

# **Towards a Framework for Achieving Effective Segregation of Duties**

Akhilesh Chandra\*  
The University of Akron  
Akron, OH 44325

Megan Beard  
Deloitte and Touche LLP  
Cleveland, OH 44114

June 1, 2007

Submitted to  
The University of Waterloo  
Symposium on Information Systems Assurance  
October, 11-13, 2007

\*: corresponding author

## **Towards a Framework for Achieving Effective Segregation of Duties**

### **Abstract**

A critical element for the success of corporate governance is the effective segregation of duties in the internal control environment. However, a standard for segregation of duties roles is still lacking both in theory and practice. This paper develops a framework for achieving effective segregation of duties in the internal control environment. The framework leverages existing control frameworks and guidelines to build best practices for segregating duties in each major business cycle. The framework has implications for companies looking to automate the resolution of segregation of duties and reduce costs. From an assurance standpoint, auditors can benefit from the framework to increase efficiency and reduce audit costs. We provide extensions of the current study.

# **Towards a Framework for Achieving Effective Segregation of Duties**

## **I. Introduction**

The Sarbanes Oxley act is a comprehensive act to regulate company's internal controls. Segregation of duties is one of the most critical, least expensive and beneficial controls integral for effective regulatory compliance. Segregation of duties is required to be tested and reviewed to mitigate the risk of fraudulent activity. Section 404, Management Assessment of Internal Controls, requires companies to include in their annual reports an internal control report that states management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and an assessment of the effectiveness of the internal control structure and procedures.

Various guidance provided by the Treadway Commission's committee of sponsoring organizations and (COSO), control objectives for information and related technology (COBIT), and AICPA have categorized segregation of duties controls into recording, custody, access and transaction authorization. Each area focuses on the unique aspect of the task within any business process. An individual that has the ability to execute or is responsible for more than one of these key tasks has the potential to jeopardize the integrity of data and controls. However, both theory and practice still lack any standard process for achieving effective segregation of duties roles. From published guidelines this paper develops a framework for reducing segregation of duties conflicts in internal control environment.

Aside from regulatory compliance, best practices in segregation of duties are also imperative in the new economic and business model. Extensive computerization, widespread implementation of ERP systems, extended and distributed enterprises, integrated business processes, and outsourcing arrangements as common business norm have made the organizations more vulnerable to potential conflicts in segregation of duties. For example, ERP systems have collapsed all processes in a business transaction into one system. Computerization has made redundant the previous model of dividing work between humans to avoid potential conflicts. Maintaining and assuring data, systems and control integrity in an extended enterprise that also has outsourcing arrangements is complex and challenging.

These emerging developments create additional risks. Strict security and effective data management processes are essential to ensure data control, quality, traceability and audit ability (Bendarx 2005). Users are now given the ability to update data throughout the organization by editing one record. Therefore, a systematic and formal organizational level approach to security administration is crucial to protect the integrity of data and systems.

Evidence suggests that about 33% of users in companies have wrong rights assignments; about the same percentage have redundant or parallel access rights; about 83% of the organizations grant privileges in an ad-hoc fashion, or through cloning (i.e., John Doe gets the same rights as Jane Doe); privileges once granted are rarely revoked even if the responsibilities change (Eurikfy survey 2006). These issues present exacerbate risks

when individuals either transfer departments or leave the organization. Good and effective business practice requires that access rights are granted based on business roles and formal provisioning policies. In this paper, we propose a role based model of segregation of duties and access rights provides an effective mechanism to safeguard information resources and ensure data integrity.

The paper proceeds as follows: In the following section we briefly review the regulatory environment and its implication for effective segregation of duties; third section describes three access control models and leverages role based access controls to develop segregation of duties framework for each of the major business cycles; section four discusses implications of the framework and concluded the paper with a summary of the goals and direction for future extensions.

## **II. Regulatory environment and segregation of duties**

Companies spend years working on developing a product and creating a brand name. Careful planning, marketing research and development are done to create a company empire which is usually recognized globally. As the brand is created customers become comfortable with the product and their loyalty increases. Product names become more common and replace common nouns. For example – tissues are most often referred to as Kleenex and soda is often called Coke. Each of these companies has established brand loyalty to its greatest extent. As a result, profits increase and stock holders continue to invest heavily.

