ERPSEC - A REFERENCE FRAMEWORK TO ENHANCE SECURITY IN ERP SYSTEMS

Prof. S.H. von Solms, M.P. Hertenberger
Rand Afrikaans University

Abstract: This paper proposes a method of integrating the concept of information ownership in an Enterprise Resource Planning (ERP) system for enhanced security. In addition to providing enhanced security, the reference framework ERPSEC developed for this study provides better manageability and eases implementation of security within ERP software packages. The results of this study indicate that central administration, control and management of security within the ERP systems under investigation for this study weaken security. It was concluded that central administration of security should be replaced by a model that distributes the responsibility for security to so-called information owners. Such individuals hold the responsibility for processes and profitability within an organization. Thus, they are best suited to decide who has access to their data and how their data may be used. Information ownership, coupled with tight controls can significantly enhance information security within an ERP system.

Key words: Database security, security policy, misuse detection, authentication, information flow

1. INTRODUCTION

The concept of information ownership has been around for some time. However, its full benefit has never been harnessed in the ERP software space[5]. In ERP software systems, security is critically important. ERP systems are fairly complex and integrate functions and data across an entire enterprise. The fact that human resources data and financial information is

integrated with production planning and sales data should illustrate the requirement for stringent security subsystems. Additionally, ERP systems in use by an organization contain critical business data. Hence, it is essential that such information be protected from unauthorized access. Unauthorized access to the data within the ERP system's database must be prevented, especially since a large percentage of fraud takes place within the organization[4].

In the study completed by the authors[1], various ERP software products where evaluated to determine how security is implemented. In all cases, the security subsystem forces centralized control by one or more central security administrators. It is the view of the authors that this approach, though practical and widely used, weakens security. In the study, a framework for implementing the information ownership approach to strengthen and enhance security within ERP software packages is proposed. This paper briefly summarizes some of the findings.

2. THE TRADITIONAL APPROACH AND ITS PROBLEMS

To provide the reader with sufficient information on the traditional way of implementing security within an ERP environment, the following brief discussion is provided.

ERP implementation projects require many skilled resources from various disciplines. To ensure adequate knowledge transfer, staff members from the organization for which the ERP system is being configured are included in the project team. The technical skills required to implement and configure the software are quite different to the business and process knowledge that is required to change the workings of the software components to support the business processes and add value to the organization. Technical skills are generally required to assist in the implementation and realization of a security policy. Briefly stated, the reason for this is due the fact that:

- security is generally considered an administrative, and therefore a technical role
- the implementation of an adequate security infrastructure requires specific knowledge relating to the ERP system's technical architecture. In all the ERP systems reviewed, detailed knowledge of system objects and their use and function is a prerequisite.

- the ERP systems available provide only a centralized way of implementing and maintaining security objects and settings

2.1 Specialization by discipline and resources

Hence, the traditional approach to the implementation of security within ERP systems is based on a centralized approach. There is nothing physically wrong with this approach. However, the centralized approach provided by ERP software packages does not allow the organization to expand its security infrastructure to comply with information ownership principles. To illustrate this in a different way, consider that ERP software systems contain a huge variety of functions and configuration possibilities. To understand all facets of a single system in detail is virtually impossible. Hence, specialization of skills takes place almost naturally. Business-oriented users are more concerned with the real-world application of the ERP software and how the configuration can be changed to mirror the processes within the organization. In contrast, technical experts and administrators delve deeply into the architecture and structure of the system; they are more concerned with how the system has been built. The knowledge divide becomes apparent when a business process owner requests the configuration of a security object from a technical security administrator. As the focus of both parties is different, understanding from both sides may be lacking.

2.2 Translation of business requirements into technical terms

The requirements of the business process owner for increased security in order to protect the organization from fraud, for example, must be translated into a technical specification by the security administrator. Though this process may be fairly simple in some cases, more complex requirements may not be easy to implement technically. An example of a simple security requirement may be the restriction of permitting only certain users print to a certain printer in the organization. The requirement can be fairly easily understood and translated into the technical format required by the system. Similarly, testing such an access restriction is fairly simple and does not provide too many possibilities for failing. A far more complex requirement may include access restrictions to data for certain material types, cost centers and locations. In a large organization many material types and locations may be present. Ensuring that all users have been allocated the correct security objects becomes far less trivial to implement and configure than the preceding example involving only a single printer.

2.3 Possible introduction of errors and hence weakened security

To restate the above concept, the assumption that a central system or security administrator has the ability to understand all nuances and specifics of each functional area is often incorrect. Instead, the security administrator must gather information from each area of the business. Once all these details have been gathered, the security administrator is able to translate the requirements of each business area into the appropriate roles and profiles within the ERP system. In many cases, the security administrator has to select objects manually to create the appropriate access authorization for the user. It should be clear that such a process is often completed with a number of errors and omissions.

