Best Practices to resolve Segregation of Duties conflicts in any ERP environment

It is a well known fact that Segregation of Duties (SOD) is a top contributor for fraud activities and is a key part of achieving Sarbanes Oxley (SOX) Compliance. The challenge of achieving this is typically more acute in the small and medium sized companies due to the lack of advanced tools or the expertise to manage this risk effectively. Hence, in this article, I have compiled a list of activities, which when combined together pose a high risk to the business. Internal Audit would need to work collaboratively with the business and the IT teams to Segregate these duties wherever possible and assign an appropriate mitigation control in cases wherein it is not feasible to do so. In addition, these controls would need to be monitored on a quarterly basis and the results need to be reported to senior management.

SOD Assessment and Remediation Process

The initiative to determine, analyze and address SOD issues can be achieved by the following three steps:

Phase I: Gather a list of applicable SOD conflicts
Use the conflicts listed below as a guideline or a starting point, but do interlock with the business to create a subset of the conflicts that would be applicable in your company's environment. This can be achieved as follows:

- Identify key responsibilities for each business process area
- Define Segregation of Duties rules
- Create a SOD matrix from these rules

Phase II: Analyze SOD Output
This can be performed manually or with the help of a tool. In case of manual analysis, for each user, analyze if he/she has the access to perform any of the conflicting functions defined in Phase I. In case of using a tool, proceed as follows:

- Upload Segregation of duties to the SOD tool
- Execute the SOD tool
- Perform SOD Conflict Analysis

Phase III: Remediate and Remain Clean phase
In this phase, evaluate if the conflicting tasks can be performed by an alternate person. If so, work with the IT team to modify the access to enable this. However, if it would not be

possible to do so due to practical difficulties, consider formulating an appropriate control to mitigate the risk. This would typically entail working with the business to setup additional monitoring procedures. Follow this process to address all the high risk conflicts.

Finally, establish a new go-forward process wherein every access request is reviewed against the SOD matrix prior to provisioning on the system.

List of conflicting tasks that pose a high risk:

Task 1	Task 2	Description of Risk
Maintain Bank Master Data	AP Payments	Create a non bona-fide bank account and create a check from it.
Maintain Asset Document	Process Vendor Invoices	Pay an invoice and hide it in an asset that would be depreciated over time.
Maintain Asset Document	Goods Receipts to PO	Create an invoice through ERS goods receipt and hide it in an asset that would be depreciated over time.
Cash Application	Bank Reconciliation	Allows differences between cash deposited and cash collections posted to be covered up
Maintain Asset Master	Goods Receipts to PO	Create the asset and manipulate the receipt of the associated asset.
Process Overhead Postings	Settle Projects	Post overhead expenses to the project and settle the project without going through the settlement approval process.
Maintain Projects and WBS Elements	Settle Projects	Use a fictitious project to allocate overages of an actual project, and settle the project without going through the settlement approval process.
Maintain Projects and WBS Elements	Process Overhead Postings	Manipulate the work breakdown structure elements (profit centers, business areas, cost centers, plants) and post overhead expenses to the project
Maintain Bank Master Data	Cash Application	Maintain a non bona-fide bank account and divert incoming payments to it.
Maintain Bank Master Data	Manual Check Processing	Create a non bona-fide bank account and create manual checks from it
Create / Change Treasury Item	Confirm a Treasury Trade	Users can create a fictitious trade and fraudulently confirm or exercise the trade
Goods Movements	Enter Counts - WM	Accept goods via goods receipts and perform a WM physical inventory adjustment afterwards.