Investors look to Wall Street for guidance in purchasing stocks. Public companies face scrutiny for not meeting Wall Streets' expectations and as a result the stock prices fluctuate. Consequent to 2002 enactment of Sarbanes-Oxley Act (SOX), public companies are struggling to provide evidence of key internal controls. Besides analysis of reported numbers in the financial statements, there is greater focus on the auditor's opinion on internal controls. A company that has met Wall Streets expectations, but has a material weakness or significant deficiency noted within the auditor's opinion could experience an adverse impact on its stock value. Thus, if a company experienced increased revenue from prior year, but had a material weakness noted with regard to revenue recognition could be viewed by investors as another potential Enron scandal. No matter how strong the efforts are of an organization in the R&D, product development, customer service, the result of one deficiency has the potential to adversely effect a company.

One of the direct effects of regulatory environment is the steep rise in cost of compliance. By some estimates, between 2003 and 2004 audit fees for Fortune 1000 companies have increased by 66 percent (Kealey and Eldridge 2005). The costs of compliance are significant, but necessary for auditors to issue accurate opinion. Section 404 of SOX specifically requires auditors to attest to the integrity of companies' internal controls. Internal controls are required to be documented and tested by management. External audit is required to conduct an independent assessment and validate management's testing. The opinions auditors are required to issue on internal control can have a greater

cost impact than the cost associated with compliance (Kumar and Mathur 2004; Nambair 2003).

The role of the external auditor is to issue an opinion on the controls reviewed through 404 testing. Each control is tested and a conclusion is derived. Once all of the individual control activities are reviewed, the conclusions are aggregated. The aggregation process is required to determine the impact of each deficiency (Bendarx 2005). Once the impact is determined it is classified as a material weakness or as a significant deficiency. These results are communicated to the public through the annual reports.

A critical element in this implementation, review and attestation process is the concept of segregation of duties. Segregation of duties is an internal control that mitigates the risk of fraudulent activity. Actual job titles and organizational structures may vary greatly from one organization to another, depending on the size and nature of the business.

Whether an internal assessment is being performed or an independent audit, it is critical to gain an understanding of the relationship among various job functions, responsibilities and authorities in making an assessment of effective segregation of duties

Segregation of duty issues have become exacerbated due to the implementation of ERP systems during 1990s and the current trend towards systems' integration. In the past, each department within a company operated as silos. It was difficult to reconcile numbers and agree upon terms. As the systems become more integrated, the easier it is to manage the data. Each company is able to relay a single version of the business

transaction. But one person in the organization is also capable of affecting all related files. If not controlled, this feature of integrated systems has the potential to corrupt the corporate database.

The most common segregation of duty errors are to allow an individual to initiate, authorization and record a transaction. If a person has responsibility to authorize invoices and also initiate the purchase and processing the invoices then s/he can potentially defraud the company without getting noticed. Good and effective segregation of duties rules protect both the company from fraudulent activity and employees from being prosecuted

### **III. Role Based Segregation of Duties Framework**

Segregation of duties is not entirely a new phenomenon. Since early years of computer evolution, security administrators have dealt with data security issues. To control access to only authorized users, system administrators typically adopted one of three user access models: discretionary, mandatory, and role based.

#### ***Discretionary access controls***

Discretionary access controls restrict access based on the identity of users or need-to-know requirements of users. These are called discretionary controls since a user with certain access privileges can potentially transfer those privileges entirely or partially to other users. Such controls are pervasive in military set ups where documents are coded hierarchically as unclassified, classified, secret, and top secret. Each user is assigned a specific clearance level that allows access to documents at the specified level and below

along the classification hierarchy. Commercial operating systems (such as UNIX and Windows) use a modified version of discretionary access control where control resides with the creator of data or file. Access control policies are determined and implemented by the creator of those data and files. Discretionary access controls are more pervasive than other two control types of maintaining data integrity. However, maintaining data security and integrity is difficult and challenging using discretionary access controls. When employees are given the ability to set their own access privileges, there is a higher risk of the data being corrupt or inaccurate.

