


Insights on IT risk
May 2010



A risk-based approach to segregation of duties

The complexity of today's enterprise systems leaves many companies struggling with the basic internal control of segregation of duties.





Segregation of Duties (SoD) is top of mind for many professionals, from compliance managers to executive-level officers. The increased interest in SoD is due, in part, to control-driven regulations worldwide and the executive-level accountability for their successful implementation. However, the underlying reason for these regulations is more important: no individual should have excessive system access that enables them to execute transactions across an entire business process without checks and balances. Allowing this kind of access represents a very real risk to the business, and managing that risk in a pragmatic, effective way is more difficult than it seems.

If this concept is common sense, why do so many companies struggle with SoD compliance and why does it repeatedly stifle information technology (IT), internal audit and finance departments? In large part, the difficulty rests in the complexity and variety of the systems that automate key business processes, and the ownership and accountability for controlling those processes.

SoD is a basic internal control that attempts to ensure no single individual has the authority to execute two or more conflicting sensitive transactions with the potential to impact financial statements. Without proper guidance and a sound approach, SoD implementation, testing, remediation and mitigation may appear to be extremely difficult to achieve. However, a risk-based approach can make the effort manageable for a company of any size.

Companies don't need to create complex role structures or undertake expensive system overhauls in order to meet SoD compliance and the principle of least privilege. By focusing on the transactions that pose the greatest risk to the business, a company can quickly understand the issues related to access and determine – at a level that satisfies management and audit parties – that appropriate steps are being taken to remedy and mitigate the root causes of the issues.

This document outlines a practical, risk-based approach to SoD compliance.



Business drivers and regulatory compliance

Proper SoD is a long-established method of preventing fraud and maintaining checks and balances within a company. However, the recent regulatory focus on public companies has driven businesses to truly understand what access their employees have within their application portfolio. Control-driven regulations, like Sarbanes-Oxley in the United States for instance, have not only imposed an unprecedented rigor around controls, they also underscore the importance of an integrated IT and financial controls approach to managing risk within a company.

Across the globe, existing and proposed regulations continue to bring the issue of SoD and controls to the forefront of agendas for auditors and executives alike. These include the European Union's 8th Directive, which is viewed to some degree as Europe's SOX equivalent; J-SOX, the Japanese Sarbanes-Oxley version; and Basel II, which addresses the method that financial institutions use to calculate capital adequacy and its alignment with the company's risk profile.

The list of regulations continues to grow, and in response, compliance initiatives expand and consume corporate resources. As companies continually rationalize spending and optimize budgets, a pragmatic, balanced approach to internal controls is expected. Regulators have listened to companies' needs in order to move towards legislation and guidance that balances the level of effort required to understand risk. An example is the release of Public Accounting Oversight Board (PCAOB) Auditing Standard No. 5, which pushed companies and their auditors to focus more on risk and significant concerns that could affect the business and financial statements; a clear message that a risk-based methodology is fundamental to an effective and efficient internal control framework.

In summary, not implementing SoD as part of a robust framework puts the organization at risk of failing to meet regulatory and compliance requirements. But this is not the only risk.

The cost of fraud and other internal control failures is well documented in dollar values, which is where the cost starts to feel more real. In addition, other costs are often hidden, such as:

- ▶ Lost shareholder value because the market no longer has confidence in the organization
- ▶ Missed business opportunities because your organization's credit rating changes and financing becomes more expensive
- ▶ Costs to recover from reputational damage

A risk-based approach enables organizations to manage – but not entirely mitigate – these risks in a balanced and efficient way that reflects the value that is being protected.

A risk-based methodology

A risk-based methodology, such as the one discussed in this document, focuses on the issues that pose the greatest threat to the business and its financial statements. Whether the drivers for investing in SoD compliance are regulatory compliance, fraud prevention or a new ERP system, a company cannot eliminate every potential risk. Rather, the goal is to hone in on the risks that threaten pre-defined thresholds of value. These are typically determined at the outset of the SoD initiative. Materiality, fraud thresholds or financially significant limits quantifying the impact of realization of financial, operational or reputational risks are examples of thresholds that serve to measure the financial sensitivity of SoD conflicts.

