A Conceptual Model for Segregation of Duties:

Integrating Theory and Practice for Manual and IT-based Processes

September, 2013
Abstract

A fundamental element of internal control is the maintenance of adequate segregation of duties (SoD), the allocation of work so that an individual cannot both perpetrate and conceal errors or fraud in the normal course of their duties. Notwithstanding its importance, there has been limited research describing the conceptual basis for determining how duties should be segregated. Significant differences exist between the SoD model proposed in the theoretical literature, the model described in the pedagogical and practitioner literature and auditing standards, and the practices commonly implemented by organizations. The purpose of this paper is to synthesize a model for SoD that reflects the insights of literature domains and is sufficiently descriptive to be applied effectively in typical business processes. The synthesized model calls for segregation of three sets of tasks: 1) asset custody, valuation and decision-making and recording; 2) primary authorization, recording of primary authorization, reconciliation and recording of reconciliation; and 3) secondary authorization, reconciliation of the record of primary authorization, and authorization of reconciliation. It also differentiates between primary SoDs, which allow detection of errors, and secondary SoDs, which help organizations to maintain a consistent, repeatable level of internal control. This is significantly different from both the three-way segregation called for in the theoretical literature and the model described in the pedagogical and practitioner literature and auditing standards. Insight provided by the new model provides an opportunity for organizations to enhance the quality or reduce the cost of internal control in organizations. Several future research opportunities are identified.
Introduction

The effective design and implementation of internal control has been a central question in accounting and auditing research and practice. A fundamental element of internal control is the maintenance of adequate segregation of duties (SoD), the allocation of work so that an employee cannot both perpetrate and conceal errors or fraud in the normal course of performing their duties (Stone, 2009). Segregation of duties is specifically cited as a control activity in the COSO framework (COSO, 1994), PCAOB Audit Standard No. 5 (PCAOB, 2007) and in auditing standard AU 314 (AICPA, 2006). In practice, implementing adequate SoD is a challenge, particularly for small firms. Gramling et al. (2010) found that in 2008, a majority of smaller firms with material weaknesses in internal control reported one or more SoD weaknesses.

Notwithstanding its importance, there has been relatively little research describing the conceptual basis for determining how duties should be segregated. Further, there are significant differences between the SoD proposed in the theoretical literature and that proposed in the pedagogical and practitioner literature and auditing standards.

Theoretical research addressing SoD (Tirole, 1986) has used agency theory to focus on collusion. It investigates the costs associated with a lack of independence between two roles: the agent (i.e., employee) and their supervisor. Agents have custody, or make decisions affecting the value, of assets. Supervisors act as conduits to the principal (the owner(s) of the firm) for information about the agent’s actions. This segregation of asset custody and decision-making from independent supervisory review and reporting to the principal is the most fundamental segregation of duties. The value of supervisory review is compromised if the supervisor colludes with agents to withhold information from the principal and share the benefits arising from this. This results in higher costs for the principal. Building on Tirole (1986), later studies examine
how these costs can be reduced by providing the principal with a second source of information about the agent’s activity, including another supervisor (Kofman and Lawarrée, 1993) or peer agents (Barra, 2010; Beck, 1986). The secondary source also provides the principal with information about the quality of primary supervisory review. This leads to a model segregating three duties: having custody of and making decisions about assets (done by the agent); primary review of the agent’s activity (done by an independent supervisor); and secondary review (by a second independent agent, supervisor or external auditor) (Figure 1).

A second, very different model is described in the pedagogical and practitioner literature and auditing standards. This model (Figure 2), hereafter called the ‘practitioner model’ (AICPA, 2006; Arens et al., 2013; COSO, 1994; Elsas, 1996; Elsas et al., 1998; Fishman, 2000; Louwers et al., 2013; Messier et al., 2012; PCAOB, 2007; Stone, 2009; Weigand and Elsas, 2012; Whittington and Pany, 2013), also recognizes the importance of segregating custody of assets from an independent review of that transaction, with two differences. First, in the practitioner model the term ‘authorization’ is used rather than ‘supervisory primary review’. Second, the duties included within custody and review/authorization are allocated differently. In the practitioner model authorizers are often described as being able to unilaterally initiate (i.e., have decision-making authority such as entering into commitments and setting prices or other valuations) and then authorize the transaction (e.g., Louwers et al., 2013), while the employee with custody merely follows the authorizer’s instructions concerning the physical custody of

---

1 Kofman and Lawarrée (1993) use the manager, internal and external auditors for their three-way model. These are equivalent to the roles of agent and primary supervisor and secondary supervisor which are more commonly used in the theoretical literature.