### ***Mandatory access controls***

Mandatory access controls assign security labels or classifications to information system resources. Access is allowed to entities (people, processes, devices) that have distinct levels of authorization or clearance. Typically, the operating system or security kernel is responsible for enforcing mandatory access controls. Thus, a formal, documented process of declassification is required for the operating system to reclassify a top secret information resource to a lower classification. Organization structures that operate on a strict hierarchical model (such as the military) utilize mandatory access controls to secure confidential information. Documents are classified and given associated levels of clearance. In most organizations, individuals are required to execute cross-functional tasks. The associated tasks typically do not reside within a hierarchy. Mandatory access controls can effectively lock documents with a top secret classification and may never be accessed by individuals without top secret clearance. Control problems arise in securing documents with lower level classification. As the security clearance broadens, users

begin to gain access to documents that do not correspond with their related job tasks. For example, a clerk's position might be classified as a mid to high security clearance level. Since no distinction is made between payables and receivables clerks, both are treated and granted equal access rights. Thus, a receivables clerk can access payables clerk's records. Access to both areas creates segregation of duties issues.

### ***Role based access controls***

Role based access controls grant access to information resources based on roles users perform in an organization. Thus, controls are tied and mapped to roles as opposed to any object, resource or user. The premise of role based controls is that role based privileges are stable (Sandhu and Coyne 1996). Roles are generic concepts and subject to least fluctuations compared with the users who fill the job function that role represents. Changes in business dynamics necessitate frequent changes in users and their privileges brought together by a role. Comparative efficiency and effectiveness of role based access controls (over the other two access controls) is apparent when ensuring data integrity during employee turnovers or transfers. The creation of roles helps to control system access during employee transfers and turnover which is the most common means of inappropriate access. When an employee is transferred s/he is simply relieved of the existing role and placed in to a new role. In the other two modes of access controls, the transferred employee would continue to maintain the original access in addition to gaining new access privileges. The mechanics of discretionary and mandatory access controls make it impossible to comprehensively determine all documents or system functions that each transferred employee had prior access.

To avoid conflicting duties as the business grows and evolves, a cross functional team should continually review and evaluate the existing roles and associated tasks. In large organizations a team of security administrators directly control and manage system roles and interrelationships.

The role based access is developed through a several step process. The process begins with identifying a set of tasks necessary to complete a job. Next, the tasks are mapped to the application system functionality. The roles are defined by the necessary function and access for each information resource. Figure I sequentially illustrates the process of assigning role based access. Specifically, following steps are needed to accomplish role based access controls:

1. All system functions are decomposed in a matrix, identifying each task on a separate line. Figure II illustrates an example.
2. The matrix is used to identify tasks that should be segregated. Figure III describes a process analysis of revenue cycle and identifies processes of potential segregation of duties conflicts. Process flow maps help to better visually identify violations.
3. The process with segregation of duty violations should be evaluated for any compensating controls to avoid potential loss. Further, if the vulnerability and associated risks are minimal, then it may not be necessary to segregate duties. Figure IV illustrates risk-vulnerability matrix to evaluate need for segregation of duties.

4. Once all tasks are appropriately segregated, they are grouped by business cycle.
5. Within each cycle, different roles are developed for each grouping of tasks.
6. The roles should be reviewed and evaluated on a regular basis by management.

This process greatly simplifies the creation and assignment of roles. The role creation process facilitates identification and resolution of segregation of duties conflicts. A primary constraint in its application is the time intensive nature of implementing role based access controls.

#### ***Role based access controls in business cycles***

In the following sub-section, we develop segregation of duties conflict and associated risk within each of the major business cycle—revenue, expenditure, financial, inventory management and fixed assets. In view of the pervasiveness and importance of information technology in business operations, segregation of duties was evaluated separately for IT. Each business cycle was evaluated individually. The rules were based on general tasks within each cycle. The listing of rules for each cycle is not comprehensive. The rules should be customized to each organization's internal job related terminology.

