks based on adaptive risk patterns.
2. **Compliant user provisioning:** Automates account provisioning and enforces preventive controls through validation of access requests, policy analysis and selection of mitigation controls (if necessary). Includes workflows for approvals, delegation and exception management.
3. **Emergency access management:** Provides users with temporary access to elevated or conflicting privileges and monitors usage of the access. Includes exception and remediation management for tracking the response to identified control failures and other deficiencies, along with the process of addressing exceptions.
4. **Access certification:** Automates the periodic recertification of users' access by supervisors, role owners or process owners.

5. **Role management:** Provides mechanisms for role design as a means to reduce SOD conflicts and improve administration efficiency. This usually includes a mechanism for transporting new or updated role definitions into appropriate application environments.
6. **Transaction monitoring:** Reporting and analytics in support of trending and audit analysis, audit trails, dashboards, and the generation of reports. Analyzes and monitors ERP and other financial application transactions to identify exceptions to policies, business rules and built-in applications, and responds accordingly.

This Market Guide focuses on SOD controls monitoring products and services that support risk analysis along with at least two other key features that can be applied to applications with complex, role-based authorization models. Gartner recommends using the vendor analysis provided in this research to assess their capabilities that go beyond static risk analysis and transaction monitoring toward adaptive risk analysis and contextual transaction monitoring.

Market Direction

There are multiple trends that appear to be driving changes in the market for SOD controls monitoring:

- **Move to the cloud:** New vendors are entering the market with cloud-based solutions that promise faster time to value and lower costs than traditional products that are deployed on-premises. Most existing vendors are also adapting their existing offerings for cloud-based delivery.
- **Risk analysis becomes adaptive:** Hard-coded static rules for authorization mapping and risk analysis are no longer effective in analyzing the SOD risks of a multienterprise business environment. Adaptive mechanisms can overcome these limitations and prioritize risks by measuring risk exposures of SOD conflicts in a multienterprise ERP environment.
- **SOD capabilities from IGA vendors:** IGA vendors such as Saviynt, AlertEnterprise and IBM have varied capabilities across SOD risk analysis, role modeling and transaction analytics for ERP and non-ERP applications with complex authorization models.
- **Expansion beyond traditional ERP and financial applications:** Vendors are starting to recognize the need to apply enhanced controls for applications beyond the traditional focus areas, such as CRM, supply chain management (SCM) electronic health record (EHR), student information system (SIS), human capital management (HCM), and travel and expense management (T&E) applications. Vendors such as Fastpath are making an entry into the deep waters of IGA by expanding key SOD controls to enterprise IT assets such as enterprise file synchronization and sharing (EFSS) systems (including SharePoint and other document management).
- **Cross-platform ERP support:** Although SOD controls monitoring tools were developed to target a specific business application, most solutions offer data models that can accommodate multiple applications with complex, role-based authorization models. More vendors are now developing risk analysis content and connectors for multiple applications, which promise to

offer access to automated SOD controls monitoring for complex business applications from vendors that may be underserved by the market.