2 The Dutch auditing literature calls for segregation of custody, decision-making (corresponding to authorization), and registration (corresponding to recording). It also calls for segregation of two other duties: checking (including reconciliation and other control tasks) and execution/value creation (Elsas, 1996; Elsas et al., 1998; Weigand and Elsas, 2012); however, the Dutch publications explaining the rationale for these latter two segregations have not been published in English and are no longer in print. This may explain their lack of impact on the English-language audit literature. We therefore do not address these last two duties.
A Conceptual Model for Segregation of Duties in Manual and IT-based Processes

assets. This is in contrast to theoretical research which places both custody and decision-making authority over the asset in the hands of the agent, and limits the supervisor to providing an independent review of the agent’s actions. As will be discussed, the practitioner model’s approach limits the scope of authorizer fraud to embezzlement while ignoring fraud arising from collusion with outside parties.³

A third difference in the two models is that the practitioner model does not address the value of secondary authorization to allow the principal to evaluate the quality of primary authorization, a central issue in the agency theoretic literature and in internal control evaluation in the field.

A fourth difference is that the practitioner model goes beyond the theoretical literature to add a third duty to be segregated: the recording of transactions. This recognizes the critical role played by reliable records in facilitating the efficient authorization of large volumes of transactions in modern organizations. The recording duty includes keeping a record of transactions involving physical assets (e.g., sales and purchases) and decision-making or valuation involving physical assets or records-based assets and liabilities (e.g. the write-off of inventory or accounts receivable).

The analysis also indicates that segregation of custody and recording, which is so prominent in the practitioner model, is not critical to effective segregation of duties. The practitioner model’s segregation of custody of physical assets (custody) from valuation and decision-making relating to records-based assets (included in recording) prevents embezzlement by employees responsible for recording records-based assets and liabilities. This supplements but does not replace the primary review/authorization function. This is clear from practice in the

³ Though segregation of authorization and recording, discussed next, is sometimes interpreted as requiring that an independently created record be kept of authorizations, the practitioner model does not call for ongoing secondary review of this record. This secondary review is essential to prevent/detect collusion with outside parties.
field, where this segregation is often not implemented. For example, it is common for retail sales clerks to have custody of both inventory and cash and complete invoices; shipping clerks to complete packing slips used in the creation of invoices, and receiving clerks to prepare receiving slips used to record accounts payable. These transactions and records are almost universally subject to independent review.

The differences between the agency theoretic model, practitioner model and business processes actually implemented in the field reflect ambiguities in the conceptual model for SoD, and present an opportunity to enhance our understanding of this vital element of internal control. The purpose of this paper is to synthesize a model for SoD that reflects the insights of these three domains and is sufficiently descriptive to be applied effectively to typical business processes. This model addresses operational design considerations that are critical to SoD as implemented by organizations. It calls for segregation of three sets of tasks that are significantly different from the three-way segregation called for in the practitioner model. Though further specialization within these sets may enhance operational efficiency, it will not significantly enhance the achievement of SoD. The focus in the development of the model is on the allocation of duties that leads to independent detection of error or fraud rather than the action to be taken in response to detection, though the latter is necessary for SoD to have any effect (Carmichael, 1970).

The model will be developed in stages, starting with the insights developed in theoretical studies and then adding duties identified in the pedagogical and practitioner literature. This new model has nine duties and distinguishes between primary and secondary internal control effects. Primary effects are those arising from establishing the existence of SoD, while secondary effects are those associated with maintaining and enhancing the quality of SoD. A final section addresses the SoD implications of using information technology to support business processes.
1. Integrated Model of Primary SoD – Custody/Valuation/Decision-making and Authorization

We start by assuming that the organization has one or more owners and that due to the volume or scope of the organization’s activities preclude the owner’s direct authorization of all asset custody, valuation and decision-making activities performed by employees. This forces them to hire managers. The objective of segregation of duties is to prevent an employee from being able to misappropriate, destroy or waste organizational assets without it being detected and acted upon. Misappropriation can be for an employee’s own possession or for someone outside the organization. Like all internal control techniques, the implementation of SoD should be subject to cost-benefit constraints so that only processes that hold the potential for non-trivial losses are evaluated.

