A framework for separation of duties in an SAP R/3 environment

The Authors

Adam Little, ***Ernst & Young, Brisbane, Australia***

Peter J. Best, ***School of Accountancy, Queensland University of Technology, Brisbane, Australia***

Abstract

The majority of medium-to-large international organizations have adopted enterprise resource planning systems (ERPs) of which SAP R/3 is the current market leader. This paper proposes a framework for the separation of duties in SAP R/3. Separation of duties is viewed as a critical component of an organization's internal control structure aimed primarily at reducing opportunities for fraudulent activities. R/3 assigns profiles consisting of authorizations to users. Accordingly, R/3 facilitates the implementation of "role-based access control", where these profiles may be designed consistent with organizational roles and assigned to users performing these roles. This paper proposes a framework for adequate separation of duties using a role-based approach in the financial accounting (FI) module of the R/3 system. Case studies were undertaken to refine the framework and to explore its application in a practical environment. This empirical research provided support for the adequacy of the proposed framework.

Article Type:

Case study

Keyword(s):

Enterprise resource planning; Financial accounting; Access control; Fraud; Security.

Journal:

Managerial Auditing Journal

Volume:

18

Number:

5

Year:

2003

pp:

419-430

ISSN:

0268-6902

1 Background

This paper develops a framework for the assessment of the separation of duties in an organization implementing the SAP R/3 enterprise resource planning system (ERP). R/3 assigns profiles consisting of authorizations to users. Accordingly, R/3 facilitates the implementation of “role-based access control”, where these profiles may be designed consistent with organizational roles and assigned to users performing these roles. This paper focuses on the separation of duties within the financial accounting (FI) module of SAP R/3. Separation of duties is viewed as a critical component of an organization’s internal control structure aimed primarily at reducing opportunities for fraudulent activities.

1.1 Threats to security

Computerised information systems, whilst providing many benefits to organizations, are also vulnerable to many threats including traditional threats to paper-based accounting systems and threats due to the nature of computerised information systems. These threats can be internal or external intruders attempting to access sensitive information, modify data, make fraudulent changes to programs, enter fraudulent transactions and perform other undesirable acts within the system.

In order to threaten security in these ways, unauthorized users must penetrate the system or authorized

users must gain access to unauthorized functions or areas within the system. Various methods have been used to perform such unauthorized functions (Peterson and Turn, 1967, pp. 291-2; Reid, 1987, pp. 103-5; Stoll, 1988, pp. 488-9; Smaha, 1988, p. 40; Spafford, 1989; Seeley, 1989, pp. 700-3; Lunt, 1993). These methods include:

- *Passive techniques*, including wiretapping, electromagnetic pickup, concealed transmitters, and electronic eavesdropping. These methods are used to discover information such as usernames, passwords, and message content.
- *Attempted break-ins*, or password guessing, which are used to gain access through an authorized user's login.
- *Masquerading*, which occurs when an intruder "masquerades" as an authorized user. This can be achieved by several methods: logging in with the target user's password and username; tapping into the line between the authorized user's workstation and the central computer; or using an authorized user's workstation that has been left logged on to the network.
- *Browsing*, which occurs when authorized users attempt to access unauthorized functions or sensitive data.
- *Viruses and worms*, which are programs that invade systems and are used to gain access to data, destroy or manipulate data and applications, or simply to use resources such as storage, memory, and processor time.

This paper focuses on browsing techniques. Authorized users can be a threat if their activities are not restricted so as to prevent possible fraud or access to unauthorized areas in the system. Albrecht *et al.* (1984) conducted a study of firms that were victims of fraud. They concluded that three elements contribute to the probability of an employee defrauding an organization. These elements are situational pressures of the employee, opportunities to commit fraud, and either a low level of integrity or some way to rationalise the fraud. Of these three elements, the organization has control only over the level of opportunity to commit fraud within the organization.

Albrecht *et al.* (1984) examined organizational factors common to organizations that were victims of fraud. The most common factor identified was that too much trust was granted to certain employees. Other factors included the lack of: a proper procedure for authorisations; separation of transaction authorisation from custody of assets; and separation of accounting duties.

