



# Segregation of Duties Solutions

*Point of View*

January 10, 2007

Audit • Tax • Consulting • Financial Advisory •

# Contents

---

---

Business Considerations

---

Example Approach to an SOD Program

---

Example SOD Tool Process and Sample Documents

---

---

# Business Considerations

# Segregation of Duties

---

***Segregation of Duties** is the separation of incompatible duties that could allow one person to commit and conceal fraud that may result in financial loss or misstatement to the company. Segregation of duties may be within an application or within the infrastructure.*

- **Represents a key internal control that ensures no single person has too much influence over any business transaction or operation**
- **Serves to prevent unintentional errors or fraud and ensure timely detection of errors that may occur**
- **Provides a method of improving organizational, business process and IT control alignment**

***Segregation of duties has always been an important component of a properly functioning internal control environment***

# Common Challenges and Pitfalls of IT Controls

---

## **Control deficiencies, typically, stemmed from changes or actions taken outside of the formal process**

- Limited mechanisms to consistently enforce policies at an enterprise level
- Lack of strong executive-level support and insufficient alignment between IT and the business
- Lack of user education & awareness regarding SOD
- Management's preference to rely on mitigating controls in place of implementing proper SOD
- Inadequate policies and procedures for effectively changing or removing access when users change jobs or leave the company
- Limited automated reporting capabilities for IT controls
- No monitoring tools/capability to periodically review "access rights"

***Typically, leads to access creep, fraud risk, and failed user management processes***

# Why the Increased Interest

---

Drivers causing companies to consider use of Segregation of Duties (SOD) in the management of their business

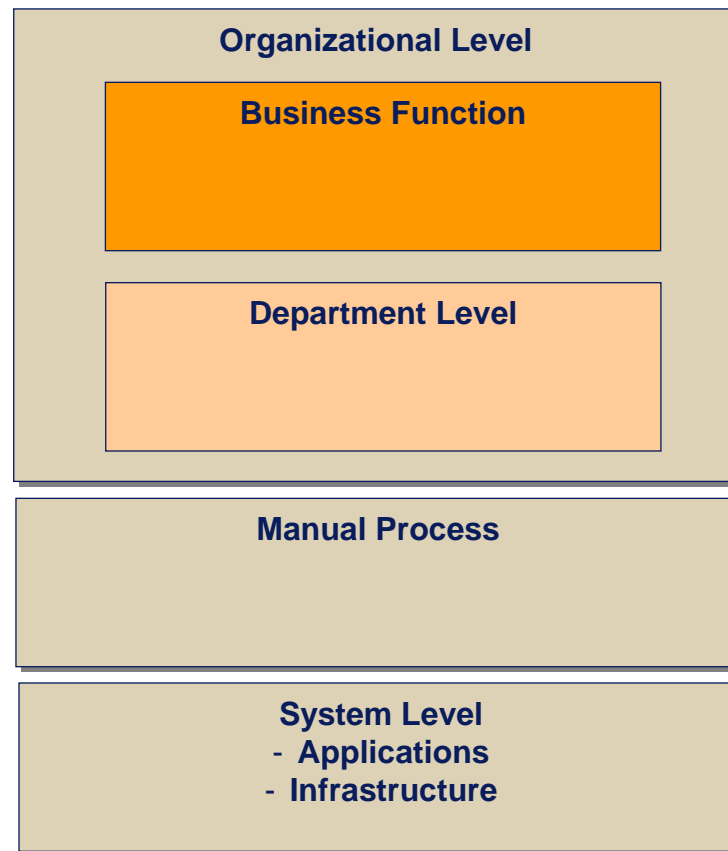
- **Regulatory Compliance** - Sarbanes-Oxley and other regulatory issues are forcing companies to increase their awareness and accountability of their employees actions within the company
- **Security and Data Management** – Recent privacy laws and prosecution of security violations is bringing a new awareness to monitoring and controlling security and access to data within the organization
- **Access Management** – Provisioning and management of users access to applications have not been enforced, resulting in access creep
- **Rapid Implementation of ERPs** – Application Security was often overlooked or implemented incompletely (Segregation of Duties was not addressed)

# Regulatory Compliance

---

**Sarbanes-Oxley is now providing a compelling case for the implementation and maintenance of appropriate segregation of duties at the organizational, manual process and system level.**

- Not only should business functions be separated departmentally, and at an even more granular level within departments, companies now finding that they need to provide system enforcement of traditional segregation of duties models
- External auditors are insisting on evidence that proper segregation of duties exists