2.4 The security administrators as a bottleneck

The security administrator in an ERP environment must contend with numerous business areas and functional areas. These include sales, finance, human resources and so on. Adding the various organizational layers on top of this, together with various stakeholders the business may have to support, creates an environment in which the centralized security administrator becomes a central bottleneck. Figure 1 illustrates this more vividly:

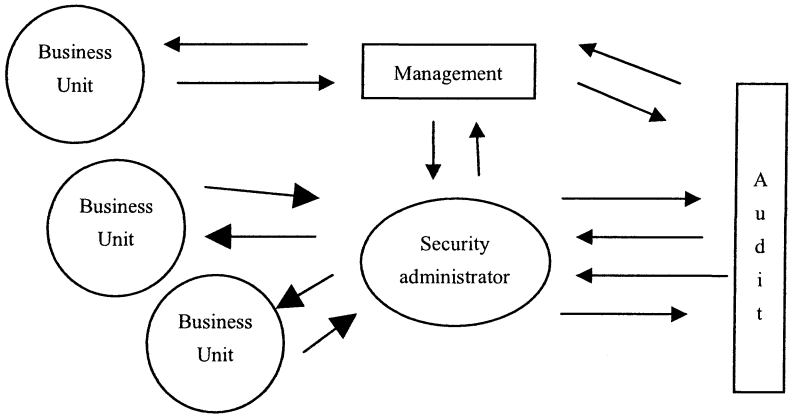

Figure 1. Centralized security within an ERP environment

Figure 1 indicates one of the main problems with the implementation of security within an ERP environment, namely that of creating a bottleneck by

having to route all requests for change through one or more administrators who possess the technical knowledge on how to deal with the request.

3. THE APPROACH USING INFORMATION OWNERSHIP

The authors are of the opinion that the support of information ownership can assist in enhancing the configuration of security objects in ERP software environments[8]. In addition, the approach using information ownership provides various additional benefits that are useful to organizations implementing ERP software packages to support their business processes. To this end, the ERPSEC framework has been developed and will be briefly discussed during the remainder of this paper. Prior to the discussion relating to the ERPSEC framework, it should be clear why the authors consider the approach using information ownership to be beneficial.

3.1 Reduction of complexity

Within traditional ERP environments, the centralized approach to implementing access control and access restrictions enables one or more security administrators to create and maintain profiles, roles and user master records. As has been mentioned above, this approach suffers from a number of problems, most notably that the security administrator cannot and usually does not understand the complexities of the actual business processes within the organization and how these have been mapped to the functionality of the selected ERP software package. To combat this problem and to promote more rigid and adequate security within an ERP environment, it is necessary to deal with complexity within the system as a whole. The provision of an integration layer to reduce complexity is a definite requirement. Such an integration and simplification layer is not available in any of the currently available ERP software packages. The ERPSEC framework proposes an integration layer to simplify the creation of ERP security objects. Figure 2 illustrates the integration layer and should be compared to Figure 1 above.

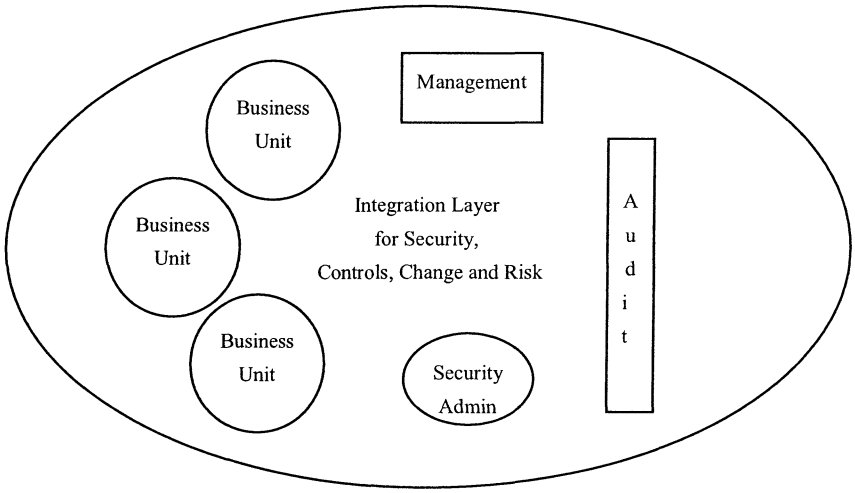

Figure 2. Providing an integration layer to support information ownership

As an aside, the addition of a suitable integration layer that has the ability to translate and present technical security objects to non-technical users makes the decentralization of security configuration a distinct possibility. This may not always be recommended, but goes a long way in supporting segregation of duties issues and need-to-know principles in certain organizations. Further comment regarding this will be made once the ERPSEC framework has been discussed in more detail.