A common theme among these organizational factors is that there is typically a lack of proper separation of duties in organizations that suffer fraud. These results indicate that organizations are under significant threat even from authorized users if those users' activities are not correctly restricted. The next section introduces the main countermeasures available to organizations to counter these threats to security.

1.2 Countermeasures

In order to protect themselves from the threats to security outlined in the previous section, organizations may employ certain countermeasures. Best *et al.* (1997) identify four main categories:

1. *Authentication*. This countermeasure is aimed at restricting entry into the system. The methods available to ensure proper authentication of users include user names with passwords, challenge-response systems, biometrics, and smart cards (Carroll, 1987, pp. 249-55; Pfleeger, 1989, pp. 233, 453-4).
2. *Access control*. This countermeasure is designed to prevent unauthorized user activities through browsing. The purpose of access control is to restrict users' access to data and functions within the system in order to prevent unauthorized use (Ferrailo *et al.*, 1992). Ideally users should be restricted to data and functions that are required for them to fulfil their organizational role. This is generally referred to as "role-based access control".
3. *Cryptography*. This countermeasure involves encoding data so that it will not be understandable if it is revealed through unauthorized access. This technique can be applied to data files, passwords, on line transactions, and other sensitive data (Davies and Price, 1989).
4. *Audit trail analysis*. This is a *post hoc* analysis of the records of user activity in the detailed system logs to detect failed attempts to perform unauthorized functions and to highlight unusual patterns of user behaviour, such as logins after hours.

1.3 Separation of duties

Ferrailo *et al.* (1992) noted that "although more of a policy than a mechanism, separation of related duties is used in deterring fraud within financial systems. Such duties can include authorising, approving and recording transactions, issuing or receiving assets, and making payments. Separation of related duties refers to the situation where different users are given distinct, but often interrelated tasks such that a failure of one user to perform as expected will be detected by another. For separation of related duties to be effective, computer capabilities must be partitioned. These capabilities must be accessible only to users or processes associated with specific tasks".

Research into internal controls and external auditors' judgments has indicated that the assessment of separation of duties is a dominating factor in an auditor's evaluation of an internal control structure (Ashton, 1974; Ashton and Brown, 1980; Hamilton and Wright, 1982). Clark and Wilson (1987) examined commercial and military security models and found that separation of duties in performing transactions in commercial security models was an important aspect of maintaining data integrity. A simple model whereby a transaction could not be executed by one user, but must be broken up into two or more steps, was proposed. The authors noted that this model was overly simplistic but stated that "the separation of duty determination can be rather complex, because the decisions for all the transactions interact".

Srinidhi (1994) performed a study of the importance of separation of duties as an internal control by means of a survey of auditors. The findings indicated that auditors place significantly lower reliance on internal control systems without adequate separation of duties. The functions identified as being incompatible were:

- Assigning the responsibilities for both authorising and executing a transaction to the same person.
- The same person is responsible for defining the conditions for a transaction and checking whether

those conditions are satisfied.
- Combining the responsibilities for the authorisation of a transaction and the custody of the asset(s) involved in the transaction.
- Combining the responsibilities for authorising and accounting for a transaction.
- Combining the responsibilities for the accounting of a transaction and the custody of the asset(s) involved in the transaction.
- Accounting functions for two different transactions are assigned to the same person.

Arens and Loebbecke (2000, pp. 295-6) prescribe four general guidelines for the separation of duties that are designed to prevent both fraud and error:

1. *Separation of the custody of assets from accounting*. This prevents a person with custody of an asset from disposing of the asset and adjusting the records to conceal the action.
2. *Separation of the authorization of transactions from the custody of related assets*. The authorization of a transaction and the handling of the related asset by the same person increases the opportunity for fraud.
3. *Separation of operational responsibility from record-keeping responsibility*. If a division is responsible for preparing its own records and reports, there may be a tendency to bias the results to improve its reported performance.
4. *Separation of information technology (IT) duties from duties of key users outside IT*. Program modifications should be performed only by authorized IT personnel. Users outside IT should be responsible for authorizing transactions, on-line data entry, correction of errors in input, and review of output from the system.

The extent to which duties may be separated depends on the size of the organization. Often, the apparent lack of adequate separation of duties in smaller organizations can be compensated for through the active involvement of the owner/manager.