### ***Expenditure cycle***

The following segregation of duties should exist within the expenditure cycle:

- Signed checks, which have been compared to appropriate supporting documentation by the signatory, are delivered to someone independent of both the preparer and the initiator of the check for prompt mailing.
- Checks should not be returned to the preparer or initiator of the check subsequent to being signed and should be timely mailed to ensure that opportunity for misappropriation including 'teeming and lading' is minimized.
- The return address on the envelopes that are used to mail checks should be to a person(s) who does not prepare checks or approve payment requests for payment.
- Checks once signed should also be timely mailed and processed to accounts payable to ensure that the cash and liability balances are fairly represented in the accounting records. This is especially important at period ends.

**Related Accounts:** Operating Expense, Payables, Accrued Expense, Prepaid Expense

Business Cycle	SOD Conflict	Risk
Expenditure	Voucher Entry & Payment Creation	Payment Create conflicts with Voucher Entry. Checks should be approved by someone who did not initiate or prepare the check, in order to minimize the potential for concealment of fraud.
Expenditure	Vendor Maintenance & Voucher Entry	User has the ability to create/maintain vendor, in combination with the ability to create a voucher for that vendor.
Expenditure	Authorize Payment & Create Payment	Authorize Payment conflicts with Create payment. Checks should be approved by someone who did not initiate or prepare the payment, in order to minimize the potential for concealment of fraud.
Expenditure	Vendor Maintenance & Payment Entry	User can create/maintain vendors and create payments for the vendor.
Expenditure	Bank Account Maintenance & Vendor Payment	User can modify vendor bank information and create payment.
Expenditure	Authorize Payment & Maintain Vendor Master	Review, Authorize or Sign Checks conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.
Expenditure	Payables Configuration & All other Payables Functions	User can change configurations that would violate all other SOD rules
Expenditure	Print Checks & Enter Vouchers	Printing Checks conflicts with Enter Voucher. Checks should be approved by someone who did not initiate/prepare the payment or someone who entered the voucher in order to minimize the potential for concealment of fraud.
Expenditure	Voucher Entry & Payment Approval	Authorize Payments conflicts with Voucher Entry. Checks should be approved by someone who did not initiate or prepare the check, in order to minimize the potential for concealment of fraud.
Expenditure	Authorize Payment & Maintain Vendor Master	Review, Authorize or Sign Checks conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.
Expenditure	Vendor Maintenance & Purchase Order Entry	User has the ability to create/maintain vendors, in combination with the ability to create purchase orders for that vendor.
Expenditure	Approve Purchase Order & Vendor Maintenance	Authorize Purchases of Fixed Assets conflicts with Edit Vendor Master File. If one individual has responsibility for more than one of these functions, that individual could conceal errors or fraudulent activity.
Expenditure	Purchase Order Entry & Approval	Purchase orders are processed without prior approval (unauthorized)
Expenditure	Purchase Order Entry and Receive Goods	User can enter purchase orders and receive goods on the order.

### ***Information technology***

In relation to computerized information systems, we typically expect segregation of duties both within the information systems department and between information systems and business unit personnel. Furthermore, we expect (1) that access to production data by information systems personnel will be on an exception basis only and will require special authorization (e.g., to correct a problem caused by a system failure) and (2) that application system users will only be granted access to those functions and data required for their job duties. For example, individuals who are responsible for transaction processing should ordinarily have no responsibility for master file maintenance. A matrix similar to Figure II should be evaluated to determine segregation of duties conflicts.

### ***Inventory management***

Most systems of internal control rely on assigning certain responsibilities to different individuals, or “segregating” incompatible functions. Such segregation of duties is intended to prevent one person from having both access to assets and responsibility for maintaining the accountability for such assets.

For instance, in an inventory management system, different individuals are typically responsible for initiating or requesting a purchase, placing and inputting purchase orders, receiving goods, custody of inventories, maintaining inventory records and/or authorizing adjustments to costs or quantities including authorizing disposal or scrapping, making changes to inventory master files, performing independent inventory counts, following up on inventory count discrepancies, authorizing production requests and/or materials transfers, receiving/transferring goods into/from manufacturing, and shipping goods. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation. For example, if one individual had both the ability to process sales orders and access to the inventory management master files, that person could modify product selling prices and process unauthorized sales.

Such segregation of duties is especially important in relation to separating the custody or handling of inventory from access to inventory records and master files. In addition, physical counts of inventory should be performed by someone independent of custody of inventory and with no access to inventory records. Discrepancies noted in the

comparison of the counts to inventory records should also be followed up by an individual who is independent of the custody and recording of inventory.