The primary duties to be segregated are asset custody/valuation/decision-making and authorization (Figure 3). Absent independent authorization, employees would be able to misappropriate or impair the value of assets without detection. Since the model does not yet address the existence of recording, all authorization is done by direct visual inspection.

Asset custody/valuation/decision-making (hereafter called custody for brevity) includes in its scope duties where things of value to the organization are handled, assigned a value or committed to, such that deficiencies in the performance of that duty could result in loss to the organization. This is consistent with the theoretical literature, which includes in its scope all decisions made by an agent that affect assets. The assignment of values and other decision-making is sometimes referred to as the initiation of transactions in the practitioner literature. In the sales cycle some examples of custody are:

---

4 If there is only one owner and they will review all transactions as they occur, further segregation of duties is unnecessary.
1) A salesperson setting prices for a sales order. An example of asset valuation without physical custody, assignment of an inappropriately low price results in a loss to the organization.

2) The quantity and promised ship date for a sales order if items are in short supply and production capabilities are constrained. Such a decision-making error could result in production scheduling problems, higher costs, and lower customer satisfaction.

3) The picking and shipment of inventory. All custody prior to shipment involves the risk of theft or damage by the employee. Shipment involves the risk of the employee shipping inventory to the customer that is not recorded on the packing slip.

4) The receipt of payments or other financial assets from customers, which can be stolen or lost by the employee.

In addition, while transactions may involve a simultaneous exchange of assets, it is more often the case that an asset is exchanged for a promise to receive a financial asset in the future. Until that financial asset is received, the asset exists only in the records of the firm (hereafter called a records-based asset) where it is vulnerable to loss. Examples from a simple sales cycle include:

1) Calculation of invoice total amounts (which become accounts receivable) based on quantity shipped per the packing slip and price per the sales order.

2) Recording invoice total amounts in the accounts receivable records.

3) Writing off of uncollectible accounts receivable.

4) Recording of payments received from customers to accounts receivable.

Including financial assets in the custody duty is in contrast to the practitioner model where maintenance of records-based assets is classified as part of the recording duty.
All asset custody duty activities should be authorized by an independent employee with expertise or predefined guidance that is sufficient to evaluate the appropriateness of the transaction. For example, if prices for complex custom-made products in a dynamic business setting are negotiated in the field by the sales agent, the authorizer must possess sufficient knowledge to assess whether the prices were appropriate. If a price list has been preapproved, the authorizer must use this list. The expertise required of the authorizer may range from being a highly trained expert with years of experience to an untrained novice who is checking conformance with easily-assessed written standards.

The independence of the authorizer is vital to the reporting of inappropriate transactions (Carmichael, 1970; Tirole, 1986). The authorizer should not directly or indirectly report to the asset custodian. Authorization by peers is possible, however peers are often a source of significant influence, therefore authorization is done most often by someone who is a hierarchical superior or in a different organizational subgroup. Independence is also essential in the opposite direction: as discussed in the introduction, the authorizer should not be involved in or otherwise control the specific custody duty they are responsible for authorizing. If the authorizer is segregated from custody but given the ability to direct custody activities without review, the lack of access to assets prevents them from embezzling assets, but the ability to control without review allows them to initiate an inappropriate transaction with a colluding external entity. This prohibition of authorizers from directing custody is consistent with the theoretical literature, where the supervisor is merely a self-interested conduit of information to the principal, and cannot affect the results achieved by the agent.

There is no restriction on the maximum number of different custody tasks that a single employee can perform to achieve this primary segregation of duties. The essential requirement is
that each one of these custody tasks be independently authorized. Thus, only two people are necessary to achieve a primary segregation of duties if one employee can perform all custody duty tasks. However, within the custody duty, the number of employees carrying out custody tasks relating to physical or financial assets (e.g. inventory, cash) should be limited in order to minimize the risk of theft or loss and associated costs of authorization. The practitioner model operationalizes this in a limited way by segregating processing of records-based assets from the custody of physical/financial assets, preventing employees handling records-based assets from embezzling physical/financial assets.