In ERP environments with hundreds or even thousands of users accessing the system on-line, the only way to separate duties within the computer system is to assign authorizations and profiles to users which prevent them from performing incompatible functions. A set of principles extending beyond those above are required to govern the development and assignment of these access rights.

1.4 Separation of duties principles

There is a significant amount of literature related to role-based access control and separation of duties (Kuhn, 1997; Moffett, 1988; Sandhu and Coyne, 1996; Bertino *et al.*, 1997; Sandhu, 1998; Kuhn, 1997; Ahn and Sandhu (1999). This literature, however, does not progress any further toward a framework for separation of duties than that of Clark and Wilson (1987).

This paper proposes seven basic principles for the separation of duties within the general ledger (GL), accounts receivable (AR), and accounts payable (AP) applications:

1. *Users who can create and modify master records should not be able to post transactions*. Users who can maintain vendor master records and post transactions (invoices and payments) could create a fake vendor record and pay a fictitious invoice without detection. If these duties were separated, this fraud could only be accomplished with the collusion of two personnel.
2. *Credit management should be separated from master record maintenance in accounts receivable*. This is to avoid the master record clerk creating a fake customer master record and granting credit to it.
3. *Dunning and credit management should be separated from invoice and receipt data entry*. This is to provide an independent check on data entry and to preserve the independence of the officer in charge of credit.
4. *Receipt data entry should be separated from invoice and credit memo data entry*. This is to provide a check against lapping and other fraud and error.
5. *In accounts payable, cheques should be managed and payments performed by someone other than the person who enters vendor invoices*. This ensures that payments and invoices are an independent check on each other. For example, if an employee could enter both then he or she could post a fictitious invoice and then pay it.
6. *Writing off an account receivable as a bad debt should be separated from receipt data entry*. This is because a clerk could fail to record a receipt and write the account off as a bad debt to cover theft of cash.
7. *Users' activities should not cross boundaries between GL, AR, and AP*. This separation is necessary so that the control accounts in GL can provide a check against AR and AP and so that offsetting transactions between AR and AP are properly authorized.

These principles are summarised in Table I.

The next section gives a brief overview of SAP R/3 and its security system.

1.5 SAP R/3

SAP R/3 is an ERP. It is comprised of a collection of modules including financial accounting, cost controlling, materials management, production planning and human resources. Of these modules, only the financial accounting (FI) module is required for R/3 to function. The other modules provide further capabilities for the system and are integrated with FI. This research is concerned only with the FI module and will focus on general ledger (GL), accounts receivable (AR), and accounts payable (AP).

The motivation for this study stems from the dominance of SAP R/3 in the international medium-to-large size organization market, the critical nature of separation of duties, and the lack of research into how to implement and assess this important internal control in R/3 environments.

The next section describes the way in which user authorizations are administered in the R/3 system.

Role-based access control in R/3

R/3 facilitates the implementation of role-based access control (RBAC). RBAC is a method of restricting users' access to certain functions within the system. It is a "logical access" control. This means that the software itself restricts access, as compared with "physical access" controls such as a lock on the computer room door. RBAC applies the "principle of least privilege", which means that users have to be "authorized" to perform a certain action rather than "restricted" from performing other actions (Pfleeger, 1989, p. 246). Authorizations are associated with roles. Roles are assigned to users. These authorizations are necessary for users to be able to perform their duties. If a user's authorization profile contains no authorizations then that user cannot perform any action on the system. Users should have sufficient authorizations to be able to perform their duties and no more than that. Reviewing separation of duties in an R/3 system requires an understanding of several concepts, namely authorization objects, authorizations, profiles, and transaction codes.

Authorization objects are defined in the R/3 documentation (SAP AG, 1997):

Authorization objects allow you to define complex authorizations. An authorization object groups together up to ten authorization fields in an AND relationship in order to check whether a user is allowed to perform a certain action. To pass an authorization test for an object, the user must satisfy the authorization check for each field in the object.

Authorization objects are templates for authorizations. For example, one authorization object is "accounting document: authorization for company code". This authorization object has two fields:

1. A list of the company codes where documents can be processed.
2. A list of the activities permitted for document processing in the abovementioned company codes.