3.2 Simplification

The sudden popularity of ERP software packages stemmed primarily from their ability to integrate all data within the organization, to deliver real-time results and reporting and to make specific functionality available to the user at the desktop level. In stark contrast to the adaptability and flexibility of being able to configure the ERP software package to the needs of the business, the configuration of security related objects is completed by technical staff. Mention has already been made of the complexity of ERP software packages. This complexity is necessary for the software package to be adaptable to different industries and legal requirements. The ERP software packages investigated during the course of this study provide full support for the configuration of the software to adapt it to support various business processes. Similar functionality for the configuration of security objects is missing. In fact, all security-related objects are generally grouped

together and are not easily distinguished from one another. The ability to document the necessary access restrictions and security objects is hampered by very technical naming conventions. In ERP systems targeted at organizations with a smaller user population, the configuration of the security subsystem is often fairly trivial, offering the security administrator very little flexibility. The ERPSEC framework attempts to simplify the creation and maintenance of security related objects within an ERP environment.

4. WHY INFORMATION OWNERSHIP?

To enhance the concept of information ownership, the concept of an information owner must first be explained. The concept of permitting individuals within the business to manage and maintain their own information security is termed information ownership. Information owners are individuals in charge of a certain business area within the organization. Generally, these individuals are already in charge of a division, such as finance or sales, for example. In other words, these individuals are stakeholders within the business and carry some form of responsibility. It is the goal of the information ownership approach within the ERPSEC framework to provide the tools to individuals who are held liable or responsible for certain actions taking place within the business. If these individuals are not provided with the tools to support their decision-making process and the ability to ensure that their data is safe, they cannot be held responsible for anything that occurs within their sphere of responsibility. This concept aligns closely with that of segregation of duties. One definition[2] states that segregation of duties is a method of working whereby tasks are apportioned between different members of staff in order to reduce the scope for error and fraud.

Prior to the ERPSEC framework being discussed, some advantages of the information ownership approach are listed here:

- Technical security administrators are experts at maintaining technical security objects, but often lack the necessary knowledge relating to the impact these objects have when allocated to the wrong user. Information owners are aware of their business area and know the impact of incorrect allocation of one or more security objects
- Technical security administrators are generally not aware of the staff members in various organizational units. Therefore, the creation of roles and allocation of security objects is done based purely on feedback and information received from the relevant organizational unit or division. In

contrast, information owners are focused on their business area, know their staff and can make informed decisions based on their capabilities and possible weaknesses

- The ability to compartmentalize security objects based on their applicability to various sections of the business can radically reduce the time and effort required to implement and configure the ERP security subsystem. As each information owner can take care of his own section of the business, this permits the security administrators to take on a role that examines security in more detail across the enterprise. The integration layer provided by the ERPSEC framework supports this compartmentalization.
- Information ownership goes a long way to promote and control segregation of duties issues and improve corporate governance. Due to a large number of legislative requirements, this is a very important topic for organizations at present. At present, very little support is provided by existing ERP software products to assist organizations in dealing with these complexities.

5. THE ERPSEC REFERENCE FRAMEWORK

The ERPSEC reference framework has one primary aim, namely to enhance and increased the security and access control within an ERP system. Existing ERP system already contain a centralized security subsystem. Hence, retrofitting the ERPSEC framework to an existing product may not be an easy task. The definition of ERPSEC in the study provides an object-oriented definition that should ease a possible physical implementation sometime in the future.

In addition to enhancing security within an ERP system, ERPSEC will attempt to cater for the following:

- a reduction in complexity of the security configuration;
- the ability to increase responsibility and accountability within the organization;
- a faster implementation time by providing decentralized access to security objects;
- to improve the quality of the security configuration as a whole;

These goals can be realized by considering the current state of security subsystems in existing ERP software packages. A brief review is provided below.

5.1 Traditional ERP security subsystems

The discussion presented in this paper provides the most basic details regarding the ERPSEC framework. The complete study by [1] contains a detailed description including object and table definitions for the creation of the framework in "real-life".

A mention of the centralized nature of the security subsystems of existing ERP software products has already been made. In the model employed by these products, a single administrator modifies and maintains the security objects for all users, regardless of their place within the organization.

This is depicted in Figure 3.