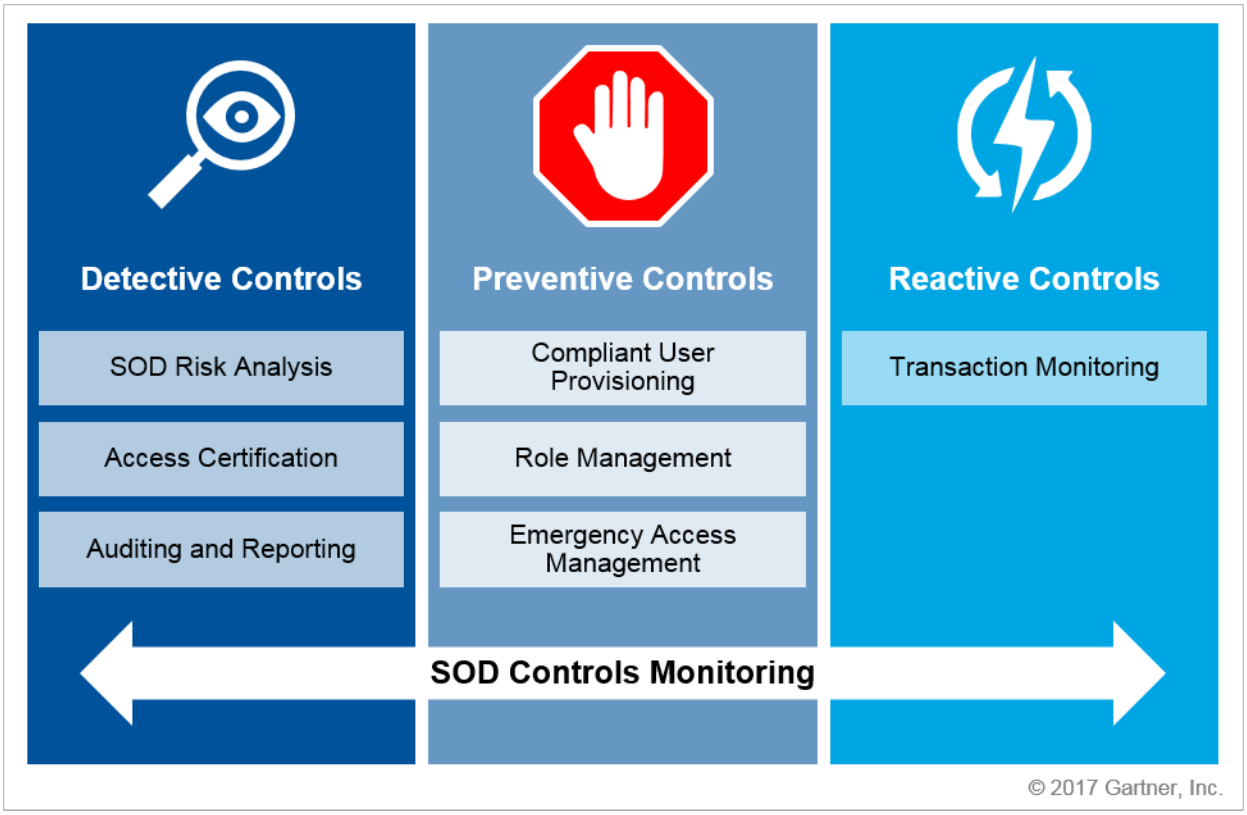
- **Support for postmodern ERP environment:** As postmodern ERP introduces several federated and loosely coupled ERP components sourced from multiple cloud providers and business process outsourcers, vendors are starting to focus on building controls to reduce multivendor complexity and support overheads by adopting a common platform for cross-application SOD risk management.
- **Intelligent transaction monitoring:** Transaction analytics will become contextual by incorporating real-time contextual information about the user, application, device and network involved in the transactional activity for determination of associated risk. Contextually derived attributes can be very helpful in detection of fraudulent transactions, especially in a hybrid ERP environment.
- **ERP license optimization:** Vendors increasingly offer ERP license optimization capabilities to reduce recurring license costs through an in-depth analysis of active roles and usage patterns. This capability allows organizations to identify dormant authorizations for potential cost reductions and gain better visibility into costs associated with each role assignment or modification. Vendors such as Security Weaver go one step ahead in offering license simulation for contract negotiations.
- **Internet of Things (IoT) enablement:** As organizations realign internal ERP resources based on IT strategy to enable IoT value-added business outcomes, vendors are starting to build capabilities to support industry-specific IoT-related processes that provide differentiation and meet integration challenges required to succeed with the strategy.

Market Analysis

The key capabilities provided by SOD controls monitoring tools can largely be classified under three major control categories: detective, preventive and reactive (see Figure 2):

- **Detective controls** provide capabilities to detect existing SOD violations based on rule-set mapping, auditing, reporting and access certification processes. Typically, a risk-based classification of identified SOD conflicts follows for remediation.
- **Preventive controls,** such as compliant user provisioning and role management, ensure that potential SOD conflicts are detected and remediated before they are introduced into the system.
- **Reactive controls,** such as transaction analytics, are useful in detecting SOD violations, responding to them and tracking remediation.