Authorizations are defined in the R/3 documentation as (SAP AG, 1997):

Authority to perform a particular action in the R/3 System. Each authorization refers to one authorization object and defines one or more permissible values for each authorization field listed in the authorization object. Authorizations are combined in profiles which are entered in a user's master record.

An authorization usually consists of two fields (but may have up to ten fields). The first field is usually the domain which could be one or more company codes for example. The second field is usually the activity permitted in the domain. This could be create, change, display, etc. Authorizations are based on authorization objects.

Authorizations in R/3 are not assigned individually to users. Profiles, incorporating lists of authorizations, are created to represent user roles within the organization. These profiles are allocated to user master records and the users are then permitted to perform the functions authorized within that profile. Users may be allocated multiple profiles, if appropriate, and composite profiles which consist of two or more "simple profiles".

Each menu function in the R/3 system is assigned a transaction code. Transaction codes are linked to authorization objects. For a user to be authorized to perform a transaction code he/she must have authorizations in his/her profile(s) that are based on specific authorization objects. For example, to perform transaction code F-01 (posting document), users must have a valid authorization in their profile that is based on authorization object F_BKPF_BUK – Accounting Document: Authorization for company code. The authorization objects required for each transaction code are detailed in Table USOBT in SAP R/3.

1.6 Scope of this research

This project involves the development of a separation of duties framework for the FI module of SAP R/3.

The framework consists of a set of organizational roles with allocated transaction codes and associated authorizations, developed from a set of separation of duties principles. Deviations from this framework by an organization may indicate a lack of proper separation of duties. A series of case studies are conducted to assess the appropriateness of this framework and to identify potential areas for refinement.

2 Framework development

The primary objective of this framework is to propose a set of organizational roles for GL, AR, and AP based on the separation of duties principles outlined in section 1. Transaction codes and associated authorizations are allocated to these roles. This framework will assist auditors responsible for assessing separation of duties in an ERP environment. Deviations from this framework by an organization may indicate a lack of proper separation of duties. As described in section 1, a breakdown in separation of duties increases an organization's exposure to employee fraud and error. These roles provide a reference point for the assessment of the separation of duties in an organization's R/3 FI profiles.

The following sections describe the design objectives of this framework in relation to general ledger, accounts receivable and accounts payable.

2.1 General ledger

The specific objective within GL is to separate the entry and posting of GL transactions from the authorization to create, change and delete GL master records (principle G.1). In order to achieve this separation, two GL roles are proposed – GL supervisor and GL data entry. Master record maintenance is deemed to be the more senior duty, and is allocated to the GL supervisor. Transaction entry and posting are allocated to the GL data entry profile. The transaction codes associated with these two functions are illustrated by Table II.

A further profile is necessary to incorporate financial accounting transactions such as closing entries, accruals, tax returns, maintenance of bank master records, and archiving functions. This profile is titled "Accountant" and it is a senior profile which spans GL, AR and AP.

2.2 Accounts receivable

The following separation of duties principles were used to develop the proposed framework in AR:

- Separation of master record maintenance from transaction entry.
- AR.1. Separation of credit management from master record maintenance.
- AR.2. Separation of dunning and credit management from invoice and receipt data entry.
- AR.3. Separation of receipt data entry from invoice and credit memo data entry.
- AR.4. Separation of bad debts management from receipt data entry.

To achieve adequate separation of these duties, four AR profiles are proposed: AR supervisor, AR clerk (master record maintenance), AR data entry (invoice), and AR data entry (receipts). The accountant profile was allocated financial accounting duties within AR. The transaction codes associated with these four roles are shown in Table III.

2.3 Accounts payable

The following two separation of duties principles were used to develop the proposed framework in AP:

1. G.1. Separation of master record maintenance from transaction entry.
2. AP.1. Separation of payments and cheque maintenance from invoice data entry.

To achieve adequate separation of these duties, three AP profiles are proposed: AP Supervisor, AP Clerk, and AP Data Entry. The transaction codes that are assigned to these roles are given in Table IV.