# Security and Data Management

---

**Recent privacy laws and prosecution of security violations is bringing a new awareness to monitoring and controlling security and access to data within the organization**

- Lack of application specific Segregation of Duties are resulting in Access Creep, Fraud Risk, Failed User Management Processes
- Disclosure of sensitive information can have a negative impact on shareholder value
- Increased use of web services (online auctions and banking) has brought increased risk of identity theft and fraud
- Privacy laws and disclosure of violations is increasing the need for proactive segregation and control over access to data

# Access Management

---

**Implementation of identity management and ERP tools provides an avenue to leverage technologies to enforce and regulate enterprise level segregation of duties**

- Established authoritative sources of information through ERP systems (HRMS)
- Leverage user lifecycle through role based access control and system integration
- Automated provisioning to lower operational costs
- Greater visibility by management to monitor user activity
- Centralization of user ID management for multiple applications through the single sign-on concept

---

# Example Approach to an SOD Program

# Companies Need a Process for Establishing and Managing Segregation of Duties

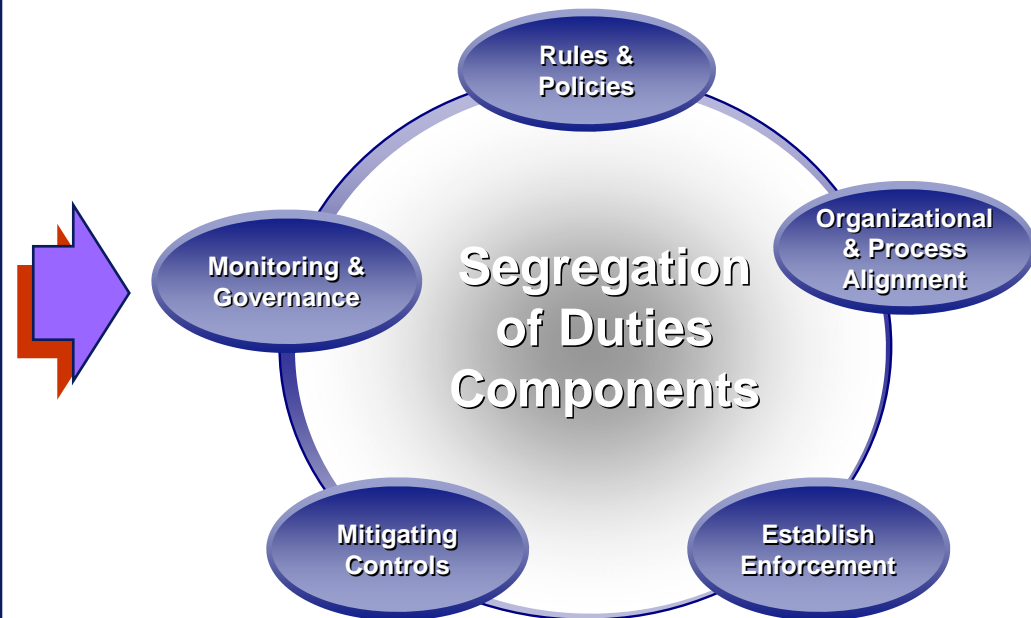
---

**Establishing a process for defining SOD rules and policies, aligning organization and process, establishing enforcement, mitigating controls and monitoring are essential components of an SOD solution that helps meet business objectives**

## Business Objectives

- Comply with the regulatory requirements, example Sarbanes-Oxley legislation
- Improve company-wide internal control structure
- Mitigate the risk of intentional fraud or unintentional error to the organization
- Align functions organizationally with common best practices
- Gain a level of comfort that the financial statements are free from misstatement
- Improve financial data, thereby improving management reporting
- Satisfy increasing customer and investor demands for sound internal controls

## SOD Solution



# Program To Establish and Manage SOD

## Rules & Policies

- Confirm SOD requirements (including regulatory compliance requirements)
- Develop segregation of duties rules
- Eliminate false positives from rule set
- Define manual segregation of duties components

## Organizational & Process Alignment

- Perform risk assessments to identify requirements and strategies
- Identify key stakeholders and establish a communication plan
- Understand and adapt standards (including policies and procedures)
- Build and maintain support within initiative and within organization
- Align processes to effect the proper balance between control value and operational efficiency (cost vs. benefit analysis)
- Identify appropriate segregation points within relevant processes
- Obtain buy-in to SOD solution from process owners