SoD dictates that problems – such as fraud, material misstatement and financial statement manipulation – have the potential to arise when the same individual is allowed to execute two or more conflicting sensitive transactions. Sensitive transactions drive processes with the potential to impact a company's financial statements, operational activities or market reputation. Many companies strive for zero SoD conflicts in their user population, though this is often unachievable, unsustainable and unrealistic given the number of employees within a typical business function. Separating discrete job responsibilities into task-oriented roles can often result in inefficiencies and unnecessary costs.

Ultimately, it is critical for the company to understand and assess the landscape of current conflicts, reduce them to the extent possible for a given staffing model (via remediation initiatives) and apply mitigating controls to the remaining issues. This approach does not yield zero SoD conflicts, but demonstrates that management has evaluated existing conflicts and reduced residual risk to an acceptable level through tested and controlled processes. Typically, this solution is palatable to auditors, regulators and financial reporting stakeholders alike, and promotes the awareness of risk beyond a compliance-only exercise.

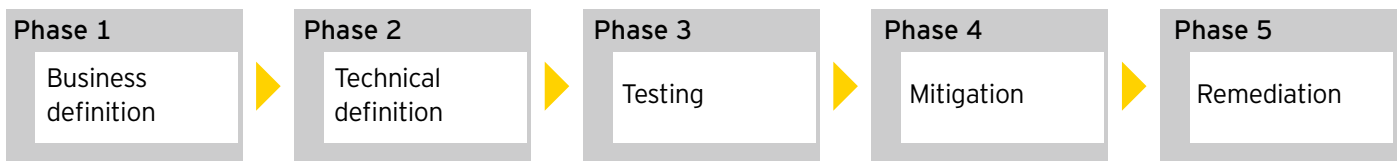
SoD glossary

- ▶ **Materiality** – the financial threshold or impact a potential SoD conflict can have over a company's financial statements
- ▶ **Principle of least privilege** – the concept that system users should have access to only the resources absolutely necessary to perform their job responsibilities
- ▶ **Segregation of duties (SoD)** – an internal control that attempts to ensure that no single individual should have control over two or more conflicting sensitive transactions
- ▶ **Sensitive transaction** – a business transaction with the potential to impact a company's financial statements
- ▶ **SoD conflict** – the pairing of two conflicting sensitive transactions or business activities



The SoD roadmap

Most successful SoD initiatives consist of five phases: business definition, technical definition, testing, mitigation and remediation.



Phase 1: Business definition

The objective of this phase is to gain an understanding of the scope of sensitive transactions and conflicts that drive the company's key business processes. These are also the transactions that pose the greatest fraud risk to the organization should someone possess excessive access. During this phase, thresholds are determined based on the risk and impact to the company for each potential SoD conflict pairing.

As this step lays the foundation for everything that follows; proper execution is critical. Many companies fail in this early stage by taking on too many conflict pairings that do not meet the threshold level of risk, resulting in onerous requirements that ultimately cannot be met or are excessively costly for the risks they are attempting to manage. For example, a company may be concerned with allowing the same individual to both create a vendor purchase order and modify the customer pricing master file. However, the combination of the two may constitute such a low risk that it does not warrant inclusion in the company's conflict matrix. It might be more appropriate to include potential conflicts for a user who could modify the vendor master file, create a vendor purchase order and issue payment to vendors as the combination represents the higher risk to the company.

Conflict matrix

The output of the business definition phase is a matrix of potential conflicts, independent of the supporting IT application driving each transaction, but including the corresponding risk statement related to each conflict. The risk statement answers the question, "Why do we care about this transaction pairing or combination?" and demonstrates what could go wrong should someone have enough

access or authority. The risk statement might say, "A user could create a fictitious vendor or make unauthorized changes to vendor master data, initiate purchases to this vendor and issue payment to this vendor." In this case, the "vendor" might be the fraudulent employee with an excessive and inappropriate level of access in the system.

Generally, the matrix and corresponding risk statements differ among companies, industries, business models and even locations within the same company, depending on what processes are significant. It is not uncommon for a large global company to have more than one matrix due to differences in the business processes by location or business unit. For example, a company may have a manufacturing business unit with a large amount of inventory, requiring an SoD matrix that focuses on specific inventory transactions. They may also have a service-based business unit necessitating a focus on project accounting, requiring a different SoD matrix. Though knowledge of similar businesses and industries can help to establish the conflict matrix, each business unit must perform a customized analysis of its conflicting transactions in order to capture the real risk for that particular business model.