As noted in the introduction, the practitioner model goes beyond the agency theoretical model by segregating custody of physical and financial assets (e.g. inventory and cash) (in custody) from the processing of records-based assets (e.g., accounts receivable and accounts payable) (in recording). This segregation precludes one type of embezzlement: theft of assets accompanied by write-off of those assets, but is only useful to the extent there is a weakness in both of the other two segregations in the practitioner model: authorization of physical/financial asset transactions (authorization and custody) and authorization of records-based asset processing (authorization and recording). This physical/financial vs. record-based asset segregation cannot substitute for the other two segregations because it does not address the threat of other inappropriate records-based asset transactions. This indicates that classifying the

---

5 The division of a task into a series of interdependent subtasks, each performed by a different employee, is neither a necessary nor sufficient condition for achieving adequate SoD. It is essential that each employee performing a subtask be subject to at least one other employee who evaluates their work and will report any inappropriate action that might lead to a loss. For example, if five workers handle successive tasks in the sales cycle, absent and independent supervisor, SoD only exists if each worker’s task activity is reviewed by a worker performing a subsequent task. Absent this evaluation and reporting, there is no reason to expect a reduction in loss, the fundamental objective of SoD.

6 Ceteris paribus, monitoring several employees handling an asset is more costly than monitoring a single employee handling the same asset.

7 Elsas (2008) describes an approach for identifying and evaluating exposure to such embezzlements (i.e. single-employee ‘solo-fraud’ involving assets being stolen directly by the employee).
processing of records-based assets as a custody duty yields a more consistent and effective model of primary segregation of duties.

In order to enhance the efficiency of the authorization task, repeating or similar transactions or their elements may be classified into standard groups and approved beforehand (March and Simon, 1958). Some examples include sales order maximum quantities, price lists, maximum amounts for specific expenses (e.g., per diems for travel expenses, rent), and preapproved customers and their related credit limits. With preapprovals in place, the authorization task becomes a simple check of compliance, which may enhance the consistency of the authorization process. The creation of preapprovals is a specialization of the valuation and decision-making tasks within the asset custody duty, and therefore should be independently authorized.

The pedagogical and practitioner literature often suggests that, especially for computerized processes, changes to ‘master files’ (e.g., lists of preapproved customers, suppliers, prices), an asset custody duty, be segregated from the initiation of transactions, another asset custody duty. This specialization reduces the scope of error that can be made by the asset custodian creating the transaction, but does not address potential errors by the employee creating the master file. This indicates that this segregation of preapprovals or master file changes from custody of assets or other transaction initiation is not a primary requirement for effective SoD, but is instead a secondary enhancement.

The segregation of custody and authorization can operate in a preventive or detective manner. If the authorization occurs simultaneously with asset custody so that the transaction can be stopped before a loss occurs, then it is preventive, e.g., independent checking of quantities after packing but prior to shipment. If the authorization occurs after a loss might occur, then it is
detective, e.g., authorization of prices on sales after they are executed by salespeople in the field. The practitioner literature and auditing standards allows both approaches by defining SoD as a technique which reduces the ability to perpetrate and conceal errors (Stone, 2009). Preventive controls reduce the likelihood of perpetration of errors, while detective controls reduce the likelihood of concealment of errors. In practice, firms often find that a preventive approach is more cost-effective (Protiviti, 2007).

The segregation of custody and authorization reflects insight from the theoretical literature, but does not address the use of records, one of the hallmarks of modern organization. This is addressed in the next section.

2. Primary SoD with Recording of Custody Duty Activity

Recording is the capture of information of all key attributes of any asset custody activity performed. It is ubiquitous in modern organizations as a mechanism for enhancing the efficiency of the authorization process, yet is not specifically addressed in agency theory-based research examining SoD. Absent recording, all authorization would have to be performed as transactions occur by visual inspection (Figure 3). If transactions do not occur continuously at a single location, much of the time the authorizer is idle, significantly increasing cost, particularly if authorization requires significant expertise rather than a simple compliance check to standards. The essential benefit of recording is that it separates the gathering of data about custody activity from its evaluation in the authorization duty, in terms of both time and location. With recording, subsequent rather than simultaneous authorization is possible, eliminating idle authorizer time and allowing authorization to be done at any location the records can be transferred to. A potentially lower-skilled and therefore less costly record keeper can monitor asset custody activities, in turn reducing cost. For example, a clerical record keeper could be present to monitor
and record prices negotiated throughout the day, while an experienced manager could use the record to authorize the negotiated pricing of all sales orders for the day from several salespeople in just a few minutes.