Business Cycle	SOD Conflict	Description
Inventory	Initiating Purchase & Receiving goods	Update Purchases and Receive goods.
Inventory	Initiating Purchase & Custody of Inventory	Authority to purchase items and custody of inventory need to be segregated. Inventory balances could be misstated, if invalid purchases are executed and not appropriately recorded in inventory.
Inventory	Initiating Purchase & Maintaining Inventory Records	Purchasing conflicts with Maintaining Inventory Records. One individual should not be able to purchase goods and update inventory accounts.
Inventory	Initiating Purchase & Execute Changes to Inventory Master File	Purchasing conflicts with Executing Changes to the Inventory Master File. All Inventory Master File updates should be done by an individual independent of the purchasing function.
Inventory	Performing Inventory Counts & Initiating Purchase	Over/Under statement of inventory value manipulated by inappropriate purchases.
Inventory	Following up on Inventory Count discrepancies & Initiating Purchases	Manipulate the purchase records to reconcile with the inventory count.
Inventory	Authorizing Production Request & Initiating a Purchase	Authorizing Production Requests conflicts with Processing Sales Order Someone independent of the authorizing production should process sales orders.
Inventory	Process Sales Orders & Update Inventory Master	Individuals with access to process sales order should have inquiry only access to the Inventory Master File.
Inventory	Performing Inventory Counts & Custody of Inventory	Physical counts of inventory should be performed by someone independent of custody of inventory and with no access to inventory records

### ***Revenue cycle***

The following segregation of duties should exist within the revenue cycle:

Most systems of internal control rely on assigning certain responsibilities to different individuals, or “segregating” incompatible functions. Such segregation of duties is intended to prevent one person from having both access to assets and responsibility for maintaining the accountability for such assets.

For instance, in a revenue system, different individuals are typically responsible for recording a sales order, approving the terms of sale, custody of inventories, maintaining inventory records, shipping the goods ordered, invoicing the customer, maintaining accounts receivable records and/or authorizing adjustments to accounts receivable, following up on accounts receivable, making changes to accounts receivable master files, and customer service calls, and/or complaints. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.

**Related Accounts:** Sales, Receivables, Allowance for Doubtful Accounts

Business Cycle	SOD Conflict	Description
Revenue	Customer Maintenance & Cash Application	User can create/maintenance customer information and apply cash to the customer.
Revenue	Customer Invoicing & Cash Application Entry	User can create customer invoices, in combination with the ability to perform cash application.
Revenue	Sales Order Entry & Cash Application	User can create a sales order and apply cash to the sales order.
Revenue	Customer Maintenance & Invoicing	User has the ability to create/maintain customer information, in combination with the ability to invoice the customer.
Revenue	Customer Maintenance & Sales Order Entry	Creation of sales orders for unauthorized customers.
Revenue	Sales Invoicing & Customer Credit	User can create a sales invoice and modify the customer credit/payment terms.
Revenue	Sales Invoices & Sales Update	User can create sales invoices, and perform the sales update process.
Revenue	Sales Order Entry & Invoicing	User can create a sales order and invoice the sales order.
Revenue	Sales Order Release & Sales Invoicing	User has the ability to release and invoice a sales order.
Revenue	Sales Invoices & Sales Price Maintenance	User has the ability to create invoices and modify pricing structures.
Revenue	Sales Order Entry & Release	User can both enter and release/ship a sales order.
Revenue	Sales Order Entry & Sales Pricing	User has the ability to enter sales orders and modify pricing structures.
Revenue	Sales Invoice & Receive goods	Access to Enter Invoice and create Automatic Receipts will allow a user to create a fictitious invoice and then record receipts against the invoice.

### ***Fixed assets***

The following segregation of duties should exist within the fixed assets cycle:

Most systems of internal control rely on assigning certain responsibilities to different individuals, or “segregating” incompatible functions. Such segregation of duties is intended to prevent one person from having both (1) access to assets and (2) responsibility for maintaining the accountability for such assets.