Phase 2: Technical definition

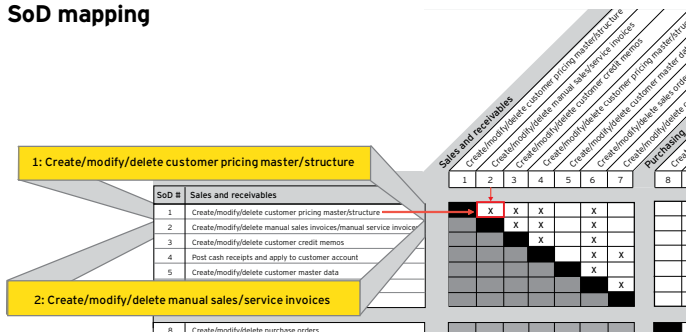
The technical definition uses the completed conflict matrix as a tool to help answer the question, "Which applications are able to execute the defined sensitive transactions, and how are they executed in the system?" The company or business unit must map each sensitive transaction to its associated access rights in the application that enable that transaction. This critical step feeds the data analysis when setting up access during implementation or to yield the testing results in live environments. While this mapping task may appear to be trivial, this step is often where many companies encounter problems due to a lack of understanding of the potential ways a transaction could be executed in a particular application.

Application mapping and exclusions

The application mapping is the rule-set by which sensitive transactions are tested in the relevant systems. For example, vendor-update rights may be executed through a series of menus within a given application. The presence of these menus assigned to specific users should be mapped, walked-through and documented in order for the company to accurately test for a particular conflict. The challenge is that in most modern applications there is more than one way to execute the same transaction. For example, there may be 20 ways to pay a vendor in an application, but the company may use only five of them. Moreover, the company is typically not aware of the other 15 ways and usually does not restrict access to or control these other methods to execute a vendor payment.

The risk-based SoD process requires a company to discover all the potential methods for executing a transaction in order to understand the full potential for fraud, not just the limited view of the known methods. Mapping all of the ways a user could potentially execute a transaction is critical to accurately depicting SoD.

SoD mapping



One of the key fallacies in menu (or access) mapping is that one only needs to map the transactions that are actually used in the application. While this method will usually capture many of the executed transactions, it will fail to identify the menus business users do not use but could use to execute a particular transaction. Even though menus may be deactivated or not provisioned to a set of business users, they must be mapped to be able to demonstrate they have been considered and it is possible to see the entire rule-set by which SoD conflicts are being tested.

Exclusions refer to the user IDs and menus or access rights intentionally omitted in the SoD analysis. Not every user ID that appears in the analysis represents a real conflict. Often system or process accounts, IT administrators, IT operations and support personnel may have access to multiple conflicting menus. This may not actually represent a conflict if the goal is to only capture the business users with SoD conflicts.

SoD testing application applicability (count) chart

SoD Group	Sales and receivables	Count of mapped access rights			
		Application 1	Application 2	Application 3	Application 4
1	Create/modify/delete customer pricing master/structure	14	0	0	31
2	Create/modify/delete manual sales invoices/manual service invoices	0	0	6	14
3	Create/modify/delete customer credit memos	0	0	5	19
4	Post cash receipts and apply to customer account	0	0	13	0
5	Create/modify/delete customer master data	2	0	9	7
6	Create/modify/delete sales orders/service orders	4	0	5	24
7	Create/modify/delete customer credit limits	1	0	0	0
Purchasing					
8	Create/modify/delete purchase orders	0	0	6	0
9	Create/modify/delete vendor master file data	0	0	3	0
10	Approve purchase orders	0	0	2	0
Inventory master data					
11	Create/change standard or actual costing	0	0	0	7
12	Create/change to material master data	2	0	1	7
Inventory transactions					
13	Record inventory movements or production	0	0	0	32
14	Record/modify shipment	1	0	0	0

Alternatively, to facilitate continuous controls monitoring, companies often include IT users in reports on standard sensitive transaction usage and SoD conflicts. Typically, read-only or inquiry functionality in the application should be excluded as it does not permit execution of sensitive transactions. Regardless of the treatment of the transaction exclusion, it is vital to document all omissions, their rationale and to communicate this information to regulators and compliance stakeholders.