## Establish Enforcement

- Assist in selecting the appropriate technology solution
- Pilot the implementation to validate the solution
- Implement the solution; deliver in phases (highest value first)
- Test performance and functionality

## Mitigating Controls

- Develop controls to address functions which cannot be adequately segregated

## Monitoring & Governance

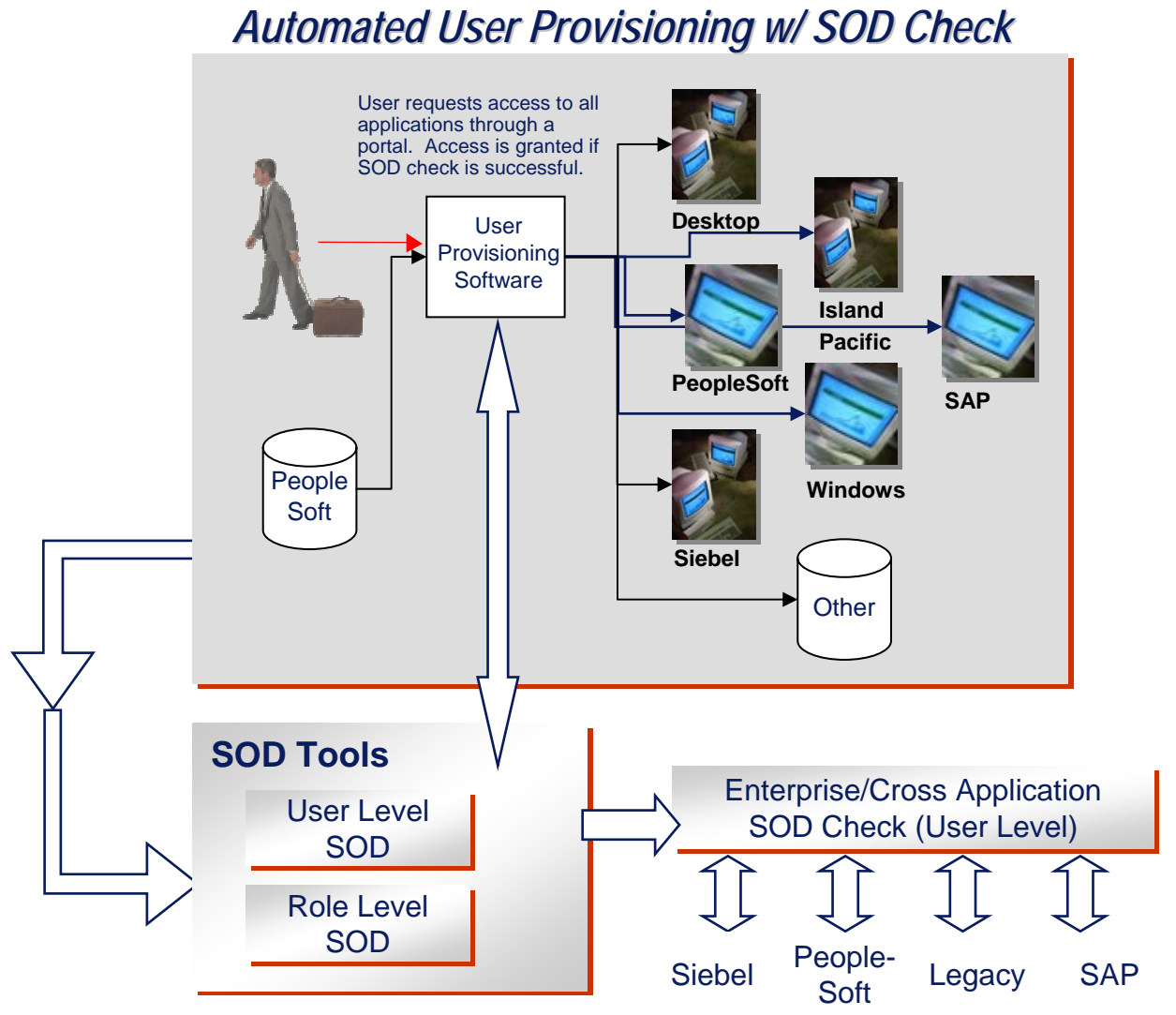
- Adhere to the business policies and procedures after initial deployment
- Perform periodic assessment to validate adherence to policies and rules
- Adapt solution as the business changes (e.g., M&A, reorganizations)