Allocating authorization objects and field values to roles

Having identified the minimum number of different roles required to achieve separation of duties, it is now necessary to allocate the remaining transaction codes to the roles created. For example, transaction code “FD03 – AR master record – display” was given to all AR roles as well as the accountant role. This was based on the assumption that merely viewing a master record was not a critical function and that for convenience it should be allocated to all AR roles. In contrast, transaction code “F.64 – correspondence – maintain” was allocated to AP supervisor and not AP data entry, even though it is not a critical function. This distinction was made on the assumption that maintaining correspondence was not something that would be performed by a data entry employee.

To permit the assessment of authorizations given to the GL, AR and AP roles, the next stage in framework development was to identify the authorization objects and required field values for each transaction code in each role. This was achieved by analysis of the USOBT table which specifies the relationships between transaction codes and authorization objects. Using this table, a list of authorizations for each profile was generated.

Once the list of authorizations was established for each profile, the next step was to examine whether the critical transaction codes were separated using these authorizations. A list of the critical transaction codes and their corresponding authorizations was reviewed for adequate separation of duties. Some problems were found – particularly with posting. For example, many of these transactions had the same authorization object – F_BKPF_BUK with the activity field value "1" (create). A profile that contained this authorization could perform any of the document posting transaction codes. A list of the critical transaction codes which only require this authorisation object and field value is given in Table V.

It follows that further restriction is required to achieve satisfactory separation of duties. One method to improve restriction is the use of the authorization object S_TCODE – Authorization Check for Transaction Start. This authorization object enables an administrator to specify what transaction codes may be executed by a profile. Use of authorizations based on this object could eliminate the problems outlined previously.

3 Case study analysis

This section describes the case studies that were performed in the course of this research. The objective of these case studies is to test the application of the theoretical framework and to further refine the framework. Three case studies were performed:

1. This initial case study analysed SAP predefined profiles. The transaction codes for each profile in FI were available for analysis.
2. This case study involved an analysis of the security model of an actual company (Company A). This security model provided details of organizational roles and authorizations for each profile. As such, the FI roles and profiles were analysed.
3. This case study analysed the security model of another actual company (Company B). This security model provided details of transaction codes not authorizations. As such, only the design not the implementation of the security model is analysed in this case study.

In each case study the methodology applied was to review the separation of duties using the framework developed and then to classify differences as either anomalies (i.e. problems with separation of duties in the case study) or as contributions to the framework. The sections following outline the findings for each of the case studies.

3.1 Case study 1

Case study 1 examined the predefined profiles available from SAP that are relevant to GL, AR, and AP within the FI module. In this case study the authorizations were not available to be reviewed. Only the transaction codes were available. The roles available in GL, AR, and AP are displayed in Table VI.

The duties assigned to the roles in case study 1 are quite broad. These profiles differ from the theoretical framework developed in this research in several fundamental aspects. The profiles do not include a GL

supervisor – these responsibilities are given to the accounting manager. The supervisor profiles inherited all of the duties of the clerk profiles. Finally, the accounting manager and accounting clerk profiles include duties from GL, AR, and AP. These combinations of duties include several assignments of incompatible duties to the same role.

The lack of roles that maintain master records presents a problem. This duty is consequently assigned to either the supervisor or the data entry (clerk in this case) profiles. The other main problem with these profiles is that the supervisor "inherits" all of the duties of the lower profiles. For example, the AR supervisor can perform all of the functions of the AR clerk and the accounting manager can perform all of the duties of AR supervisor, AP supervisor, AR clerk, AP clerk, and GL clerk.

The lack of separation of duties in this case study can be demonstrated by a few examples:

- AR and AP clerks can maintain master records and post transactions. Therefore, an AP clerk could change the payment details of an accounts payable to a bank account held by that employee and then post payments to that account payable to his or her own bank account. Alternatively, an AP clerk could create a fake vendor master record and post fabricated invoices to that vendor and have the system pay his or her bank account.
- The supervisor can maintain master records, post transactions, maintain credit (in AR), maintain cheques, and perform cheque reconciliations. There is no control over the activities of this user. He or she could defraud the organization in any of a number of ways.

In summary, the profiles of case study 1 offer very limited separation of duties. This supports the statement by Haelst and Jansen (1997) that, "… usage of standard R/3 authorizations and profiles is not recommended as these are defined too broadly".