Phase 3: Testing

The testing phase draws on data from the business definition and technical definition phases to produce an analysis of users with SoD conflicts. The results highlight the SoD conflicts in a number of ways – by user and by role and (or) group for example – and shows the extent of the conflicts among the company's user population. This analysis, in combination with the business and technical definitions, typically serves as the compliance testing package disclosed to management, audit parties and regulators.

Intra-application vs. cross-application testing

Very few companies have just one system or one single platform on which key sensitive transactions are executed. Transactions and financial statements are often processed through an interconnected portfolio of applications and automated business processes. Typically, users have access to numerous systems when executing a particular job function. This access across multiple systems often yields the potential for fraud and control issues. Consequently, it is essential that the company not only perform intra-application (i.e., within one application) testing, but cross-application (i.e., between two or more applications) testing to reveal the underlying risk of an SoD conflict.

Invariably, the question arises over which systems to include in the testing scope. The single consideration is whether any of these systems drive the sensitive transactions defined in the SoD conflict matrix. For example, identifying all the places with the potential to modify the vendor master file will yield the scope of applications to be included in testing for that particular transaction. If this capability resides in multiple applications, the company should include these applications in testing.

End-to-end processing

When a single individual is able to execute end-to-end processing of a transaction, this indicates a lack of control over the multiple steps within a single business process. Typically, in this scenario, a user can complete a whole process – from initiation and authorization to approval and execution – without any checks or balances.

This type of systemic problem can occur in lean workforces or departments where job responsibilities are shared (i.e., anyone can serve as a backup for anyone else). Data analysis may detect the same users in multiple conflict tests within a particular business process. If this scenario arises, the company may need to place special emphasis on the use of mitigating controls or consider fully remediating the issue by redesigning the process entirely.

This issue is especially important to company workforce downsizing. When employees who are in charge of key processes are released (and not replaced), job functions or roles are often combined. What was once a segregated access model now becomes a heavily conflicted population of users with significant control issues. Smart companies assess the SoD impact of employee terminations and plan accordingly prior to actual termination of personnel. Where formerly segregated processes must be combined, strong mitigating controls should be applied and monitored in the interim.

Conflict risk ratings

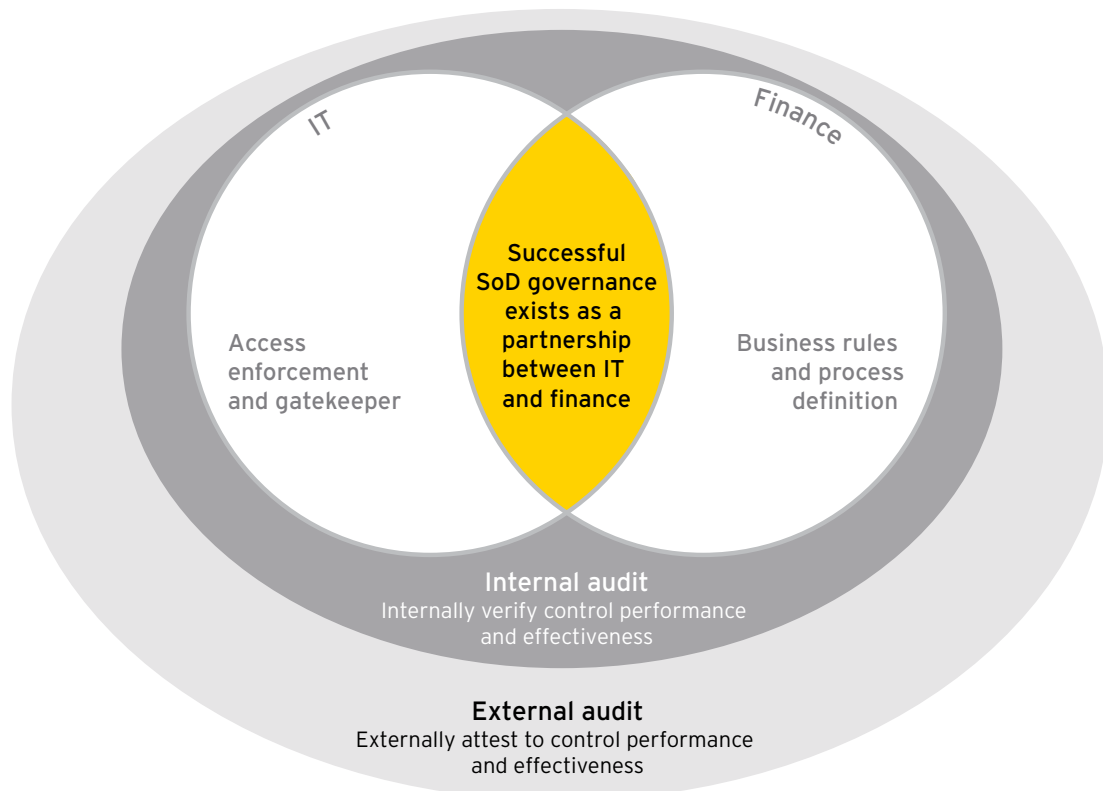
No two SoD conflicts are equal; each conflict poses a different risk to the business and ideally, each conflict should be rated according to the likelihood and impact of a user executing the conflicting transactions. Companies have adopted many schemes and notations for risk-ranking their conflicts. Companies have defined tiers of high, medium and low based on the output of their risk calculation. It is not uncommon to see conflicts deemed "prohibited" within the risk criteria, indicating conflicts that are unconditionally barred from provisioning. These are typically transactions that – when executed together – have no potential for mitigation, or there is no business justification for an assignment of conflicting access rights. Whatever the classification notation may be, it is important for the company to prioritize the conflicts so that remediation and management of the user population can be focused on those conflicts with the greatest potential for risk reduction.