Goods Movements	Enter Counts - IM	Accept goods via goods receipts and perform an IM physical inventory adjustment afterwards.
Goods Movements	Enter Counts & Clear Diff - IM	Accept goods via goods receipts and perform an IM physical inventory adjustment afterwards.
Vendor Master Maintenance	Process Vendor Invoices	Maintain a fictitious vendor and enter a Vendor invoice for automatic payment
AP Payments	Vendor Master Maintenance	Maintain a fictitious vendor and create a payment to that vendor
Process Vendor Invoices	AP Payments	Enter fictitious vendor invoices and then render payment to the vendor
Maintain Purchase Order	Process Vendor Invoices	Purchase unauthorized items and initiate payment by invoicing
Maintain Purchase Order	Goods Receipts to PO	Enter fictitious purchase orders for personal use and accept the goods through goods receipt
Process Vendor Invoices	Goods Receipts to PO	Enter fictitious vendor invoices and accept the goods via goods receipt
Maintain Purchase Order	AP Payments	Enter a fictitious purchase order and enter the covering payment
Vendor Master Maintenance	Maintain Purchase Order	Create a fictitious vendor and initiate purchases to that vendor
Maintain Purchase Order	Enter Counts & Clear Diff - IM	Inappropriately procure an item and manipulating the IM physical inventory counts to hide.
Bank Reconciliation	Process Vendor Invoices	Can hide differences between bank payments & posted AP records
Service Acceptance	AP Payments	Receive or accept services and enter the covering payments
PO Approval	Goods Receipts to PO	Approve the purchase of unauthorized goods and hide the misuse of inventory by not fully receiving the order
PO Approval	AP Payments	Commit the company to fraudulent purchase contracts and initiate payment for unauthorized goods and services.
PO Approval	Process Vendor Invoices	Release a non bona-fide purchase order and initiate payment for the order by entering invoices

PO Approval	Enter Counts - IM	Release a non bona-fide purchase order and the action remain undetected by manipulating the IM physical inventory counts
PO Approval	Vendor Master Maintenance	Create a fictitious vendor or change existing vendor master data and approve purchases to this vendor
AP Payments	Purchasing Agreements	Enter fictitious purchasing agreements and then render payment
Vendor Master Maintenance	Purchasing Agreements	Risk of entry of fictitious Purchasing Agreements and the entry of fictitious Vendor or modification of existing Vendor especially account data.
Purchasing Agreements	Goods Receipts to PO	Modify purchasing agreements and then receive goods for fraudulent purposes.
Process Vendor Invoices	Purchasing Agreements	Enter unauthorized items to a purchasing agreement and create an invoice to obtain those items for personal use
AP Payments	Service Master Maintenance	Risk of modifying service master data (to add a service that is normally not ordered by the company) and the entry of covering payments
AP Payments	Bank Reconciliation	Risk of entering unauthorized payments and reconcile with the bank through the same person.
Maintain Purchase Order	Enter Counts - IM	Inappropriately procure an item and manipulating the IM physical inventory counts to hide.
Maintain Purchase Order	Enter Counts - WM	Inappropriately procure an item and manipulating the WM physical inventory counts to hide.
PO Approval	Enter Counts & Clear Diff - IM	Release a non bona-fide purchase order and the action remain undetected by manipulating the IM physical inventory counts
PO Approval	Enter Counts - WM	Release a non bona-fide purchase order and the action remain undetected by manipulating the WM physical inventory counts
Manual Check Processing	Vendor Master Maintenance	Maintain a fictitious vendor and create a payment to that vendor
Process Vendor Invoices	Manual Check Processing	Enter fictitious vendor invoices and then render payment to the vendor
Maintain Purchase Order	Manual Check Processing	Enter a fictitious purchase order and enter the covering payment
Service Acceptance	Manual Check Processing	Receive or accept services and manually enter the covering check payments

PO Approval	Manual Check Processing	Commit the company to fraudulent purchases and initiate manual check payments for unauthorized goods and services.
Manual Check Processing	Purchasing Agreements	Enter fictitious purchasing agreements and then render manual checks for payment
Manual Check Processing	Service Master Maintenance	Risk of modifying service master data (to add a service that is normally not ordered by the company) and the entry of covering payments
Manual Check Processing	Bank Reconciliation	Risk of entering unauthorized manual payments and reconcile with the bank through the same person.
Maintain Purchase Order	PO Approval	Where release strategies are utilized, the same user should not maintain the purchase order and release or approve it.
Credit Management	Sales Order Processing	Enter or modify sales documents and approve customer credit limits
Sales Order Processing	Clear Customer Balance	Create sales documents and immediately clear customer's obligation
Sales Order Processing	Maintain Customer Master Data	Create a fictitious customer and initiate fraudulent sales document
Maintain Customer Master Data	Process Customer Invoices	Make an unauthorized change to the master record (payment terms, tolerance level) in favor of the customer and enter an inappropriate invoice.
Maintain Customer Master Data	Sales Rebates	Inappropriately create or change rebate agreements and manage a customer's master record in the favor of the customer. Could also change a customer's master record to direct payment to an inappropriate location.
Clear Customer Balance	Maintain Billing Documents	Potentially clear a customer's balance before and create or make the same change to the billing document for the same customer, clearing them of their obligation.
Sales Order Processing	Maintain Billing Documents	Inappropriately create or change a sales documents and generate a corresponding billing document for it.
Credit Management	Sales Rebates	Manipulate the user's credit limit and assign generous rebates to execute a marginal customer's order.
Cash Application	Maintain Billing Documents	Create a billing document for a customer and inappropriately post a payment from the same customer to conceal non-payment.
Maintain Customer Master Data	AR Payments	Create a fictitious customer and initiate payment to the unauthorized customer.