Figure 2. Control Categories for SOD Controls Monitoring Capabilities



Source: Gartner (August 2017)

The vendors in the SOD controls monitoring market offer a mix of control capabilities across the board. Most SOD controls monitoring tools exhibit at least two or more of the six key controls discussed in detail below.

SOD Risk Analysis

Risk analysis is generally carried out by applying predefined rules to the users and associated roles in the ERP system. SOD conflicts and other access risks such as sensitive access are evaluated by mapping from a predefined business process model, perhaps based on a reference model like APQC, into an application's authorization model.

The granularity of rules correlating users and associated roles can vary depending on the product and the organization's focus to identify and remediate SOD conflicts. Highly granular processing of detailed privileges results in a thorough analysis but requires more effort in terms of rule definitions and more processing resources, and is typically achieved at a higher cost. Less-granular analysis involving group-related transactions at the role and business process levels delivers faster performance and is typically offered at a lower cost, but must still meet the SOD requirements established by the auditor.

An effective SOD product will have a built-in rule set that identifies generic access conflicts at different levels of risk and criticality. Most vendors provide bundled rule sets with varying capabilities to build, customize and enhance the rules based on an organization's own processes, requirements and usage information. The rule base provided with such tools is based on the experiences of multiple organizations and can be considered as best practices. The use of an existing rule base can greatly improve the ease and accuracy of the assessment phase. It also provides a starting point for definition and significantly reduces the amount of customization needed during implementation.

Organizations with minimal to modest SOD requirements have reportedly been able to detect 70% to 80% of SOD risks in their environment by using this technique. As this is one of the foundational requirements of an SOD product, all vendors in the SOD market are able to meet the control criteria.

Compliant User Provisioning

Once existing SOD risks have been identified and accounted for, it is important for organizations to ensure that provisioning of access privileges for new users does not reintroduce these risks. As part of the SOD remediation process, organizations should ideally address the root cause by identifying and preventing SOD conflicts before the roles are assigned to users. Compliant user provisioning can be achieved by:

- Integrating directly with the ERP system to prevent provisioning of new users and assigned roles in the system until the associated SOD conflicts are addressed. This is normally tied to online risk analysis functions to deliver conflict decisions in near real time.
- Enforcing role simulation and modeling functions into an existing external third-party provisioning workflow process that identifies potential SOD conflicts created by the proposed set of privileges.
- Owning the provisioning workflow to enforce the role modeling function, carrying out detailed risk analysis of potential conflicts being introduced, triggering risk-based approval workflow and suggesting appropriate role remediation measures.

Vendor products offer varying strengths and levels of integration for compliant user provisioning. Most provide either out-of-box connectors or web-service-based integration with third-party provisioning tools to offer request and approval workflow functionalities. Few have partnered with other vendors in the market to provide advanced compliant user provisioning capabilities.

Traditionally, most IGA products have been reluctant to offer out-of-box rule sets for SOD analysis. However, this reluctance is changing as:

- More clients ask for IGA capabilities to integrate with ERP systems and other enterprise systems, such as CRM and HR management systems.
- The focus of IGA products shifts toward providing enhanced role management, governance and compliance capabilities.

We expect to see greater convergence of SOD functions with IGA products in the next two to three years.

Emergency Access Management

Emergency access management allows users to take responsibility of tasks outside of their normal job functions. This capability grants temporary elevated access to users to perform sensitive transactions in the system when assigned with responding to an incident or problem, while being closely monitored and audited. This includes, for example, when developers need temporary access to production to fix code or data to allow for proper processing of transactions, or when people with responsibilities for tasks that would normally result in SOD conflicts or sensitive access risks (such as responsibility for monthly or quarterly close activities) can use emergency access instead of running with these elevated permissions for routine activities.