The correct assessment and definitions of how to manage each of the risk ratings is a key factor in delivering benefits from a risk-based approach.



Testing considerations

- ▶ The tone at the top drives the level of commitment from all personnel. Many companies fail by placing little emphasis on SoD, resulting in significant concerns or worse, pervasive fraud and control breakdown.
- ▶ IT, finance and other management stakeholders must take co-ownership of the SoD process. Finance understands the financial impact associated with the business processes, risks and mitigating controls better than any other function. Business management will have the clearest view on the operational impact. IT understands how to translate that into system data, reporting and technical remediation. Either way, one organization cannot simply point to the other or transfer responsibility to the other party.
- ▶ In our experience where the driver for an SoD initiative has been an audit finding, it becomes extremely important for the company to work with its auditors on a regular basis. The auditors can often provide advice and feedback, helping to keep the process focused on risk rather than over-compliance.
- ▶ SoD is not a project, but a process. It needs to continue into the future. The longer term undertaking is much easier if tasks are performed properly early on, thus an investment in sound practices and processes today will inevitably yield savings down the road.
- ▶ Where a specific compliance deadline is driving an organization to address SoD, the timing of testing is critical. A company should not wait until the last minute to conduct the activities. Allowing for adequate time can help when controls need to be remediated and retested, or user access needs to be modified in the system. The testing timeline should be developed with the input of key business and IT stakeholders and the audit team(s). Proactive involvement of the auditors helps prevent unnecessary audit fees and allows for streamlined, efficient testing and reporting.



Phase 4: Mitigation

As suggested by the name, mitigation is the next step in limiting the potential impact of an SoD conflict violation. This mitigation phase can be completed concurrently with remediation; or depending on the objectives and compliance time frame, mitigation can be performed last, when conflicts have been reduced to their absolute minimum. Mitigation looks at each of the identified SoD conflicts and asks, "Which control is in operation to reduce the residual risk of a particular SoD conflict such that it does not pose a significant threat to the business?" In other words, can the company identify any existing controls that will prevent or detect the unauthorized or fraudulent activity? Many companies will choose to mitigate every potential conflict in order to have a safety net of control in place should a conflict arise. This is a sound and practical strategy for companies looking to control unforeseen or unpredictable risk.

Mitigation does not fix or correct the conflict; rather, it allows for the conflict to exist in the system and creates or cites existing controls that compensate for the risk of excessive access. When a company chooses to mitigate an SoD conflict, it accepts the risk associated with that conflict and attempts to compensate through the use of application, IT-dependent or manual controls (or some combination thereof). For example, a mitigating control typically seen in the vendor master update or vendor payment scenario is the use of automated approvals for vendor check writing or the use of month-end vendor reconciliations or reviews. These detective controls may provide management the comfort needed to allow the SoD conflict to exist while catching unauthorized activity through its financial controls.

When leveraging mitigating controls, management should develop a conflict-by-conflict analysis to document the existence of specific key controls that mitigate the risk related to the particular conflict. Management and the auditors can assess the strength of the mitigating controls and conclude the appropriate level of reliance to be placed on the controls' ability to manage – to an acceptable level – risk. This important aspect of the risk-based approach enables management to accept that certain conflicts will exist within their pre-defined tolerated levels of risk, thereby determining their residual risk threshold.





Mitigation considerations

- ▶ For financial risks, document the financial statement assertions related to the conflict risk. Specifically, the assertions and objectives addressed by the cited mitigating controls are:

- ▶ Completeness
- ▶ Rights and obligations
- ▶ Valuation or allocation
- ▶ Existence or occurrence
- ▶ Presentation and disclosure

This is important as it enables the company to demonstrate that the assertions related to the mitigating controls adequately address the assertions related to the conflict risk. The external auditor may also request that the controls map to their audit framework or methodology; it is advisable to work with the auditor to determine the relevant frameworks to which the mitigating controls are mapped.

- ▶ More than one mitigating control can address a conflict. Implementing a balance of preventative and detective controls helps manage the risk should one control fail and supports the use of a risk-based approach. While there is no ideal number of controls, a good rule of thumb is: more than one control is preferred, but one well-designed control is better than ten that do not compensate for the risk of the conflict. Mitigating controls should address a precise risk. Generally, it is insufficient to deploy “budget to actual reviews” as the mitigating control for all SoD

conflicts as this control is too general; granularity of controls is important when attempting to detect and prevent fraud or material misstatement. The conflict matrix should document precisely why each control mitigates the specific conflict risk. This will enable management to more effectively address risk and serves as a justification to auditors and regulators as to why the control was selected and its relevance as a mitigating factor.

- ▶ List who (name and job title) performs each of the mitigating controls in the company, since it is important to know if the person performing the mitigating control is also one of the conflicted users. The level of reliance that can be placed on the mitigating control is greatly reduced (if not eliminated entirely) when personnel who are in the conflicted population also perform the mitigating controls. Ideally, this scenario should be remedied through reassignment of the control to another non-conflicted user or elimination of the user from one or both of the conflicting sensitive transactions.
- ▶ In some cases, the company can mitigate an entire application or system without conducting any testing to determine the number of conflicted users in the system. Should the company find that there are a limited number of users in the system or the system covers a small number of potential conflicts (such as update vendor master), a memo explaining why testing does not need to be performed may be sufficient.

Phase 5: Remediation

The goal of the remediation phase is the permanent correction of SoD conflicts. Remediation techniques include role redesign, role cleanup, user appropriateness review and SoD tool implementation. A combination of people, process and technology changes help sustain effective control and compliance. There is no proscribed leading practice or method for remediating conflicts. Every scenario is unique, based on the degree of complexity and extent of the conflicts in a given environment.

Remediation initiatives generally fall into two categories: tactical cleanup of the user population and strategic role redesign. The tactical component represents the items that can be addressed quickly, while role development typically involves a full complement of organizational changes in people, process and technology. The choice of tactical or strategic paths is not an either-or proposition; most companies execute a combination of approaches in a phased time frame. The decision to pursue a particular remediation path depends on the complexity, degree of severity of the SoD conflicts and the mandated time line.

Tactical role clean up

Tactical user population clean up refers to the process of reviewing the role or security model to evaluate whether both sides of the conflicting transactions are required for a particular user to do his or her job. This clean up process requires the company to analyze a particular role and the conflicts that exist within that role in order to establish a clean, conflict-free role or security model.

Misconfigured roles and security models are often the source of SoD conflicts. For example, some applications are configured for maximum flexibility and agility – in other words, anyone can do anything. While this creates a very easy-to-use and flexible system, it can also result in control deficiencies if access is not separated through the customization of roles. Many companies have developed the security aspects of enterprise roles without considering the sensitive transactions that must be segregated. Roles alone cannot be used to test for SoD conflicts; rather, a company must look to the lowest level of security (i.e., menu item, screen, executable, transaction code) that make up a particular role to understand what transactions a user can execute. However, roles can be leveraged to correct SoD conflicts by creating a known effective role model, thereby establishing consistent enforcement of that model through the application's security controls. This short-term tactical role redesign can often easily correct many conflicts, while leaving the more difficult user conflicts to be addressed through a strategic approach.

Strategic role redesign

Strategic role redesign seeks to define what constitutes SoD conflict-free access across the company. It maps job function and responsibility in the business to the required access rights in each system. This approach is typically used when the existing role model is heavily conflicted and cannot be salvaged through cleanup initiatives. Strategic role design builds sustainable capabilities and processes that serve to maintain the "cleaned" role structure.

Once remediation is completed, relevant people, process and technology governance activities must remain in place to help ensure the situation does not arise again. It is critical to assign accountability for the tasks of role maintenance, user administration and SoD rule definitions. Periodic testing and conflict checks should be incorporated into provisioning processes. A critical success factor is to support the redesigned processes with the appropriate technology. For small organizations with very simple applications, this may be managed with a basic solution such as a spreadsheet which captures the conflicting activities and can perform straight-forward analysis to determine whether a user's access will result in SoD issues. However, for medium and large organizations (over 500 users) with more complex applications (e.g., ERPs such as SAP and Oracle), an access control tool will almost certainly be required to enable an efficient and sustainable solution. That said, while there are a number of third-party applications that facilitate testing, mitigation and some remediation activities, they do not replace the necessity for a sound methodology based on the business risk to the company.

Remediation return on investment

Initial investment in the people, processes and technology governing the SoD process can potentially yield:

- ▶ Reduced business risk
- ▶ Lower incidence of control features
- ▶ Avoidance of regulatory fines
- ▶ Savings in consulting hours
- ▶ A better control environment



Remediation considerations

- ▶ **Master record source** – When a company establishes a master record source, it has taken the first step in understanding the conflicting access rights in the system. A master record source is a single view of the user population and all associated access rights of users. Since many companies maintain disparate and disconnected user databases, this task is often more challenging than it sounds. The undertaking is easier when supported by policies such as standard user ID naming conventions. This makes it less difficult to compare a user ID for conflicting access across multiple systems. Otherwise, user IDs with a common identifying trait – such as employee number, email address and user ID – must be linked across various systems. For a company with thousands of employees and dozens of systems, this process can be tedious but it is necessary for an accurate view of the conflicts.
- ▶ **Default access** – Star or default access (known by many names depending on the system) provides the standard set of access rights to every user registered on that application. This default access provides a user with the system's standard minimum functionality. For example, all users of a particular system should be able to see the log-in screen, help menu and policy banner screen. These three screens or menus would be considered default access. Risk arises when companies assign default access to sensitive menus, transactions or security levels. Default access should be assigned sparingly and careful consideration given to any menu or security level to which it has been assigned.
- ▶ **Roles** – Roles are helpful to the management of any IT system in that they streamline the assignment of access rights and provisioning by aligning system access with job responsibility or function. This built-in logic enables non-IT personnel to assign required access when an employee is on-boarded. Yet for many businesses, the notion of roles is highly complex and controversial. Whether a company chooses to define its roles within one system or across many systems, SoD testing should be considered beyond the role level to account for various, discrete access rights. Many companies simply stop at the role level and do not seek to understand the security and access rights that constitute that role, yet conflicts are frequently identified within the role itself. Management will not uncover these issues through role testing alone.
- ▶ **Reviews** – User appropriateness reviews provide an easy and effective way to reduce the number of SoD conflicts revealed in the testing process. The activities of users without proper authorization and documented access can make it difficult for the company to define proper user access levels. Companies often find that users are granted additional access over time as their responsibilities and job functions change, but the de-provisioning of unnecessary (or inappropriate) access does not always happen, thereby further compounding the SoD problem. A careful review of the user population – determining whether users should have access to a particular role or group – can correct this situation. A simple check of the user population, in the context of job title or function, can be used to identify such SoD conflicts. Once identified, such SoD conflicts can be eliminated.
- ▶ **Non-standard IDs** – Non-standard user IDs and accounts indicate deviations from the standard naming conventions of the company. These accounts should be investigated for inappropriate access and potentially changed to meet company policy naming conventions. For example, if the standard naming convention is the first initial of the first name plus the last name (i.e., John Smith is jsmith), specific attention should be paid to naming conventions outside this policy. Thus, if instead of seeing “jsmith” one noted “john.smith,” this should raise an alarm and be investigated for inappropriate access. The risk is that this user may have multiple accounts that, when used in combination, constitute inappropriate access per the defined SoD business definition.
- ▶ **Terminated employees** – Though expired and terminated user accounts fall within the realm of logical access, examining the current user population for terminated employees from the human resources (HR) list is vital. This step not only reduces the number of users to be analyzed, but establishes the population on which to base the SoD testing and may even help reduce licensing costs.
- ▶ **System access** – Users with direct access to the lowest level of security (i.e., menus, screens, transaction codes) should be carefully analyzed. This represents a potential security loophole since individual users may be able to gain access rights without following the standard user administration process. The problem often occurs when consultants, contractors or specialists require access to specific system functionality and bypass roles in favor of assignment to individual menu items or screens outside the normal provisioning process.
- ▶ **System accounts** – Generic, shared and powerful system accounts (that users can log into) present a challenge as it is impossible to tell with certainty who has used that specific account. Since the SoD analysis is concerned with individual users who have the ability to execute sensitive transactions, generic or shared accounts (especially shared super user accounts) negate the aim of the analysis. Powerful system accounts only present a problem when these accounts are not locked-down and can be logged into by users of the system. These unsecure accounts limit the ability to monitor who is executing which sensitive transaction. All that is known is the responsible account, not the actual user. To prevent unauthorized activity, the company should ensure that it is not possible for a user to log into the system or process accounts.



Conclusion

SoD remains an integral part of a company's internal controls. While the appropriate level of effort and emphasis needs to be placed on SoD compliance, companies must also continue to strive for simplicity and precision in the execution of their controls. SoD presents a unique challenge to control compliance as it requires close alignment of business and IT stakeholders to assess, mitigate, reduce and monitor the risk of fraud or material misstatement.

Spending money on applications and tools alone will not fix deficient processes. Similarly, expecting improvement over time without a continued focus on the risks they are addressing or value that is being protected is not a sustainable compliance or IT strategy. Management must take a step back and ask what is the enterprise trying to accomplish through SoD. A well-designed, risk-based SoD initiative can enable compliance, and also demonstrate real business value by enhancing controls while improving, streamlining and efficiently redesigning key business and IT processes.

About Ernst & Young

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that every need and issue is unique to that business.

IT is one of the key enablers for modern organizations to compete. It gives the opportunity to get closer, more focused and faster in responding to customers, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective IT risk management helps you to improve the competitive advantage of your information technology operations, to make these operations more cost efficient and to manage down the risks related to running your systems. Our 6,000 IT Risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice – wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need a tailored service as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject- matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or any of the people listed in the table below.

Contacts

Global		
Norman Lonergan (Advisory Services Leader, London)	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Advisory Services		
Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	aembury@uk.ey.com
Nigel Knight (Far East Leader, Shanghai)	+86 21 2228 8888	nigel.knight@cn.ey.com
Isao Onda (Japan Leader, Chiba-shi)	+81 4 3238 7011	onda-s@shinnihon.or.jp
Doug Simpson (Oceania Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
IT Risk and Assurance Services		
Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Paul van Kessel (Europe, Middle East, India and Africa Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Troy Kelly (Far East Leader, Hong Kong)	+81 2 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Chiyoda-ku)	+81 3 3503 1100	stagno-gvnn@shinnihon.or.jp
Iain Burnet (Oceania Leader, Perth)	+61 8 9429 2486	iain.burnet@au.ey.com

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 144,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services

The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization, you require services that respond to your specific issues, so we bring our broad sector experience and deep subject-matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

© 2010 EYGM Limited.
All Rights Reserved.

EYG no. AU0529

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

www.ey.com