# Technology can help companies manage the enforcement and monitoring of segregation of duties rules and policies

---

- In response to the current regulatory environment, commercial software solutions are available to provide an automated platform to support SOX compliance by providing functionality such as defining and monitoring Segregation of Duties (SOD), monitoring critical transactions, fine tuning authorizations, and reporting
- Key features of Segregation of Duties products include:
  - Ability for SOD analysis as new accounts are added/updated
  - Support for both preventative and detective controls
  - Support for multi-application analysis
  - Links to security policies; drill down capabilities
  - Rule building and customization support
  - Ad-hoc reporting capabilities
  - Support for the capture of mitigating controls
  - Linkage to role access request process/ e-Provisioning
  - Support for broader controls monitoring programs

# Sample IdM Segregation of Duties Architecture



# SOD Assessment Process

---

## Step I

### Determine SOD Rules

- Identify Key Responsibilities within each Business Process Area
- Establish Segregation of Duties Rules for each Business Process
- Create SOD Conflict Matrix (Rules)

## Step II

### Gather Data, Execute SOD Tool, Analyze SOD Output

- Upload Segregation of Duties Rules to SOD Tool
- Extract data from Application for User and Roles (Functions or Objects)
- Execute SOD Tool
- Perform SOD Conflict Analysis

## Step III

### Remediate, Retest, Roll-Forward

- Remediation Plan
- Resolve SOD issues or Identify Compensating Controls
- Re-perform Application SOD testing

**Client****➤ Process Owners to indicate:**

- SOD rules that are currently enforced
- Conflicts that may be important but not currently enforced
- Conflicts that are not relevant
- Conflicts that are low risk based on company's Business Model
- Unique Application Customizations for which conflicts need to be identified
- Known conflicts that exist for business reason

**➤ Application Support Team to provide information:**

- Super User and System Administrator's Access in Applications
- Risk Mitigation methods (of Super User & System Administrator access) employed

Continued..

### Deloitte

- **Review SOD information gathered with BPOs:**
  - ❑ Edit SOD rules to reflect suggested additions and deletions
  - ❑ Confirm that rules include proper cross-business cycle rules
  - ❑ Finalize SOD rules with Business Process Owners (BPOs)
- **Obtain consensus and Sign-off on SOD design from BPOs**
- **Discuss SOD Rules with External Auditors**
- **Finalize SOD Design with BPOs**

Continued..

### Client

- Remediate current conflicts identified in Step I
- Identify compensating controls where appropriate

### Deloitte

- Upload Segregation of Duties Rules to SOD Tool
- Extract data from Application for Roles and Users
- Upload the extracted data into the SOD Tool
- Execute SOD Tool
- Validate data extracted from Applications

*Note: For a cross-application analysis, a user identity mapping exercise must also be conducted.*