Process Customer Credit Memos	AR Payments	Initiate an unauthorized payment to the customer by entering fictitious credit memos.
Cash Application	Sales Document Release	Change the accounts receivable records to cover differences with customer statements.
Sales Order Processing	Delivery Processing	Cover up unauthorized shipment by creating a fictitious sales documents
Process Customer Invoices	Sales Pricing Condition	Sales price modifications for sales invoicing.
Sales Order Processing	Sales Pricing Condition	Enter sales documents and lower prices for fraudulent gain
Credit Management	Cash Application	Perform credit approval function and modify cash received for fraudulent purposes.
Cash Application	Sales Rebates	Enter a fictitious sales rebates and then render fictitious payments.
Cash Application	Maintain Customer Master Data	Risk of the same person entering changes to the Customer Master file and modifying the Cash Received for the customer.
Process Customer Invoices	Credit Management	Risk of modifying and entering Sales Invoices and approving Credit Limits by the same person.
Maintain Billing Documents	Sales Pricing Condition	Risk of Sales Price modifications for Sales invoicing.
Maintain Customer Master Data	Clear Customer Balance	Maintain a customer master record and post a fraudulent payment against it
Maintain Customer Master Data	Maintain Billing Documents	User can create a fictitious customer and then issue invoices to the customer.
Cash Application	Process Customer Invoices	User can create/change an invoice and enter/change payments against the invoice.
Delivery Processing	Cash Application	User can create fictitious/incorrect delivery and enter payments against these, potentially misappropriating goods.
Sales Order Processing	Process Customer Invoices	User able to create a fraudulent sales contract to include additional goods and enter an incorrect customer invoice to hide the deception.
Clear Customer Balance	Process Customer Credit Memos	Create a credit memo then clear the customer to prompt a payment.

Maintain Employee (PA) Master Data - 0008 - 0009 (	Process Payroll	Modify payroll master data and then process payroll. Potential for fraudulent activity.
HR Benefits	Process Payroll	Change employee HR Benefits then process payroll without authorization. Potential for fraudulent activity.
3rd Party Remittance	HR Vendor Data	Change to master data and creating the remittance could result in fraudulent payments.
Maintain Time Data	Approve Time	Change payroll master data and enter time data applied to incorrect settings.
Maintain Time Data	Process Payroll	Modify time data and process payroll resulting in fraudulent payments
Maintain Payroll Configuration	Process Payroll	Change configuration of payroll then process payroll resulting in fraudulent payments
Maintain Employee (PA) Master Data - 0008 - 0009 (	Maintain Payroll Configuration	Change configuration of payroll then modify payroll master data resulting in fraudulent payments
Modify PD Structure	Maintain Employee (PA) Master Data - 0008 - 0009 (	Change payroll master data and modify PD Structure
Maintain Time Data	Payroll Maintenance	Enter false time data and perform payroll maintenance.
Payroll Maintenance	Process Payroll	Change payroll and process payroll without proper authorization.
Maintain Payroll Configuration	Payroll Maintenance	Change payroll configuration and perform maintenance on payroll settings.
Maintain Time Data	Maintain Payroll Configuration	Modify payroll configuration and enter false time data.
Maintain Time Data	Modify PD Structure	Enter false time data and maintain PD structure
Maintain Employee (PA) Master Data - 0008 - 0009 (	Maintain Time Data	Users may enter false time data and process payroll resulting in fraudulent payments.
Maintain Employee (PA) Master Data - 0008 - 0009 (	Payroll Maintenance	Users may maintain employee master data including pay rates and delete the payroll result
Payroll Schemas	Maintain Time Data	Users may enter false time data and perform work schedule evaluations