Vendors in the SOD controls monitoring market mainly offer two approaches for emergency access management:

- **ID-based emergency access:** A user requests access to the emergency ID in the system to carry out the required task, providing the reason for access and the details of expected activity. The credentials for ID are checked out to the user upon approval and all changes made to the system are recorded under the emergency ID.
- **Emergency role-based access:** Emergency roles predefined in the system can be assigned to the user upon request. In some cases, the emergency role assignment can be soft-approved for certain users based on type of transaction activity to be performed.

Some vendors also provide integration with privileged account management (PAM) tools to leverage advanced emergency access controls and monitoring capabilities offered by these tools.

Role Management

Role management is an essential preventive control to support the creation of SOD conflict-free roles. Organizations not only should take due care of SOD conflicts while role designing and assignment, but also should periodically review the roles for any unauthorized modifications, accumulation of access and proliferation of roles over time. An effective role management practice allows role owners and system administrators to create and maintain consistent SOD conflict-free roles across the enterprise's systems. The role management provided by SOD controls monitoring tools applies to roles that are maintained within applications that provide their own role management frameworks as part of their authorization models.

Most vendors offer an access simulation capability, enabling administrators and role owners to perform "what if" analysis at various stages of a role's life cycle management and support compliant user provisioning. In a typical role-based access control (RBAC) setting, role life cycle management includes these six features for managing SOD conflicts within ERP systems:

- **Role design —** Logical grouping of access privileges by business functions. The work is done in the tool on a model of roles for the target application, rather than working with live roles for the target application.

- **Role governance —** Seeking consent of business and role owners, including workflow-based role analysis and approval capabilities. Changes to role definitions can be subject to oversight by requiring approvals and other conditions be met before new definitions can be released into a target application. Sometimes this is used to enforce a software development life cycle process over role definitions, where candidate roles would need to be tested in a test environment before being available for release into production.
- **Role transport —** Implementing of roles in production.
- **Role assignment —** Assigning roles to users, including integration with a compliant user provisioning capability. This is an alternative, administrative way to assign roles that is distinct from what is typically done with compliant provisioning.
- **Role modification —** Making changes to roles, including an audit trail of all role modifications.
- **Role maintenance —** Maintaining roles on an ongoing basis to keep the role information current, including role optimization and consolidation based on role usage analysis.

Most products in the SOD controls market offer a combination of these role management capabilities. SOD analysis must be performed during role design and approval processes to generalize the use of roles across these systems. Some vendors also provide advanced role discovery and mining features using top-down or bottom-up approaches for other enterprise applications with a complex role-based authorization model.

Enterprises must decide how broadly and deeply to embed SOD controls within enterprise role management.

Access Certification

This feature provides the necessary workflow support for process and role owners to collect and manage attestations that users only have the access privileges required to perform their job functions. It facilitates faster and accurate access reviews of user privileges by highlighting conflicting permissions in users' access entitlements across multiple applications that are to be revoked or approved under listed exceptions.

Although many vendors offer detailed built-in access certification features similar to what is available from IGA tools, these typically are not as detailed as those provided by leading IGA tools, such as SailPoint and Oracle.

Transaction Monitoring

This feature allows for continuous monitoring of ERP and financial applications to improve financial governance and audit processes by detecting privilege conflicts and preventing unauthorized transactions.

Transaction analytics provides the following capabilities:

- Imports periodically data from ERP and other financial applications to apply a set of predefined toxic role combinations to correlate events and identify fraudulent transactions involving SOD conflicts
- Supports continuous monitoring to ensure that controls operate as designed and transactions are free of SOD conflicts
- Supports the prohibiting, notification and alerting of SOD conflicts occurring in real time
- Provides reports and analytics to support trending and audit analysis, dashboards of risks, and the generation of reports including impact statements of actual and potential SOD violations
- Supports exception and remediation management by tracking the responses to identified SOD failures and the processes of addressing exceptions

Implementing transaction analytics at the beginning of SOD remediation projects can help security and risk management leaders understand the scope and trend of privilege conflicts that have occurred. During the early stages of the clean-up process, transaction analytics can detect the pattern of conflicting permissions and other policy violations, offering prioritization of these conflicts for earlier remediation. Once the findings are remediated, this becomes useful as a continuous control to ensure that no SOD conflicts appear unexpectedly in the transactions. Transaction analytics can also be used to mark and monitor the use of risky, yet approved, permissions on the exceptions list.