Given that recording arises from an efficiency-driven division of the authorization task, it could be performed by the same employee as the evaluative authorization task and still maintain the primary level of segregation of duties described in Figure 3, i.e., preventing losses arising from custody/valuation/decision-making from being detected by a authorizer (Figure 4). As noted in the previous section, the practitioner model segregates recording from authorization. We believe that with respect to the recording of custody activity this is an artifact of the inappropriate classification of records-based asset activities as part of the recording duty.

3. Primary SoD with Reconciliation

The specialization of recording within authorization mitigates the cost of, but not the requirement for, an independent employee to review asset transactions. It is well-established in business process design practice that the cost of recording is largely eliminated if the employee engaging in the custody activity creates a record of their work while doing it;\(^8\) e.g., it is common for sales clerks to scan UPC tags to record sales and enter cash receipts, receiving clerks to enter quantities received, and bank tellers to record cash receipts and payments. However, an employee with asset custody has an incentive to create an inaccurate record of an inappropriate transaction. This renders the record unreliable, which in turn makes the authorization task ineffective. This conflict between the goals of productivity and safeguarding assets has long been recognized in the agency theoretical literature (Carmichael, 1970). Organizations mitigate the risk of inaccurate custodian-created records using two strategies.

---

\(^8\) This includes paper records created manually and computerized records created based on input by the employee performing the asset custody/valuation/decision-making task (e.g., scanning or keying).
First, for valuation and decision-making transactions with external parties, standard record forms are created (e.g., a sales order form) which state that only terms recorded on the form are a valid part of the transaction. This precludes a divergence between the agreed-upon value or commitment and the records.

Second, for custody activities involving physical or financial assets (e.g., inventory, cash) a new duty is created: reconciliation of assets involved in the transaction to the record (Figure 5). This duty can be performed on a periodic or sampling basis. Any discrepancy is reported for follow-up. The reconciliation duty arises from the subdivision of recording into two tasks: the creation of records (recording), and ensuring these records correspond to assets on hand (reconciliation). Because the latter task provides the information originally provided by direct visual inspection and creation of records in Figure 4, reconciliation should be segregated from asset custody, but need not be segregated from authorization. Examples include:

1) Prior to shipment, the reconciler checks the quantities in a sample of packages to the completed packing slips. Note that this is distinct from the authorization task, which focuses on whether the quantity recorded as shipped is appropriate i.e., it was the quantity authorized based the customer’s request and credit limit.

2) Cash and inventory given to a traveling salesperson being counted and recorded in the presence of the reconciler at the beginning and end of each trip, and the reconciler compares the differences to the quantity of each item recorded in the sales invoices.

3) Inventory in a warehouse is counted by the reconciler and compared to the quantities in the records used to determine inventory values.

4) Account receivable balances in the records are periodically confirmed with customers by the reconciler.
A limitation of this approach is that it requires that assets associated with all reviewable transactions be available to the reconciler. This may not be possible because the assets are no longer under the organization’s control (e.g., goods have been shipped), or have become indistinguishable from other transactions’ assets (e.g., currency cash receipts, or inventory received that have been incorporated into finished goods). This renders the transaction unable to be reproduced by the reconciler.\(^9\)

To address this limitation, the reconciliation may be done at the aggregate record-keeping level (e.g. total cash, accounts receivable or inventory accumulated at a point in time), however this allows the asset custodian to inaccurately record transactions so long as the recorded total agrees to the change in assets. For example, a salesperson could record a cash sale at a price lower than the amount they received and pocket the difference. To compensate for a potential understatement of the records for the asset sale, organizations often create incentives for the other party involved in the transaction to identify errors in the recorded document, e.g., require the customer to produce an invoice reflecting the price paid if they wish to obtain a refund, or offer a payment to the customer for reporting any errors to an independent manager.

The benefit to be gained from the use of reconciliation depends upon the frequency and time required for periodic reconciliations in comparison to continuous monitoring of the asset custody duty. As the reconciliation is done more frequently, its cost will approach that of recording and authorization discussed in the previous section (Figure 4).

In summary the four duty model segregated between two individuals that is portrayed in Figure 5 illustrates an efficient method for providing a primary level of SoD, so that

---

\(^9\) Blokdijk (2004) identifies this issue in the context of reperformance of internal controls by auditors, however it is also applies to the reconciliation duty.
inappropriate transactions engaged in by an employee responsible for asset custody will be detected by another employee, the authorizer.