Basis Development	Configuration	A developer could modify an existing program in production, perform traces to the program and configure the production environment to limit monitoring of the program run by increasing alarm thresholds and eliminating audit trails through external OS comma
Basis Development	Transport Administration	A developer could create or modify a program in production and force the transport of these changes after the fact to conceal irregular development practices. This also enables the reverting back to the program's original version without any trace of the changes made in production.
Basis Utilities	Configuration	A developer could modify program components (menus, screen layout, messages, queries) and configure the production environment to limit monitoring of the program runs using the modified program components by increasing alarm thresholds and eliminating audit trail
Basis Utilities	Transport Administration	A developer could modify program components (menus, screen layout, messages, queries) and force the transport of these changes after the fact to conceal irregular development practices. This also enables the reverting back to the program components origin
Basis Table Maintenance	System Administration	An individual could modify data in tables or modify valid configuration values and setup the production environment to run transactions and programs using the inappropriately modified data. This could affect data integrity, system performance, and proper
Basis Table Maintenance	Client Administration	An individual could modify data in tables or change valid configuration and replicate these changes to other clients. This is particularly sensitive if client administration transactions come with client-independent authorization allowing the developer to
Security Administration	Client Administration	An individual could inappropriately modify roles and assignments and reflect this change to the production's mirror copy eliminating the chance to revert to the appropriate setup.
Security Administration	Transport Administration	A security administrator could make inappropriate changes to unauthorized security roles, transport them, and assign them to a fictitious user for execution.
Create Transport	Perform Transport	Can create transports, add objects to the transport, and move the transport: Can put unauthorized object changes into production, bypassing the Change Control process.
Maintain Number Ranges	System Administration	Can reset the number ranges (1) and delete your log/audit trail (2).
Maintain User Master	Maintain Profiles / Roles	One person controlling both the access in the profile/role and the user Ids increases the risk of inappropriate access
APO Maintain Model	APO Supply & Demand Planning	Unauthorized maintenance of planning model and version may adversely impact the production planning data stored in APO. This transaction should be limited to selected demand planning super user or manager.
APO Model & Version Management	APO Supply & Demand Planning	Unauthorized deletion of active planning version may adversely impact the production planning data stored in APO. This transaction should be limited to selected demand planning super user or manager.
APO active version)	APO Supply & Demand Planning	Unauthorized maintenance of planning model and version may adversely impact the production planning data stored in APO. This transaction should be limited to selected demand planning super user or manager.

APO Define Advanced Macros	APO Supply & Demand Planning	Access to maintain macros/rules should be controlled via change management process. Unsupported or incorrect adjustments are made to the macros/rules may result in inaccurate production planning and production scheduling.
Maintain Business Partner	Process CRM Sales Order	A user could create a fictitious business partner and initiate fraudulent sales orders for that partner. Master data such as business partners should not be maintained by the same users who process transactions using that master data.
Process CRM Sales Order	Delivery Processing	A user could create a fictitious sales order to cover up an unauthorized shipment.
Process CRM Sales Order	CRM Billing	Inappropriately create or change sales documents and generate the corresponding billing document in CRM.
Process CRM Sales Order	Maintain Billing Documents	Inappropriately create or change sales documents and generate the corresponding billing document in R3.
Service Order Processing	Service Confirmation	Enter fictitious service orders for personal use and accept the services through service acceptance. The user could prompt fraudulent payments. In addition spare parts could be fraudulently issued from inventory as a result of the confirmation.
CRM Billing	Maintain Business Partner	User can create a fictitious business partner and then process billing in CRM for that partner.
Maintain Billing Documents	Maintain Business Partner	User can create a fictitious business partner and then process billing in R3 for that partner.
Service Confirmation	CRM Billing	Inappropriately accept or confirm a service order and generate a corresponding billing document in CRM for the order.
Service Confirmation	Maintain Billing Documents	Inappropriately accept or confirm a service order and generate a corresponding billing document in R3 for the order.
Process Credit Memo	CRM Billing	User could create a fictitious credit memo and run billing due in CRM to prompt a payment to a customer. The customer could provide a kickback to the internal user.
Process Credit Memo	Maintain Billing Documents	User could create a fictitious credit memo and run billing due in R3 to prompt a payment to a customer. The customer could provide a kickback to the internal user.
Process Customer Invoices	Maintain Conditions	Pricing conditions could be manipulated to provide inappropriate discounts or incentives to customers which will be realized in an incorrect invoice.
Process CRM Sales Order	Maintain Conditions	A user could enter a sales order in CRM and lower prices via conditions for fraudulent gain
Maintain Opportunity	Process Payroll	Commission or Incentives may be paid based on the number of qualified leads. Inappropriately qualified leads could result in fraudulent commission payments.
Service Order Processing	Process Payroll	Commission or Incentives may be paid based on the number of service orders. Fraudulent orders could be entered to achieve higher sales for commissions.
Process CRM Sales Order	Process Payroll	Commission or Incentives may be paid based on the number of sales orders. Fraudulent orders could be entered to achieve higher sales reporting for commissions.