3.2 Case study 2

Case study 2 consisted of an analysis of Company A's FI security model. This document contained details about the various organizational roles and the profiles that were created to fill those roles. The document gave details of the duties assigned to each role and the authorizations assigned to each profile.

3.2.1 Design of roles for case study 2

The security model gives details of the duties to be authorized for each profile. The profiles or roles developed include GL supervisor, GL data entry, AP supervisor, AP clerk, AP data entry, AR supervisor, AR clerk, AR invoice entry, and AR receipt entry. These profiles are summarised in Table VII.

These roles differ minimally from the framework developed by this research in the duties to be authorized for each profile.

The design of these roles incorporated satisfactory separation of duties. In addition to the critical

separations of duties included in the framework, the security model of Company A included a separation of the entry and posting of AR and AP transactions. This is achieved through the use of the “park” and “post parked” transactions. In Company A’s security model the data entry profile can park transactions such as invoices and credit memos, and the supervisor can post the parked transactions. This mechanism provides a separation of the entry from the authorization of transactions and may be included in the framework as an optional separation. If an organization separated invoice and credit memo data entry from posting using this method, separation of invoice and credit memo data entry is unnecessary.

The documentation provided by Company A for case study 2 includes both the design of the roles, and the authorizations that will be assigned to the profiles for these roles.

3.2.2 Authorizations for case study 2

This section analyses the authorizations assigned to each profile by Company A to assess the effectiveness of the implementation of the security model.

Problems were apparent with the authorizations granted to the FI profiles for Company A. These problems include: no S_TCODE authorizations, use of “*” in ACTVT (activity) fields, and the use of “*” in KOART (account type) fields.

Authorizations based on the S_TCODE Authorization Check for Transaction Start authorization object are necessary to achieve adequate separation of duties. The transaction codes executable by a profile should be specified using the S_TCODE authorization object as well as the authorization objects that are linked to the critical transaction codes through the USOBT table. The implication of Company A not using the S_TCODE authorization object is that there is no separation of duties between AR invoice entry and AR receipt entry. It appears that Company A has attempted to overcome this inadequacy by using the authorization object F_BKPF_BLA Accounting Document: Authorization for Document Types to specify different authorization groups for the data entry profiles. This is not an adequate solution however, as F_BKPF_BLA is not linked to any of the data entry transactions through the USOBT table. The result is that authorizations based on this authorization object will not be checked for the critical data entry transactions (invoices, credit memos, receipts, etc.).

Company A has used “*” in its activity fields. In R/3 a “*” is interpreted as being any value. Use of “*” in authorizations could potentially grant more authorization to users than is intended. Company A has used “*” in its account type fields as well as its activity fields. This reduces the separation of duties between GL, AR, and AP. The account type fields should contain a “k” for accounts payable, an “s” for general ledger, or a “d” for accounts receivable.

3.3 Case study 3

Case study 3 involved an analysis of Company B’s transaction codes that were assigned to the various organizational roles. The authorizations used to implement these profiles were not available for analysis.

The roles that were deemed to be relevant to this research and the critical duties allowed for each are summarised within Table VIII.

The allocation of responsibilities in GL and AP in Company B corresponds with the proposed theoretical framework for separation of duties. The allocation of responsibilities in AR, however, results in a breakdown of separation of duties in this area.

Anomalies are apparent only in AR. One major cause of these anomalies is that there is not a specific role for customer master record maintenance as there is for vendor master record maintenance in AP.

The AR clerk should not be permitted to maintain customer master records as well as posting invoices and credit memos. The ability to perform both of these functions increases the opportunities for an employee to defraud the organization. The AR clerk would also not normally be permitted to maintain customer credit and post invoices. The ability to post invoices and maintain credit results in a loss of the independence of the “credit manager”.

The AR supervisor should not be permitted to post invoices and maintain credit for the same reason as for the AR clerk. For the same reasons, the AR supervisor should not be permitted to post invoices and maintain master records.

Finally, the cashier should not be permitted to post AR credit memos as well as record AR receipts. This is critical as a credit memo could be substituted for a receipt in order to cover a theft of cash.