The effectiveness of the segregation of duties illustrated in Figure 5 depends directly upon how well the authorization and reconciliation tasks are performed. Either task may be compromised by a lack of skill, effort, or by collusion between the asset custodian/recorder and authorizer/reconciler (Tirole, 1986). Ensuring that the authorization and reconciliation duties are performed effectively involves the performance of secondary duties which must be segregated from those in Figure 5. In practice, this is most commonly achieved by following the logic employed in moving from Figure 3 to Figure 4, so that records of primary authorization and reconciliation activities are kept and independently authorized (Figure 6). We use the term ‘secondary authorization’ to describe the independent review of primary authorization. We use the term ‘authorization of reconciliation’ to describe the independent review of the record of reconciliation. None of these forms of authorization or reconciliation is an explicit component of the practitioner model; however, as discussed in section 2, without them there is no justification for the practitioner model’s segregation of recording and authorization.

*Secondary authorization* can be performed via direct visual inspection in the physical presence of the primary authorizer as the primary authorization is performed, or by periodic/sample review of the record of primary authorization. The latter records-based approach is more common and requires a reliable record of the primary authorization; however records of primary authorization are usually created by the primary authorizer (e.g., signature noting supervisory approval of a sales order). If the transaction record indicates it was approved, the
secondary authorization will assess the quality of the recorded decision, whether the error is one in authorization or the recording of that authorization. An alternative approach is to have a second employee authorize asset-custody transactions in parallel with the primary authorizer, so that each transaction is authorized by two people (e.g., requiring two signatures on a check). This provides an alternate path for inappropriate transactions to be identified and reported. Two variations of the alternative path approach are investigated in the theoretical literature. Beck (1986) and Barra (2010) examine the use of informal peer agent monitoring (i.e., reporting of errors by other asset custodians), while Kofman and Lawarrée (1993) examine the use of a second authorizer on a selective basis.

Reliability of the record of primary authorization is provided by an independent reconciliation of the record of primary authorization. Its objectives are to ensure that all transactions were subject to primary authorization and that all recorded denials of transactions were in fact rejected or reported. It must be done by someone independent of the asset custody and primary authorization duties to ensure that gaps in recording of authorizations will be reported. As will be pointed out in the next section, this task is unnecessary if the primary authorization is recorded as part of an automated workflow process that includes all transactions (e.g. online review of electronically scanned expense reports).

This reconciliation can be done preventively or detectively. A preventive approach in a multi-step process has the custodian performing a task require that a record of the authorization of a prior custody task exist before commencing the current task, e.g., a supplier invoice will be rejected by the accounts payable clerk unless it is signed by the authorizer, and sales orders will not be shipped by the shipping clerk unless signed by the authorizer. A detective approach checks all asset custody transaction records for evidence of primary authorization and checks all
rejections/reported items to ensure the transaction either did not occur or was reported for follow-up.

The *authorization of reconciliation* ensures that the primary reconciliation task is performed effectively. It must be done by someone independent of the custody/recording and reconciliation tasks to ensure that reconciliation errors are reported. Whether done at the transaction level (e.g., checking of individual shipment quantities to the packing slip), or periodically (e.g., monthly bank reconciliations or quarterly inventory counts), the authorization of reconciliation duty must independently verify the assets and records that existed as of the date of the primary reconciliation by reviewing the record of reconciliation in order to detect errors in it. This is straightforward for assets that can be confirmed with other parties, such as bank accounts, accounts receivable and accounts payable, but imposes a challenge for internally managed assets like inventory because it demands that the reconciliation authorizer obtain their own evidence concerning the existence of assets as at the reconciliation date. Therefore in addition to the count of each inventory item performed by the reconciler, the reconciliation authorizer must perform his/her own count, though this could be done on a sample basis. Absent such evidence, there is no way for the reconciliation authorizer to evaluate the counting subtask within the reconciliation task,\(^\text{10}\) precluding the higher level of reliability associated with secondary SoD effects.

5. **SoD considerations arising in IT-supported processes**

The introduction of information technology (IT) to support the business process introduces additional considerations in implementing SoD. Any task performed by a computer involves software which may have programming errors (i.e., ‘bugs’) arising from its

\(^{10}\)As previously noted, Blokdijk (2004) describes an analogous challenge in the context of reperformance of internal controls by auditors which is also relevant to reconciliation and authorization of reconciliation.
development or maintenance. These defects could result in an erroneous transaction or attribute of a transaction, and/or erroneous records of the transaction. It is important to distinguish between IT-based execution of custody transactions or IT-based reporting used in authorization, and IT-based execution or recording of a manually input transaction.