Many vendors provide their own library of toxic role combinations and various internal controls for the monitoring of transactions to restrict SOD violations occurring in real time. Organizations that have proactively deployed these capabilities are reportedly able to detect and prohibit 70% to 80% of SOD and other access control violations occurring in real-world transactions.

Market Size

While new vendors entering this mature market find it challenging and somewhat disappointing to compete with existing players, the foundational concept of the SOD controls monitoring market remains strong. The vendors with a realistic understanding of ERP market trends and differentiating features continue to grow at a healthy rate.

Overall, the market for SOD controls monitoring within ERP and financial applications has continued to grow at a compound annual growth rate (CAGR) of more than 20% during the last five years. It is estimated that the market will cross the $850 million mark in total software and service revenue by the end of 2017, representing an annual revenue growth of 21% over last year.

Among vendors that provided revenue information, revenue growth through 2014 was in the range of 7% to 120%, with a median growth rate of 27%% in 2016, compared with 34% in 2015. The vendors observed an average growth rate of 28.4% in 2016.

Consistent with ERP implementations, SOD controls monitoring tools are long-tail software with an average life span of 10 to 20 years, making software upgrades and maintenance a recurring and significant revenue generator for many vendors — even exceeding license revenue in most cases.

The market is largely dominated by global vendors that provide SOD controls monitoring tools for specialized ERP systems. The midsize and small vendors combined only represent one-third of the overall market size. We estimate this disparity to shrink as small and midsize vendors will continue to grow at a higher rate. These vendors will find growing demand in the market as more organizations, especially small or midsize businesses (SMBs), recognize the need for implementing enhanced SOD controls beyond ERP systems and across multiple enterprise applications at a reasonable price. Postmodern ERP represents a growth opportunity for the smaller vendors as they fill niches in the market that are underserved by the dominant vendors.

Pricing

The vendors in this market offer a mix of functionalities for each SOD controls at varied pricing options. Pricing models for SOD controls monitoring tools largely include perpetual licenses for on-premises deployments as well as subscription models for private hosted or SaaS-based solutions.

Overall, the prices for SOD controls monitoring products and services have mostly remained constant during the last couple of years (falling by 2% to 3% for on-premises and by 10% to 12% for cloud), toward lesser differentiation between on-premises and cloud solutions.

We asked vendors to provide information on their pricing models and average deal sizes. Here, we provide guidance on relative pricing expectations derived from the information gathered on three deployment sizes, including private cloud and SaaS-based delivery. Cloud is, on average, 51% less expensive than on-premises implementation over a period of three years.

Table 1 shows estimated annual pricing for an initial period of three years based on deployment sizes and organizational hierarchy.

Table 1. Estimated Pricing Based on Deployment Sizes and Organizational Hierarchy

Deployment Sizes	Average Price	
	On-Premises	Cloud
Small-Scale Deployments 1,000 users 50 to 100 roles Simple organizational hierarchy	$771,500	$563,000
Midsize-Scale Deployments 3,000 users More than 200 roles Moderately complex organizational hierarchy	$187,000	$119,000
Large-Scale Deployments 10,000 users More than 500 roles Complex organizational hierarchy	$455,000	$225,800

Source: Gartner (August 2017)

Market Penetration

The SOD controls monitoring market has experienced moderate, steady growth over the past three to five years, and its maturity level is characterized as mainstream with a market penetration of 30% to 50%. Although SOD controls monitoring tools have found the most interest in developed markets, they are also gaining traction in developing markets such as China, South Africa and India, where local regulators are increasingly emphasizing the role of SOD controls monitoring to combat fraud, bribery and other persistent risks.