Although not specifically an anomaly, care should be taken with some of the transaction codes assigned in these roles. Transaction codes such as F.80 – Mass Reversal of Documents, FB01 – Post Document, FB02 – Change Document, and FB08 – Reverse Document are powerful transaction codes and care should be taken to ensure proper authorizations are in place to restrict the use of these transaction codes.

4 Conclusion

This paper has proposed a framework for the separation of duties within the GL, AR, and AP functions of the FI module of the SAP R/3 system. The development of this framework involved understanding the role of access controls, examining the SAP R/3 access control mechanism, developing principles for the separation of duties, and the development of a theoretical framework.

Analyses of three case studies provides support for the appropriateness of the framework. Both Company A and Company B had attempted to implement separation of duties using principles similar to those developed in this paper. The deficiencies in the SAP predefined profiles are well known and this was confirmed by the analysis in case study 1. Opportunities to refine the proposed framework were identified based on the results of case study 2.

Two limitations of this research must be acknowledged. It is recognized that decisions about the internal

controls to be implemented within an organization should be based on an appropriate risk analysis. Discussion of the relative costs of controls such as separation of duties was deemed to be beyond the scope of this study. Second, the framework developed was based on theory and refined using case studies. The limitation of case study research is that the results can provide support only for theoretical propositions and are not generalisable to populations (Yin, 1989). Rigorous empirical testing has not been performed on this framework.

This paper presents opportunities for several new avenues of research that would be beneficial. The theoretical framework could be extended to the other modules and the other functions within R/3. This would provide a complete picture of the duties and roles within R/3 as well as providing guidance for appropriate separation of duties within FI as a whole. A complete framework would be of great value for management and internal auditors, external auditors, and SAP implementation partners.

A decision support application could be developed to automate the arduous task of checking the authorizations within profiles to assess adherence with the theoretical framework. This application could be designed using software such as Microsoft Access whereby the SAP tables could be downloaded and tested using a Visual Basic application. Development of an application of this type would improve the analysis of an organization's separation of duties by eliminating human error and improving efficiency.

The case study research performed in the course of this research has identified problems with separation of duties in both of the organizations examined as well as identifying separation of duties problems in the SAP predefined roles. Although the empirical studies undertaken are not generalisable to the population, they do identify the need for further research on the adequacy of separation of duties in the population of organizations using SAP R/3 and the consequential implications.

Finally, the theoretical framework could be assessed through a survey of experts (CIS auditors and SAP security administrators). Consensus on the adequacy of this framework could be assessed and useful feedback on cost-benefit issues could be gathered.

Table I *Principles for the separation of duties*

ImageGL critical transaction codes

Table II *GL critical transaction codes*

ImageCritical AR transaction codes

Table III *Critical AR transaction codes*

ImageCritical AP transaction codes

Table IV *Critical AP transaction codes*

ImageTransaction codes requiring authorization object F_BKPF_BUK

Table V *Transaction codes requiring authorization object F_BKPF_BUK*

ImageCase study 1: roles and duties

Table VI *Case study 1: roles and duties*

ImageCase study 2: roles and duties

Table VII *Case study 2: roles and duties*

Table VIII *Case study 3: roles and duties*

References

Ahn, G.J., Sandhu, R. (1999), "The RSL99 language for role-based separation of duty constraints", *Proceedings: Fourth ACM Workshop on Role-based Access Control*, NIST, VA, pp.43-54.

[Manual request] [Infotrieve]

Albrecht, W., Howe, K., Romney, M. (1984), *Deterring Fraud: The Internal Auditor's Perspective*, The Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, .

[Manual request] [Infotrieve]

Arens, A.A., Loebbecke, J.K. (2000), *Auditing: An Integrated Approach*, Prentice Hall, Upper Saddle River, NJ, .

[Manual request] [Infotrieve]

Ashton, R. (1974), "An experimental study of internal control judgements", *Journal of Accounting Research*, Vol. 12 No.1, pp.143-57.

[Manual request] [Infotrieve]

Ashton, R., Brown, R. (1980), "Descriptive modelling of auditor's internal control judgements: replication and extension", *Journal of Accounting Research*, Vol. 18 No.1, pp.269-77.

[Manual request] [Infotrieve]

Bertino, E., Ferrari, E., Atluri, V. (1997), "A flexible model supporting the specification and enforcement of role-based authorizations in workflow management systems", *Proceedings: Second ACM Workshop on Role-based Access Control*, NIST, VA, pp.1-12.