*Computerized execution, recording, reporting, or authorization of transactions*

An erroneous transaction arising from a programming error could occur if the computer is responsible for the execution of a custody task, regardless of whether the transaction is performed automatically or is initiated by an employee e.g.,

1) Robotic routing of inventory items to create shipments, even if the desired destination is specified by an employee – a programming error could lead to incorrect allocation of items to shipping containers;

2) Funds transfer to suppliers, even if desired amount and payment destination are specified by an employee – a programming error could to a different amount being transferred than was entered;

3) Creation of invoices total amounts based on quantity shipped per the packing slip and price per the sales order – a programming error could lead to multiplication and addition errors; and,

4) Recording invoice total amounts in the accounts receivable records – a programming error could lead to a lost, invalid or inaccurate amounts recorded.

In such cases, the computer will also create a record of the transaction.

In this case the IT personnel who control the program (i.e., computer developers and operators) must be treated as if they simultaneously perform custody and recording duties. As a result, the program must be subject to independent review to detect errors that could result in
inappropriate custody transactions or inaccurate records of them. This is achieved by having all programs independently tested to ensure that (i) all custody tasks operate correctly and (ii) a complete, valid and accurate record of each transaction is created. Programs should be independently tested while stored in libraries that do not allow the programs to be modified. This precludes inappropriate changes to programs from being made during or after testing. Further, programs in the testing library should only be able to be copied from approved developer libraries, with copying controlled by a single employee who is independent of development and testing. This prevents insertion of inappropriate programs. Programs that are used in daily business processes are generally those run by IT operations staff. The IT staff should be limited to running programs that were copied into the production library after approval by independent testers, and logs of programs run should be kept and independently reviewed with reference to original user requests.

This SoD between programming, testing and operations within the IT function is necessary to provide a level of SoD consistent with the primary segregation of asset custody and authorization, allowing inappropriate transactions to be prevented or detected. Once this level of SoD has been achieved within IT, the activity that the computer performs without human input can be considered segregated from other duties performed by people.

Achieving secondary SoD within the IT function to ensure that the primary SoD are operating effectively requires a review of the operational effectiveness of both the testing function and controls preventing operators from using unauthorized programs, including access controls and review of IT operations logs.

Once computer-generated transaction records are created, they should not be able to be changed because records are the foundation of effective authorization. Therefore, the ability to
modify or delete records should be limited to a small number of employees independent of the custody task being recorded.

Similar considerations apply when the computer program is directly responsible for the authorization of transactions (e.g., an input control comparing prices input by the salesperson to a preapproved price range), or when IT-generated reports such as exception reports are used by an authorizer. Errors or omissions in an authorization or report would not directly result in an erroneous transaction; however they limit the effectiveness of the authorization task. When reports used by an authorizer are produced in a system where adequate SoD within IT exists, then the access controls described below are also necessary.

*Computerized execution and recording of a manually input transaction or manual authorization of a computer-generated report*

If the computer executes a custody or authorization task and does so based on user input, or a computer-generated report is used for the authorization duty, e.g.,

1) salesperson inputs a negotiated selling price into a computerized order system;
2) sales clerk scans UPC code and inputs quantities of items sold; and
3) authorizer approves expense reports online,
4) authorizer examines a report of checks prior to signature
then, in addition to SoD within the IT function, two further steps must be taken to restrict end-user access to each input task in order to maintain a primary level of SoD.

First, one employee should not have access to computer input functions for duties that are segregated. This requires that each user have a unique ID and that their access to system input functions be restricted so that they cannot perform incompatible functions. Absent this restriction, people using the system could perform incompatible duties, eliminating SoD, e.g., an
accounts payable clerk could enter an invoice on the computer system and then access the approval screen to approve it.

Second, the system must authenticate each employee accessing the system to ensure they are who they claim to be. This requirement also exists for manual systems in order to prevent forged documents; however it is more important in computerized systems because of the ease of access to such systems from remote locations and the lack of alternative means to identify forged transactions. It is usually achieved using a password known only to the user. This is sometimes supplemented by tokens or biometric measures. Absent adequate authentication, one user can impersonate another to override SoD, or a third party inside or outside the organization can impersonate both an asset custodian and authorizer to misappropriate assets.