Personnel responsible for fixed asset acquisition, disposal, recording, and maintenance should have responsibility for only one such function and have no system access to functions other than their assigned function. In addition, personnel who are responsible for fixed asset transaction processing should have neither responsibility for fixed asset master file maintenance nor update access to the fixed asset master file.

Related Accounts :Property, Depreciation Expense

Business Cycle	SOD Conflict	Description
Fixed Assets	Fixed Asset Maintenance & Transaction processing (Disposal or acquisition)	Initiate Disposal of Fixed Assets conflicts with Edit Fixed Asset Master File. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.
Fixed Assets	Fixed Asset Maintenance & Depreciation	Record Fixed Asset Transactions conflicts with Edit Fixed Asset Master File. One person should not have responsibility over both the access to assets and the responsibility for maintaining the accountability for such assets.
Fixed Assets	Fixed Asset Disposal & Adjustment	Initiate Disposal of Fixed Assets conflicts with Record Fixed Asset Transactions. One person should not have responsibility over both

		the access to assets and the responsibility for maintaining the accountability for such assets.
Fixed Assets	Asset Depreciation & Depreciation Adjust	One person should not calculate depreciation and create journal entries to adjust the depreciation account. There is increased risk of mis-stating depreciation due to inaccurate calculations.
Fixed Assets	Asset Acquisitions & Transaction Authorization	Asset Acquisitions conflicts with Transaction Authorization. One person should not have the ability to create and approve a purchase requisition for an asset.
Fixed Assets	Transaction Authorization & Recording	Transaction Authorization conflicts with Transaction recording. If one individual has authority to authorize and record transactions there is a high risk for fraudulent activity. Assets maybe acquired for personnel use but recorded on the books.
Fixed Assets	Custody of Assets & Disposals of Assets	Custody of Assets conflicts with authority to dispose assets. There is a risk of early asset disposal for personal use.

### ***Treasury***

The following segregation of duties should exist within the treasury cycle:

Most systems of internal control rely on assigning certain responsibilities to different individuals, or “segregating” incompatible functions. Such segregation of duties is intended to prevent one person from having both (1) access to assets and (2) responsibility for maintaining the accountability for such assets.

For instance, in a treasury system, different individuals are typically responsible for (1) recording of investment and/or borrowing transactions, (2) approving new investments and/or borrowings, (3) following up on reconciliation or confirmation of investments and borrowing to statements from third parties, (4) review and analysis of recorded

investments and/or borrowing transactions by means of summary reports of activities (e.g., describing liquidity, interest rate gap, dealing positions, exposure to counterparties), and (5) authorized signature of payments with respect to investment and/or borrowing transactions. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation.

In a manual system, segregation of duties may be enforced administratively, based on assignment of job responsibilities. In an automated system, segregation of duties is typically enforced through use of automated access restrictions.

Related Accounts: Notes Payable, Long-Term Debt, Investments/ Derivatives, Off-balance sheet derivative transactions, Investment Income, Interest Expense

### ***Payroll and personnel***

The following segregation of duties should exist within the payroll and personnel cycle: Inquiries from employees regarding payroll calculations and disbursements may arise for a variety of reasons. Any such queries should be followed up by personnel independent of the payroll preparation and disbursement process to ensure:

- Appropriate segregation of duties exist between preparation, disbursement, and human resources (or personnel management); thus, the potential for concealment of fraud is minimized.
- Any errors in calculation and/or disbursement are properly identified and corrected and not concealed.

- Confidentiality of employee personnel matters is maintained.

Typically, all payroll queries are directed to supervisory level staff in the human resource or personnel management department.

**Related Accounts :** Salary/ Wage Expense, Payroll Related Accruals

#### **IV. Implications and Conclusions**

Achieving effective segregation of duties has implications for streamlining the implementation and evaluation of internal controls. Once the process is established, it can be leveraged by available technologies to derive efficiencies. Operational efficiency requires that control mechanisms and their monitoring should be automated to reduce costs and increase their effectiveness. In this context, application developers have promoted tools to continuously monitor the control environment. While almost all major ERP systems can be configured to achieve segregation of duties goals, most of the challenges with the tools occur during implementation. For example, Oracle's 11i E-Business Suite can be configured to implement a continuous monitoring tool called the Internal Control Manager ("IC Manager"). The manager is designed as an "out-of-box" solution. The functionality and usefulness of the tool relies on the client's customization. The IC Manager requires specific rules to be programmed into the risk library identifying any combination of tasks in an enterprise as incompatible and report on those occurrences where a single user has access to them.