EBP / SRM Vendor Master	EBP / SRM Invoicing	Maintain a fictitious vendor and enter an invoice to be included in the automatic payment run
EBP / SRM Purchasing	EBP / SRM Invoicing	Purchase unauthorized items and prompt the payment by invoicing
EBP / SRM Purchasing	EBP / SRM Goods Receipt/Service Acceptance	Enter fictitious orders for personal use and accept the goods or services through goods receipt or service acceptance
EBP / SRM Invoicing	EBP / SRM Goods Receipt/Service Acceptance	Enter fictitious invoices and accept goods or services via goods receipt or service acceptance
EBP / SRM Vendor Master	EBP / SRM Purchasing	Maintain a fictitious vendor and initiate purchases to that vendor.
Bank Reconciliation	EBP / SRM Invoicing	A user can hide differences between bank payments and posted AP records.
EBP / SRM Goods Receipt/Service Acceptance	Enter Counts - WM	Accept goods via SRM goods receipts and perform a WM physical inventory adjustment afterwards.
EBP / SRM Goods Receipt/Service Acceptance	Enter Counts - IM	Accept goods via SRM goods receipts and perform IM physical inventory adjustment afterwards.
EBP / SRM Goods Receipt/Service Acceptance	Enter Counts & Clear Diff - IM	Accept goods via SRM goods receipts and perform IM physical inventory adjustment afterwards using powerful IM transactions
EBP / SRM Purchasing	Goods Receipts to PO	Enter fictitious orders for personal use and access the goods or services through goods receipt
EBP / SRM Purchasing	Service Acceptance	Enter fictitious orders for personal use and access the goods or services through service acceptance
EBP / SRM PO Approval	Goods Receipts to PO	Approve the purchase of unauthorized goods and hide the misuse of inventory by not fully receiving the order in R3
EBP / SRM Purchasing	EBP / SRM PO Approval	Where release strategies are utilized, the same user should not maintain the purchase order and release or approve it.
EBP / SRM Vendor Master	EBP / SRM PO Approval	Create a fictitious vendor or change existing vendor master data and approve purchases to this vendor
EBP / SRM Purchasing	EBP / SRM Maintain Org Structure	Enter fictitious orders for personal use and manipulate the organizational structure to bypass approvals
EBP / SRM Vendor Master	EBP / SRM Maintain Org Structure	Create or maintain fictitious vendor and manipulate the organizational structure to bypass approvals or secondary checks

EBP / SRM Maintain Shopping Cart	EBP / SRM PO Approval	Initiate purchases to selecting goods to be included in a shopping cart then approving the purchase
Maintain Hierarchies	AP Payments	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Process Vendor Invoices	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Manual Check Processing	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Cash Application	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Process Customer Invoices	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Maintain Cost Centers	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Maintain Asset Document	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Maintain Asset Master	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Revenue Reposting	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Post Journal Entry	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Maintain GL Master Data	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Post Journal Entry (misc Tax/Currency)	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Vendor Master Maintenance	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output
Maintain Hierarchies	Maintain Customer Master Data	AP/AR/GL master data creation and posting functions in conjunction with payment processing, receipt of money, GL account access; and the ability to modify ECCS hierarchy and reporting output