The implications of these requirements are that both SoD within the IT function and across end-user functions are necessary to achieve a primary level of SoD in business processes supported by IT. Further, IT-supported tasks are only considered segregated from other business process tasks if they do not involve user input or evaluation e.g., automatic creation of invoices based on previously input sales order and shipping data, automatic posting of invoice amounts to customer accounts, and automatic recording of a primary authorization within a computerized workflow process.

An efficiency benefit of the computerization of the primary authorization task as part of a larger computerized work flow process (e.g. online submission and approval of expense reports) is that recording of primary authorization is performed by the computer, allowing recording to be considered segregated from the performance of the primary authorization, and this is done for all transactions in the underlying asset custody process. This removes the need for the reconciliation of primary authorization task, one of the secondary authorization duties in Figure 6.
6. Conclusion, Contributions and Future Research

The synthesized model calls for a segregation of three sets of tasks that distinguishes between primary segregations of duties which are necessary to detect misappropriation of assets, and secondary segregations which detect failures in performance of the primary duties and help organizations to maintain a consistent, repeatable level of internal control. It is significantly different from both the model implicit in previous agency theory-based research and the practitioner model described in the pedagogical and practitioner literature and auditing standards. Though further specialization within these three sets may enhance operational efficiency in larger firms, it will not significantly enhance the achievement of SoD.

This new model contributes to agency-theory-based SoD research by adding recording, the primary method of information gathering in organizations, and reconciliation, the dominant method for enhancing information quality when recording of asset custody is done by the agent, to the SoD model. This extension provides a deeper understanding of the implications of the model in realistic control settings, and suggests that its structure captures the attributes most salient in describing real-world business processes.

The model also suggests changes to the dominant practitioner model and contributes to the pedagogical and practitioner literature and professional practice in several ways. First, it highlights that the duty of authorization should only review and report on, and not direct or control, the actions taken by those performing asset custody duties. Allowing the authorizer to direct the actions of asset custodians limits the model to detecting embezzlement, and ignores the potential for inappropriate transactions with outside parties, even if these parties could be created by the authorizer. Second, it recognizes that in practice recording is often performed by the employee having asset custody, contrary to the segregation called for in the practitioner model.
The new model incorporates the reconciliation task to provide reliable records to be used in authorization. Third, the key role played by reconciliation and the importance of its segregation from asset custody and recording duties, but not authorization, is made clear. Fourth, the new model foregrounds the critical role of secondary authorization in enabling organizations to maintain segregation of duties at a consistent level over time. Fifth, it highlights that the segregation of custody of physical and financial assets from records-based assets that is called for in the practitioner model is not a primary requirement of SoD. Finally, the discussion of IT-supported tasks clarifies that they are only considered segregated if they are not subject to with human manipulation of input or evaluation. Altogether, the insight provided by the new model may provide an opportunity to enhance the quality or reduce the cost of internal control in organizations in the field.

Future theoretical modeling research could examine the behavior of cost functions arising from the transfer of recording to the agent responsible for asset custody, with performance of related reconciliations on a periodic basis. Empirical research could be conducted which compares the SoD proposed here to those recommended in the evaluation tools sold by commercial vendors. This could be complemented by a design science model to extending the REA framework (e.g., Church and Smith, 2008) to address SoD in the design of IT-based systems.
References
Figure 1. Agency Theory-based Model of Segregation of Duties

![Agency Theory-based Model of Segregation of Duties](image1)

Figure 2. Practitioner Model of Segregation of Duties

![Practitioner Model of Segregation of Duties](image2)

Figure 3. Integrated Model of Primary Segregation of Duties without Recording

![Integrated Model of Primary Segregation of Duties without Recording](image3)
Figure 4. Integrated Model of Primary Segregation of Duties with Recording\(^a\)

\(^a\) The information flow from Custody, Valuation, Decision-making to Primary Authorization allows for review by direct visual inspection in addition to indirect review via the records.

Figure 5. Integrated Model of Primary Segregation of Duties with Reconciliation allowing combination of Custody, Valuation, Decision-making with Recording to enhance efficiency
Figure 6. Integrated Model of Primary and Secondary Segregation of Duties allowing combination of Custody, Valuation, Decision-making with Recording