**Final note**

A critical element for the success of corporate governance is the effective segregation of duties in the internal control environment. However, a standard for segregation of duties roles is still lacking both in theory and practice. This paper developed a framework for achieving effective segregation of duties in the internal control environment. The framework uses role based access controls to identify segregation of duties conflicts within each cycle. Future extensions can develop industry specific framework to serve as a decision aid for effective internal control. Theory can also benefit by developing matrices that map each violation of segregation of duties to company's performance.

## References

- Bendarx, Ann. 2005. Compliance: Thinking outside the Sarbox. February 2005.  
<http://www.networkworld.com/research/2005/020705sox.html> (last accessed on May 30, 2007)
- Eurikfy Survey 2006. <http://www.eurikfy.com/solutions.sage.erm.survey.asp> (last accessed on May 30, 2007)
- Kealey, Burch T. and Susan W. Eldridge. 2005. *SOX Costs: Auditor Attestation under Section 404*. SSRN working paper series, June 13.
- Kumar, Ashwini and Mathur, Raghav. 2004. Implementing Sarbanes-Oxley. November :  
[http://websphere.sys-con.com/read/47221\\_p.htm](http://websphere.sys-con.com/read/47221_p.htm) (last accessed on May 30, 2007)
- Nambair, A. 2003. Solving Sarbanes-Oxley: A Business Intelligence Perspective. *DM Review*, December:1-3.
- Network Report 2005. Rules and policies vs. actual practice. *Network World*, February.  
<http://www.networkworld.com/newsletters/dir/2005/0207id1.html> (last accessed on May 30, 2007)
- Sandhu, R. and E. Coyne. 1996. Role-Based Access Control Models. *IEEE Computer* February: 38-47.

Figure I: Sequential process of assigning role based access



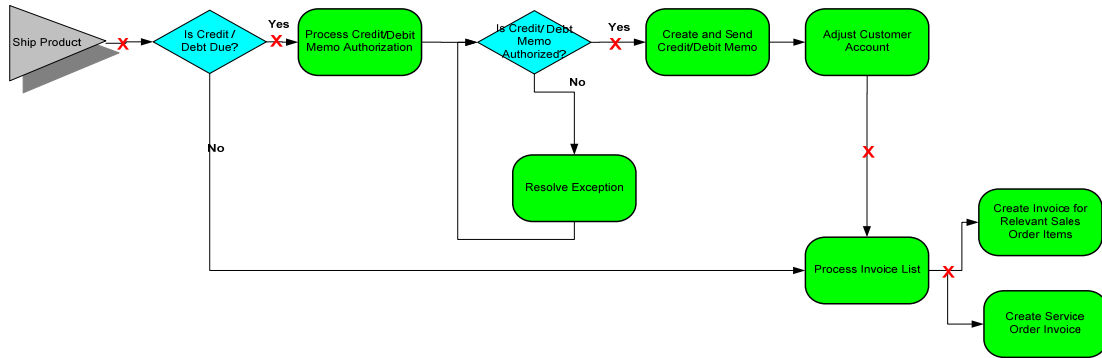
Figure II: An illustration of segregation of duties control matrix

	Systems Analyst	Application Programmer	End User	DB Administrator	Network Administrator	Systems Administrator	Tape Librarian	Systems Programmer	Quality Assurance
Systems Analyst			X			X	X		
Application Program			X	X	X	X	X	X	
End User	X	X		X	X	X	X	X	X
DB Administrator		X	X		X			X	
Network Administrator			X	X			X		
Systems Administrator		X		X			X		
Tape Librarian	X	X	X	X	X	X		X	
Systems Programmer		X	X	X			X		X
Quality Assurance			X					X	

**‘x’ indicates segregation of duties conflicts.**

*Adapted from ISACA Guidelines*

Figure III: Example of revenue process flow to illustrate segregation of duties violations



'x' identifies potential segregation of duties conflict

Figure IV: Segregation of Duties Evaluator