The consumption of SOD controls monitoring tools spans across a range of industry verticals. However, highly regulated industries, such as financial services, banking and insurance, telecom, and healthcare, remain the largest consumers of these tools. Retail, manufacturing, and energy and utilities are increasingly adopting SOD controls monitoring tools as an extension of their governance, risk and compliance (GRC) policies. Adoption of these tools in the public sector and other similar industries like education is lagging significantly behind other industries.

Geographic Distribution

Table 2 shows the market revenue share by geography. The U.S. is the largest consumer of the offered SOD controls monitoring products and services, followed by EMEA. The consumption in the Asia/Pacific region is significantly lower, but we expect this to grow at a higher rate than in 2014 as vendors' focus shifts to SMBs and service localization.

Table 2. Market Revenue Share by Geography

Region	Percentage Share
Asia/Pacific	7%
Canada	3%
EMEA	33%
Latin America	2%
United States	55%

Source: Gartner (August 2017)

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

A summary of product offerings available in the SOD controls monitoring market from various vendors is provided in Table 3. The firms range from small, specialized providers to global giants that offer a range of capabilities. These include mainstream SOD controls monitoring vendors, as well as audit analytics and ERP security vendors, with significant presence in the market; some

notable smaller, specialist customer communications management (CCM) vendors; and vendors in adjacent markets (IGA, identity and access management as a service [IDaaS] and GRC) with notable SOD capabilities as part of their broader CCM capabilities. In Table 3, we present the representative vendors.

Table 3. Representative SOD Controls Monitoring Vendors

Vendor	Headquarters	Geographic Focus	Technology/Market Focus	Remarks
AuditBot	Delaware, U.S.	North America	SOD CM	
AutoSeg	Sao Paulo, Brazil	Latin America	SOD CM	
Brainwave	France	Europe	SOD CM, GRC, IGA	
CaoSys	U.K.	North America, U.K.	SOD CM	
CaseWare Analytics	Toronto, Canada	Canada	AA, CCM	
CSI tools	Belgium	Europe	SOD CM	
ERP Maestro	Florida, U.S.	North America	SOD CM	
ERPScan	Netherlands	Europe	SOD CM	Code Reviews, Vulnerability Management
Express GRC	Virginia. U.S.	North America	AA, GRC	Only Role Management
FastpPath	Iowa, U.S.	North America	GRC, SOD CM	
Greenlight Technologies	New Jersey, U.S.	North America	SOD CM, AA	
Infor Approva	New York City, U.S.	North Americа	SOD CM, AA	
Nasdaq BWise	Netherlands	Europe	AA, GRC, CCM	
Oracle	California, U.S.	North America, Europe	GRC, SOD CM, IGA	
Q Software	England	Europe	SOD CM	
SafePaaS	California	North America	GRC, SOD CM	AccessPaaS
SAP	Germany	North America, Europe	SOD CM, IGA	
Saviynt	California, U.S.	North America	SOD CM, IGA	
Security Weaver	California, U.S.	North America	SOD CM, AA	
Soterion	South Africa	Middle East and Africa	SOD CM	

Vendor	Headquarters	Geographic Focus	Technology/Market Focus	Remarks
Symsoft	Wisconsin, U.S.	North America	GRC	ControlPanelGRC
Mesaforte (wikima4)	Switzerland	Europe	SOD CM	
Xpandion	Israel	North America	SOD CM	

Source: Gartner (August 2017)

While most vendors focus on providing SOD controls capabilities specific to Tier A ERP systems such as SAP and Oracle E-Business Suite, a few vendors target Tier B ERP applications, and some even extend these capabilities across a wide range of non-ERP applications. Although most vendors have developed in-house capabilities and expertise, some are heavily reliant on audit and consulting firms to deliver a reasonable amount of customized SOD analysis for clients.