[Manual request] [Infotrieve]

Best, P., Mohay, G., Anderson, A. (1997), "MIATA: a machine independent audit trail analyser", *Australian Computer Journal*, Vol. 29 No.2, pp.57-63.

[Manual request] [Infotrieve]

Carroll, J.M. (1987), *Computer Security*, Butterworths, Stoneham, MA, .

[Manual request] [Infotrieve]

Clark, D., Wilson, D. (1987), "A comparison of commercial and military computer security policies", *IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Oakland, CA, .

[Manual request] [Infotrieve]

Davies, D.W., Price, W.L. (1989), *Security for Computer Networks*, Wiley, New York, NY, .

[Manual request] [Infotrieve]

Ferraiolo, D.F., Gilbert, D.M., Lynch, N. (1992), *Assessing Federal and Commercial Information Security Needs*, National Institute of Standards and Technology, Gaithersburg, MD, .

[Manual request] [Infotrieve]

Haelst, W., Jansen, K. (1997), "Control & audit of SAP R/3 logical access security", *IS Audit & Control Journal*, Vol. 3 pp.37-44.

[Manual request] [Infotrieve]

Hamilton, R., Wright, W. (1982), "Internal control judgments and effects of experience: replications and extensions", *Journal of Accounting Research*, Vol. 20 No.2, pp.756-65.

[Manual request] [Infotrieve]

Kuhn, D. (1997), "Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems", *Proceedings: Second ACM Workshop on Role-based Access Control*, NIST, VA, pp.23-30.

[Manual request] [Infotrieve]

Lunt, T.F. (1993), "A survey of intrusion detection techniques", *Computers & Security*, Vol. 12 No.4, pp.405-18.

[Manual request] [Infotrieve]

Moffett, J. (1998), "Control principles and role hierarchies", *Proceedings: Third ACM Workshop on Role-based Access Control*, NIST, VA, pp.63-9.

[Manual request] [Infotrieve]

Peterson, H.E., Turn, R. (1967), "System implications of information privacy", *Proceedings AFIPS Conference*, Vol. 30 pp.291-300.

[Manual request] [Infotrieve]

Pfleeger, C.P. (1989), *Security in Computing*, Prentice-Hall, Englewood Cliffs, NJ, .

[Manual request] [Infotrieve]

Reid, B. (1987), "Reflections on some recent widespread computer break-ins", *Commun. ACM*, Vol. 30 No.2, pp.103-5.

[Manual request] [Infotrieve]

SAP AG. (1997), *FI System Administration Guide Release 3.1*, SAP AG, Walldorf, .

[Manual request] [Infotrieve]

Sandhu, R.S. (1998), "Role activation hierarchies", *Proceedings: Third ACM Workshop on Role-based Access Control*, NIST, VA, pp.33-42.

[Manual request] [Infotrieve]

Sandhu, R.S., Coyne, E.J. (1996), "Role-based access control models", *Computer*, Vol. 29 No.2, pp.38-47.

[Manual request] [Infotrieve]

Seeley, D. (1989), "Password cracking a game of wits", *Commun. ACM*, Vol. 32 No.6, pp.700-4.

[Manual request] [Infotrieve]

Smaha, S.E. (1988), "Haystack: an intrusion detection system", *4th Aerospace Computer Security Applications Conference*, Orlando, FL, pp.37-44.

[Manual request] [Infotrieve]

Spafford, E.H. (1989), "The Internet worm: crisis and aftermath", *Commun. ACM*, Vol. 32 No.6, pp.678-87.

[Manual request] [Infotrieve]

Srinidhi, B. (1994), "The influence of segregation of duties on internal control judgements", *Journal of Accounting, Auditing & Finance*, Vol. 9 No.3, pp.423-44.

[Manual request] [Infotrieve]

Stoll, C. (1988), "Stalking the wiley hacker", *Commun. ACM*, Vol. 31 No.5, pp.484-97.

[Manual request] [Infotrieve]

Yin, R.K. (1989), *Case Study Research: Design and Methods*, Sage, Newbury Park, CA, .

[Manual request] [Infotrieve]