### Deloitte

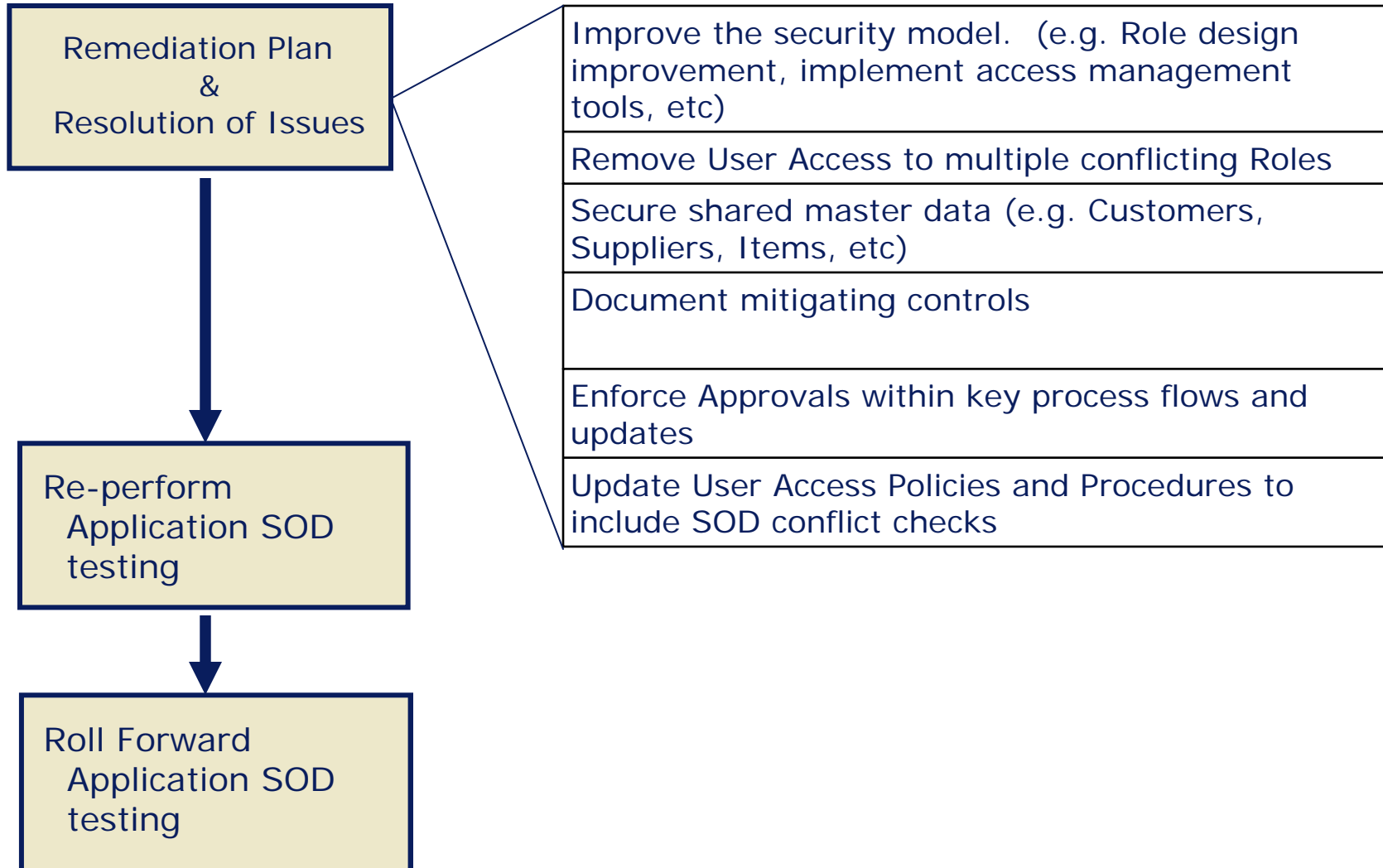
#### ➤ Document SOD Conflict Results

- ❑ Conflicts within Roles – Role Design
- ❑ Conflicts by Users - Users with access to Roles within an Application \*
- ❑ Cross Application Conflicts - Users with access to multiple Roles across Applications

*\* In some cases, users may have direct access to conflict (without going through a role).*

Step III

# Remediate, Retest, Roll Forward



---

# Example

# Conflict Rule Set

Conflict Matrix			Merchandise Purchase setup											
			Vendor setup					Item Setup			PO creation	PO Approval	Purchasing maintenance	
			Initiation - Signing of Vendor and item agreement	Vendor setup in iSeries	Review of Vendor agreement	Approve Vendor setup in iSeries	Verify that the vendor number and name are not duplicates	Initiation	Review of item agreement	Verification of Spoils and warranty and Hazmat information	Creation of PO in iSeries	Approval of PO in iSeries	Auto replenishment	Future cost and Future sell
			MNL1	VM	MNL2	VMM	VCREF	ITEM	MNL3	SWI	POE	POA	ARR	FC
Merchandise Purchase setup	Vendor setup	Initiation - Signing of Vendor and item agreement	MNL1											
		Vendor setup in iSeries	VM			4								
		Review of Vendor agreement	MNL2											
		Approve vendor setup in iSeries	VMM		3									
		Verify that the vendor number and name are not duplicates	VCREF											
	Item setup	Initiation	ITEM											
		Review of item agreement	MNL3											
		Verification of Spoils and warranty and Hazmat information	SWI											
	PO creation	Creation of PO in iSeries	POE									1		
	PO Approval	Approval of PO in iSeries	POA							4			2	
	Purchasing maintenance	Auto replenishment	ARR											
		Future cost and Future sell	FC											

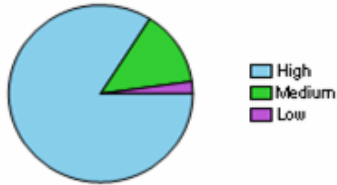
- **Conflict 1** - Create PO vs. Approve PO
- **Conflict 2** - Auto-replenishment vs. Approve PO
- **Conflict 3** - Setup Vendor vs. Approve Vendor
- **Conflict 4** - Conflict between Create PO, Approve PO, Create Vendor and Approve Vendor