In Figure 3, we present the ability of representative vendors to support SOD risk analysis and controls monitoring across the range of ERP platforms. The tools from smaller, niche vendors are usually offered in highly modular configurations to allow them to deliver targeted functionality to fit a variety of budgets.

Figure 3. Support for ERP Platforms and Key Features

Vendor	SAP	Oracle	Microsoft Dynamics	Others	Cross-Platform SOD Analysis	Advanced Role Management	Transaction Monitoring
AuditBot	✓	×	×		×	×	×
AutoSeg	✓	✓	×	PS	×	×	✓
Brainwave	✓	✓	×	CashPooler, JDE, PS	×	✓	✓
CaoSys	×	✓	×		×	✓	×
CaseWare Analytics	✓	✓	✓		✓	×	✓
CSI tools	✓	×	×		×	✓	×
ERP Maestro	✓	×	×		×	×	✓
ERPScan	✓	×	×	PS	×	×	✓
Express GRC	✓	×	×		×	×	×
Fastpath	✓	✓	✓	NetSuite, SFDC	✓	✓	✓
Greenlight Technologies	✓	✓	×	JDE, PS, EO	✓	×	✓
Infor	✓	✓	×	PS, Infor Lawson, M3 and LN	✓	✓	✓
Nasdaq BWise	✓	✓	×	Infor M3	×	×	✓
Oracle	×	✓	×	EBS, JDE, PS	×	✓	✓
Q Software	×	✓	×	JDE, EO	×	×	×
SafePaaS	✓	✓	✓	EBS, JDE, PS, Siebel, SFDC, Workday	✓	✓	✓
SAP	✓	✓	×	EBS, JDE, Hana	✓	✓	✓
Saviynt	✓	✓	×	Oracle EBS, JDE, PS, SFDC, Workday, Hana	✓	✓	✓
Security Weaver	✓	✓	✓	JDE, PS, Infor M3 and Lawson	✓	✓	✓
Soterion	✓	×	×		×	×	✓
Symsoft	✓	×	×		×	✓	✓
wikima4	✓	×	×		×	×	✓
Xpandion	✓	✓	✓	EBS, Infor M3 and Lawson	✓	✓	✓

JDE: JD Edwards; EO: EnterpriseOne, Oracle EBS: Oracle E-Business Suite; PS: PeopleSoft; SFDC: Salesforce

Source: Gartner (August 2017)

Market Recommendations

SOD controls monitoring can reduce the load of compliance monitoring and reporting for key business applications. Funding these tools, however, can require a substantial investment. Most organizations start out with manual spreadsheet-based or consultant-driven approaches for evaluating SOD risks and reporting for auditors and compliance. The decision to automate some aspects of SOD controls monitoring with a tool is typically triggered by one or more of the following events:

- There is internal recognition that the current process is expensive, time-consuming, error-prone, inefficient or generally not cost-effective.
- An auditor makes the recommendation to pursue automation, perhaps because current processes are not defensible.
- A significant deficiency or material weakness is identified by auditors — or worse, by a regulatory investigation.

The most important consideration when selecting an SOD controls monitoring tool is whether it supports your organization's business applications that are in scope for risk analysis and compliance reporting. Most organizations start with risk analysis, reporting and emergency access features as baseline services when deploying SOD controls monitoring tools, so these should be the features that are initially evaluated.

It is then necessary to consider the organization's needs for more advanced functionalities, such as role management, access certification, compliant provisioning and transaction analytics. These are the areas where SOD controls monitoring tools will differ the most between vendors. It is more important to know what your organization's minimal requirements and process peculiarities are than it is to look for a product that checks the most boxes feature-wise.

Implementation cost may also be an important consideration. Some products can be very complex and require three to six months for deployment with significant professional services, while other products and cloud services promise much faster deployments.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Detect and Prevent Internal Fraud With Effective SOD Controls"

"Magic Quadrant for Identity Governance and Administration"

"IGA Best Practices: Take Control of Enterprise Role Management"

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp