Separation of Duties: Basics and Applications
Table of Contents

What Is Separation of Duties? 4
SoD Rulesets and Controls 5
The Importance of Separation of Duties 5
Separation of Duties and SOX Compliance 6
Examples of Separation of Duties 9
Implementing Separation of Duties 10
Roles and Role Creation 11
Finding where the SoD conflicts are 11
Creating and assigning roles 12
Access Reviews and Certifications 13
Cross-Application SoD Conflicts 14
How Fastpath Can Help 16
About Fastpath 17
As companies seek greater effectiveness in their operations, they add best-of-breed solutions, such as ERP, CRM, HCM, warehouse management, and supply chain management applications, to their environment. While these interconnected business applications increase productivity and reduce errors, they require more and more stakeholders, including employees, contractors, clients, suppliers, and partners, to access the data in these applications.

Many of these organizations struggle with tracking who has access to these applications, what their access allows them to do, and what they are doing with that access. Too often, companies rely on low-productivity manual processes to manage their application risks; multiple spreadsheets, email requests, and sticky notes are part of the error-prone and labor-intensive activities at many organizations. Not only do these legacy processes increase costs, but they are hard to audit, leading to questions about data reliability and control effectiveness.

The inability to track user access across a company’s business systems, coupled with granting users more access to your systems than they need, can result in regulatory compliance violations, fines, loss of data, fraud, and loss of funds. As a result, Access Risk Management, which identifies and addresses the risks related to user access provisioning, has become top of mind for today’s information security and audit professionals. Separation of Duties is an essential element of application user lifecycle management in a company’s overall risk management plan, which is fundamental to a company’s overall Governance, Risk, and Compliance (GRC) initiatives. This eBook takes a deep dive into the subject of Separation of Duties.
What Is Separation of Duties?

Separation of Duties (also known as Separation of Duties or SoD) is a policy that aims to distribute the critical functions of a process to more than one person in the organization. By identifying and separating conflicting duties, an organization can ensure that a single person can’t complete a process without oversight. Giving a single entity control over all aspects of a business process can expose the company to risk because that individual or entity can commit errors, omissions, or fraud and then hide the activity from others. A typical SoD conflict example is a user who can create and pay a vendor. The risk here is that the user can create a fraudulent vendor account that deposits into their personal bank account and then pay that fraudulent vendor via standard accounts payable functionality in the system, all without oversight or detection. By separating the ability to create a vendor from the ability to pay a vendor, the organization ensures that more than one person would have to be involved in completing the process.

Separation of Duties also extends beyond financial roles to IT and Development roles within an organization. For instance, software developers should not be able to develop and test their solutions and then move the solution directly into production without oversight. Instead, different individuals or departments should handle each of these tasks. Otherwise, there is the potential risk that a developer might provide a “backdoor access” to the code or data in production systems, even if that risk was introduced unintentionally. For example, suppose a programmer has introduced debug functions into their code to monitor and change system variables during the code and unit test phase of development. As an innocent (even if careless) oversight, suppose those debug functions are never removed, and the developer moves the code into the production environment. Without even knowing it, the developer can now manipulate the code or data on the running production system.
SoD Rulesets and Controls

A Separation of Duties ruleset is a collection of SoD conflicts identified by the organization as presenting enough risk to require enforcement. This SoD ruleset considers the business environment, the control environment, and the systems environment. In an ideal world, businesses would define and enforce SoD across all their in-scope applications (ERP, HCM, CRM, etc.). In reality, this is too expensive and too complex to achieve. In many small organizations, where resources must take on multiple roles, it is not even possible to separate duties (for example, if there is only one person in the accounting position). Within a risk-based audit and compliance approach, SOD rules should still be defined across all in-scope applications. Enforcement should consider both remediation (removal of conflicting access) as well as mitigation. Mitigation of conflicting access risk can use either manual controls or automated controls:

- **Manual Control:** For example, a manual review of all new vendors created each month to validate the existence of a valid tax ID number and relevant use case and approval.
- **Automated Control:** For example, implementation of an automated workflow in the business application to require all new vendors to be approved, or all new vendor payments are validated and approved, or both.

The Importance of Separation of Duties

Effective separation of duties helps prevent individuals or groups from committing and then concealing errors and fraud. Adding mitigating controls helps minimize errors or fraud if they occur by exposing them early.
The analyst group, Gartner, has said, “Effective separation 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” (Market Guide for SoD Controls Monitoring Tools, Gartner, 2017). The Association of Certified Fraud Examiners also notes that the failure to maintain separation of duties is a leading cause of fraud in many organizations. The more prolonged fraud goes undetected, the more significant the loss to the company (ACFE Report to Nations). The report predicts that the average company will lose $1.5M each year to fraud.

Financial errors and fraud could lead to erroneous financial statements. As a result, companies can easily under or overestimate their profit or balance sheet and based on those figures, make unsound financial investments that jeopardize the company's solvency.

**Separation of Duties and SOX Compliance**

The Sarbanes-Oxley Act of 2002 (SOX) is primarily aimed at public companies and was passed following a series of corporate scandals involving falsified financial statements, including Enron, Tyco, and Worldcom. The legislation is intended to help restore investor confidence and protect shareholders, employees, and the public from future fraudulent financial practices in publicly traded companies.

Two sections of the Sarbanes-Oxley Act are of particular interest here.

- **Section 302, Corporate Responsibility for Financial Reports** – This section requires the CEO and CFO of companies affected
by the legislation to be held personally accountable to provide accurate financial reports. The legislation allows for severe criminal and financial penalties to these individuals for non-compliance. Auditors and regulators are looking closely at how companies of all sizes address internal security and access risk management. Fastpath enables organizations to streamline and automate key processes by delivering a variety of preventative, detective, and reactive control capabilities.

- **Section 404, Management Assessment of Internal Controls** – Section 404 requires that affected organizations establish oversight in defining roles, responsibilities, policies, and procedures and have internal controls in place to detect and prevent fraudulent activity. Section 404a outlines management’s responsibility to assert they have these controls in place in compliance with SOX. Section 404b outlines the requirement that an external auditor must attest that the company’s controls are in compliance.

While SOX does not offer a list of specific controls, it does expect organizations to show proof of security controls for areas such as change management, backup systems, and access to the company premises and business systems.

The SEC guidance on SOX compliance approaches it this way (*Sarbanes-Oxley Section 404: A Guide for Small Business*):

Think about “what could go wrong” by considering:
- Risk factors inherent in your business, both internal and external
- Risks in the way you authorize, process, and record transactions that are reflected in the financial statements
- Your company’s vulnerability to fraud

Effective management of separation of duties conflicts and user access to business-critical applications can significantly improve a company’s ability to meet SOX audit requirements.
Among other stipulations, SOX requires that publicly traded companies certify that they have instituted controls over their financial reporting. SOX compliance programs include Separation of Duties controls in critical areas of financial responsibility.

SOX provides some latitude for small companies and companies that have recently gone public by offering them an exemption period before requiring their full compliance with Section 404b of SOX. In addition, the Jumpstart Our Business Startups Act (JOBS Act) further extended the Section 404b exemption period to up to five years for certain companies covered by the act.

Regardless of the length of the exemption, all public companies must eventually demonstrate full SOX compliance. It is in their best interest to put the necessary controls in place sooner than later. Automated SoD tools like Fastpath can help these companies develop rulesets and controls for the Separation of Duties and create streamlined workflows for access reviews.

Some questions that an auditor might ask include:
- How do you know that your financial data is correct?
- Can you produce management sign-off on each employee’s request for access into each of your financial systems?
- Do you have proof of regular reviews of users in your financial system?
- Can you pass an audit of your financial systems today? How long would it take you to put all the documentation together? How confident are you in that documentation?

Sarbanes-Oxley is only one of many federal, state, and local laws, regulations, and ordinances that pertain to data security, user access risk management, and Separation of Duties. Others include the Gramm-Leach-Bliley Act, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), and Food and Drug Administration (FDA) regulations, to name a few.
Auditors and regulators are looking closely at how companies of all sizes address internal security and access risk management. Management, internal auditors, IT, and business process owners must work together to develop a robust security architecture for their critical business applications and ensure they have complete visibility of the user access and Separation of Duties risks in these applications.

The traditional role of IT has been to administer the company's network and software, and that has included setting up application security and provisioning users. However, when it comes to managing user access to business applications like ERP and CRM systems, it is the managers and business process owners in finance, accounting, sales, and human resources that are most capable of determining who in the organization should be granted access into the system—as well as the amount of access they should be authorized to have. Even if IT personnel are the ones who ultimately provision users, the responsibility of identifying who gets access and developing SOD rulesets is the responsibility of business management, not IT.

**Examples of Separation of Duties**

Some common examples where Separation of Duties conflicts arise include the following combination of job functions:

- Create a purchase order and approve that order
- Enter a journal entry and approve the entry
- Deposit cash and perform reconciliation of bank statements
- Create a new vendor and make vendor payments
- Maintain credit limits and release credit holds
- Ordering products and accounting for inventory
Implementing Separation of Duties

Implementing the Separation of Duties for various transactions follows the same general outline:

- Identify transactions that have the potential for financial impact on the organization if performed incorrectly or fraudulently.
- Rank the transactions according to highest to lowest risk.
- List the critical steps required to complete the task.
- Next, identify the responsibilities of each step. Pay particular attention to the steps where a person can authorize the actions from a previous step, as this is where fraud is most likely to occur. These will usually fall under one of the following areas of responsibility:
  - Custody of assets
  - Authorizations of transactions affecting those assets
  - Reporting the transactions
  - Reconciling the transactions
- Evaluate the process and design controls that will ensure separation of duties and operating effectiveness.
  - Ensure that each step in the process is assigned to different individuals or departments.
  - Consider employing mitigating or compensating controls as necessary to prevent potential abuse of the process.

SOD can be applied to individuals, groups, or entire companies.

- **Individual** – The most common form of SOD ensures that key duties are separated among individuals within the organization; for example, an accounting clerk issues a payment that then must be approved by a supervisor.
- **Group** – Here, duties are separated by different groups or departments within an organization. One department manages vendor information while another department issues payments to vendors.
- **Company** – Different legal entities are assigned the responsibility to perform various duties in the process. For example, a subsidiary can only make capital investments upon approval by the parent company.
Roles and Role Creation

For most organizations, SoD involves granting or denying users access to key functions within their business applications by assigning roles.

Most SoD risk comes from the company’s financial application, which, for most businesses, is an Enterprise Resource Planning (ERP) software application. While the term “role” may differ depending on the specific ERP being considered (for example, both SAP and Microsoft Dynamics 365 Finance and Operations will refer to a user’s “role”, while Oracle EBS uses the term “Responsibility”, Workday uses the term “Security Group”, and Oracle Cloud uses “Job Role”), they all refer to essentially the same concept: what tasks can this person do with his or her assigned permissions in the system?

Finding where the SOD conflicts are

The work environment is fluid: job requirements change, employees take on new responsibilities, new roles are defined, and new permissions are added to existing job roles. Sometimes, these responsibilities overlap, creating SoD conflicts for role definitions that did not exist before. In these situations, automated SoD tools can assist in finding the conflicts and suggesting mitigations that will resolve the SoD violations.

Rather than focusing on the names assigned to the various roles in these business applications, the actual SoD conflicts will only be found by analyzing permissions that are granted to the roles and the underlying security objects they can access. Here, the term “security objects”, like roles, will vary from ERP to ERP: “menu item displays or actions” in Dynamics 365, “functions” in Oracle EBS, “privileges” in Oracle Cloud, “T-codes” in SAP, etc. The bottom line is that it is not simply the role title, it is the user’s access to the underlying security objects that will drive the SoD conflicts in each ERP application.

To truly manage SoD risk, the organization must be able to identify the permissions of each user at the most granular securable object level.
Creating and assigning roles

To illustrate the challenge of object-level analysis, consider the issues raised by using pre-configured roles.

Most ERP applications come with common job assignments pre-configured ("out-of-the-box"), including titles like "Purchasing Department Manager" or "Receivables Inquiry," and it can be tempting for system administrators to save time by simply applying these roles to the appropriate individuals as needed.

Unfortunately, many of these pre-configured role definitions include access permissions to underlying security objects that aren’t obvious by simply looking at the role name. Using these out-of-the-box role definitions without first looking at the access privileges they provide often leads to many SoD conflicts. Administrators and business process owners must look at the specific access permissions granted by these role definitions to understand what this role assignment can do.

For example, role definitions with "Inquiry" in the name (such as "Receivables Inquiry" or "Payables Inquiry") seem harmless enough – they should simply permit the user to view, but not edit, add, or delete, the company’s receivables or payables. However, in some ERP systems, such out-of-the-box roles will also allow the user to create a manual journal entry or modify vendor information, potentially circumventing any internal controls you have in place to catch this type of activity.

As another example, the role of "Bookkeeper" sounds innocuous enough. However, in some ERPs, this out-of-the-box role can enter an invoice, generate a payment for that invoice, and process the bank reconciliation for that payment.
A guiding rule in designing user roles is the Principle of Least Privilege, which states that a user should only be granted the minimum permission to access a system or operation to complete their job functions or tasks. In addition, access should only be granted for the minimum length of time necessary for a person to complete their task. Granting a person more access than necessary could result in user access risk or an SoD violation, exposing the business to the possibility of having critical data accidentally or maliciously altered or deleted, intellectual property stolen, or finances fraudulently taken. Regardless of the ERP system your company uses, it is best to avoid pre-configured role assignments because they might provide the user with access to change transactional or master data within the application. And simply editing the pre-configured roles might not be enough because software updates often add new responsibilities to these out-of-the-box role definitions, replacing your edits with a new version containing the original conflicts or adding new ones.

The better option is to use the pre-configured role definitions as a starting point, or template, for designing and building your own customized roles.

Out-of-the-box role definitions should only be used in special situations, such as granting a person temporary elevated account access to cover for a person who is out sick or on vacation. Even then, all such temporary assignments should be given an end date when the elevated access will be terminated.

**Access Reviews and Certifications**

Job roles change as a normal course of business: people are promoted or leave the company and business processes are updated. All too often, the access privileges of these users are not updated, which can lead to increased security risks.
Businesses should hold regular access reviews to ensure users have the appropriate access for their job responsibilities to avoid potential SoD conflicts and regulatory compliance issues.

Access reviews ensure that managers and business process owners review the access of the individuals in their department to the business applications used by the company. Access reviews reveal who has appropriate and inappropriate access and provides a means for organizations to correct any potential security issues early, helping the company avoid incidents of fraud, errors, and misstatements in the future.

Once the user access reviews are completed, the managers and business process owners should certify the access showing that the users are indeed authorized to have the access they have been granted. Automated risk management systems will include tools for conducting regular access reviews and certifications, routing the reviews to the appropriate business process owner, identifying the individuals who require sign-off, and tracking the responses in an auditable report.

Access reviews and certifications, showing the roles that are authorized access to critical areas of the company's applications, the individuals to whom those roles are assigned, and the person who authorized that access, are important for Access Risk Management audits.

**Cross-Application SoD Conflicts**

Many companies manage their finances and business operations using an ERP application like Microsoft Dynamics 365, Oracle, SAP, or NetSuite, to name just a few. Today, companies are looking at best-of-breed solutions for all aspects of their business. In addition to an ERP, these companies might also use a Customer Relationship Management (CRM) application like Salesforce and a Human Capital Management (HCM) application like Workday. There are also instances where a parent company might run Oracle or SAP while a subsidiary or a new acquisition is running NetSuite or Dynamics GP.
The result is that, for many of these businesses, financial transactions are no longer limited to a single ERP software application. Instead, transactions are taking place in multiple business applications. For example, a company might maintain their supplier or vendor master data in their ERP and send payments to those suppliers in another application, such as Coupa.

Here are just a few of the potential cross-application SOD conflicts that are possible when companies have business processes interact with different business-critical applications:

• Hire-to-Retire: A company uses Oracle as their ERP for payroll processing but manages employee data in Workday.
• Order-to-Cash: A company uses Salesforce as their CRM to maintain customer master data and book sales orders but issues the AR invoice for each sales order through their Microsoft Dynamics 365 ERP.
• Procure-to-Pay: A company uses Coupa to issue their purchase orders, but they process their payments using NetSuite.

In each of these examples, a user with permissions to perform each task in both systems creates a potential Separation of Duties risk for the company, even though their permissions in each application, when viewed in isolation, will not indicate an SoD conflict.

Most automated Identity Management and Access Control tools are designed to only check for SoD violations within a particular business application. They will not find SoD conflicts that might exist across interconnected business systems. So, while administrators are able to design user roles and privileges in these business applications individually, there is now a need to look at how these roles interact between the business applications themselves and identify potential SoD conflicts across business applications.
How Fastpath Can Help

Fastpath is a cloud-based access orchestration platform that helps organizations of all sizes to manage and automate the processes around access governance and security, quickly and efficiently. Fastpath can analyze user access to critical data at a granular level across multiple business applications to help companies identify and mitigate their cross-platform SoD risks. Fastpath Access Control comes with predefined and easily modified rulesets built by Fastpath’s team of certified internal auditors. Fastpath automates User Access Reviews notifying the necessary parties of the tasks requiring sign-off, following up on incomplete assignments, and generating reports for audit compliance. Other security tools available from Fastpath include:

- **Change Tracking**
  - Whether you leverage out-of-the-box templates or define the scope of the change tracking yourself, Fastpath’s change tracking will identify who made the change and provide before & after values and other metadata to determine appropriateness. Integrations into common ITSM platforms allows you to close the loop by validating tickets and approvals where required.

- **Certifications**
  - No matter how effective preventative control of user access is, inappropriate access in key applications will happen. Fastpath helps you build a robust continuous monitoring program that detects issues quickly, reducing exposure time and eliminating issues. Certification campaigns can be set up with different targets and schedules to give you the most coverage possible.
• **Identity**
  - Access security and risk management starts and ends with the end user. Each user’s role defines their digital identity, which requires an access level relative to the needs of the job function. Since most data needed to define the identity resides in your HR system, we start there. Using deep integration into your HR application, we automate access management for each event in the user’s lifecycle. With birthright access, streamlined access, request & approval for non-standard user needs, and automatic deprovisioning, Fastpath drives compliant user management simply and efficiently, so you don’t have to.

Since 2004, Fastpath has produced software to address user access and security for organizations of all sizes. Fastpath provides the following benefits:

- **Unrivalled Integrations**- Fastpath integrates out-of-the-box, working across multi-application environments and custom-made software to deliver insight into your security risks
- **Rapid Time to Value**- We’re easy to implement and quick to deploy, and with no expensive customization required, you can immediately reap ROI.
- **Frictionless Automation**- Effortlessly automate processes like onboarding, testing and proving controls to continuously identify, quantify, and eliminate risk.
- **Improved Efficiency**- Ease of use and out-of-the-box content allow security teams to get up to speed fast, focus on what matters, and save valuable time.

**About Fastpath**
Since 2004, Fastpath has been a global leader in application governance, risk and compliance, enabling organizations to manage and automate the processes around access control and data access risk quickly and efficiently. In a world full of complexity, Fastpath simplifies audit and compliance activities by helping to quickly identify, quantify and manage key risks within all major ERP, CRM and HRM systems. We enable businesses to seamlessly orchestrate their security, compliance and risk management across multisite, multi-application environments. We help clients all over the world make strategic business decisions confidently, knowing their organization is secure and compliant.