# Conflict Report

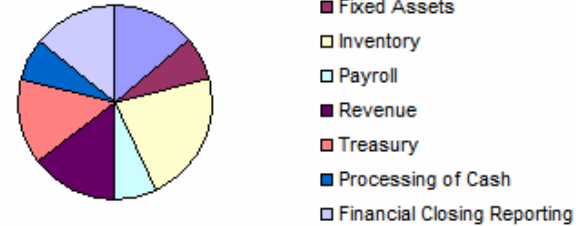
## SOD Conflict Violation Summary

1/30/2006

Risk Category

















BP Cycle Category



Risk	Business Process Cycle*								Conflict Rule Name	Conflict Rule Description	No. User	No. Role
	1	2	3	4	5	6	7	8				
High	x								Enter Sales Orders and Receipts	Enter Sales Orders and Receipts	67	15
High		x							Receiving Transactions and Setup Organization	Receiving Transactions and Setup Organization	66	18
High			x						Enter Purchase Orders and Returns	Enter Purchase Orders and Returns	60	22
High			x						Enter Purchase Orders and Corrections	Enter Purchase Orders and Corrections	58	18
High						x			Enter Sales Orders and Define Payment Terms	Enter Sales Orders and Define Payment Terms	48	7
High				x					Enter Payment and Setup Currency	Enter Payment and Setup Currency	47	27
High	x								Enter Payment and Setup Payment	Enter Payment and Setup Payment	41	26
High					x				Enter Journal and Eliminations	Enter Journal and Eliminations	33	25
High					x				Enter Journal and Consolidation Mapping	Enter Journal and Consolidation Mapping	33	25
High						x			Enter Purchase Orders and Enter Receipts	Enter Purchase Orders and Enter Receipts	60	22
Medium			x						Enter Payment and Receive	Enter Payment and Receive	18	12
Medium							x		Collections Customer Accounts and Collections	Collections Customer Accounts and Collections Setup	10	2
Medium								x	Create Buyers and Enter Receipts	Create Buyers and Enter Receipts	2	2
Low								x	AutoCreate Purchase Order and Enter Invoice	AutoCreate Purchase Order and Enter Invoice	24	12

\*BP Cycles: 1-Expenditure 2-Fixed Assets 3-Inventory 4-Payroll 5-Revenue 6-Treasury 7-Processing of Cash 8-Financial Closing Reporting

# Software Tool Comparison

Example Control Objectives (Summarized)	SOD Tools	User Provisioning	Single-Sign-On
<b>S-1:</b> Proper segregation of duties exists among the IT functions (e.g. application development and DBA).			
<b>S-2:</b> Formal policies govern user access administration, config and monitoring.			
<b>S-3, S-7, S-11, S-15:</b> Additions / modifications to security privileges are properly authorized.			
<b>S-4, S-8, S-12, S-16:</b> Access privileges are timely disabled or modified in response to terms and transfers.			
<b>S-5, S-9, S-13, S17:</b> Periodic review of user access privileges is performed.			
<b>S-6, S10, S14:</b> Review of unauthorized access attempts is performed.			



**IdM technique could be deployed to address some of the objective**



**IdM technique could be deployed to address most of the objective**

---

# Deloitte.

## **About Deloitte**

Deloitte, one of the nation's leading professional services firms, provides audit, tax, consulting, and financial advisory services through nearly 30,000 people in more than 80 U.S. cities. Known as an employer of choice for innovative human resources programs, the firm is dedicated to helping its clients and its people excel. "Deloitte" refers to the associated partnerships of Deloitte & Touche USA LLP (Deloitte & Touche LLP and Deloitte Consulting LLP) and subsidiaries. Deloitte is the U.S. member firm of Deloitte Touche Tohmatsu. For more information, please visit Deloitte's Web site at [www.deloitte.com/us](http://www.deloitte.com/us).

Deloitte Touche Tohmatsu is an organization of member firms devoted to excellence in providing professional services and advice. We are focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, our member firms, including their affiliates, deliver services in four professional areas: audit, tax, consulting, and financial advisory services. Our member firms serve more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies.

Deloitte Touche Tohmatsu is a Swiss Verein (association), and, as such, neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other, related names. The services described herein are provided by the member firms and not by the Deloitte Touche Tohmatsu Verein. For regulatory and other reasons, certain member firms do not provide services in all four professional areas listed above.

Member of  
**Deloitte Touche Tohmatsu**