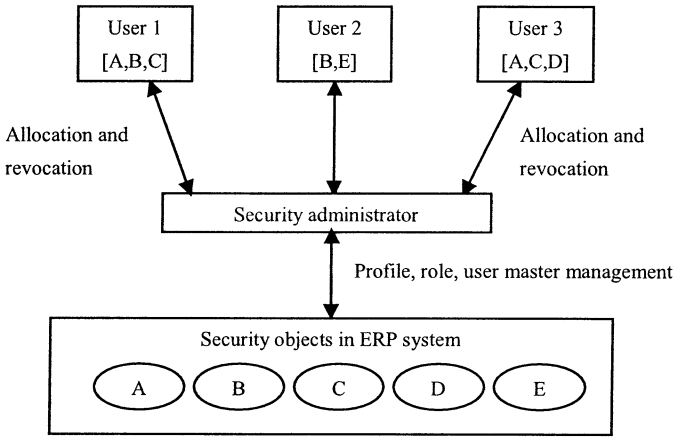

Figure 3. Centralized security within an ERP environment

A simple solution to include the concept of information ownership for purposes of the ERPSEC framework is to define individual information owners. From the preceding discussion of information ownership it should be clear that information ownership implies a form of decentralization. The decentralization is such that individual stakeholders become responsible for groups of users within the organization.

5.2 Information owners

The information owner is an important part in the ERPSEC framework. Not only does the information owner know what access is required in order for the department or organizational unit to function, but also has an in-depth

knowledge of the jobs and tasks performed within that department. Hence, the translation of a particular task to its security and access restriction requirements within the ERP system is far simpler to determine. A further advantage is that the requirements do not have to be communicated to a third party, such as the central security administrator.

The information owner thus plays the role of a decentralized security administrator, albeit only for the area of the business the information owner belongs to. For this to be possible, the ERPSEC framework must cater for some additional requirements. From the preceding discussion, it was made clear that the translation of access restrictions and security requirements was a major factor that inhibited and decreased security within a traditional ERP system. The requirement of an information owner within the ERPSEC framework cancels this complication, but does not fully solve all problems. To be useful, the ERPSEC framework must provide some way of allowing security objects to be configured without the need for the detailed technical understanding of the system that security administrators generally have.

5.3 Dealing with technical complexity

The previous section has dealt briefly with the requirement the ERPSEC framework has for dedicated information owners in the organization. In order to permit these information owners to be able to create and maintain their own security objects, a high level of abstraction is required. Abstraction of the technical details regarding the configuration and maintenance of security is an absolute necessity when placing such responsibilities with the information owners.

Abstraction can be achieved in the proposed ERPSEC framework. Instead of relying on a central security administrator who must know all technical details to create and maintain security objects, ERPSEC introduces an additional layer in the security subsystem that allows security objects to be configured and maintained in a very simple yet powerful fashion. It should be clear that retrofitting existing ERP software packages with such an additional software layer may not be practical. However, future versions of current ERP software packages could easily incorporate such an abstraction layer to promote and support the concept of information ownership. Figure 4 below depicts the additional abstraction layer. The abstraction layer can also be considered a simple interface layer. The layer has the responsibility of translating the input of the non-technical information owner into technical object names and function codes. In effect, the interface translates technically detailed security objects and presents them to the information

owner in a very simplistic fashion. Ideally, the interface for the information owner should be a point-and-click environment in which allocation of security objects and settings can be made quickly and easily. A technical implementation of such an interface is beyond the scope of this paper. A description may be found in the full study relating to ERPSEC.

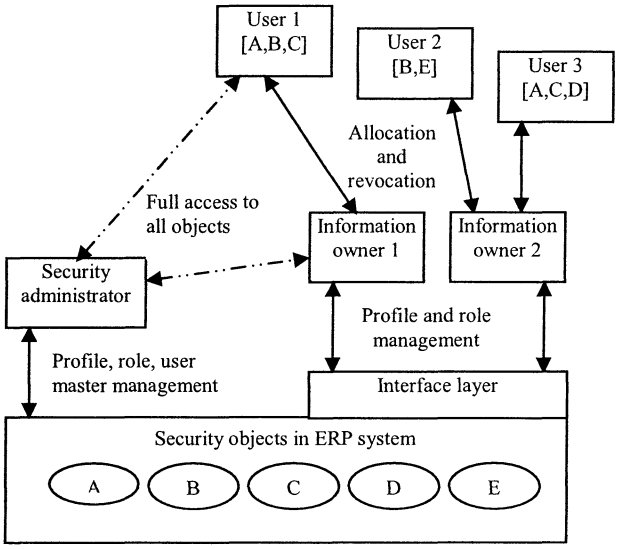

Figure 4. Decentralized security within an ERP environment

Though the inclusion of an interface in the ERPSEC framework allows the concept of information ownership to be supported more fully, additional requirements still exist. Most importantly, ERPSEC must validate and handle information owners in a slightly different way to ordinary users of the system. In addition, the interface for the information owner should be restrictive enough to ensure that only appropriate security objects for that information area can be configured and maintained.

5.4 Validating information owners

As mentioned in the section above, validation of information owners is important to ensure that access restrictions can be defined. The ERPSEC framework does not require too many special mechanisms to validate information owners. An information owner within the ERPSEC framework is simply another user of the system. The crucial difference is that an information owner has some additional access rights that an ordinary user would not have.

ERPSEC requires information owners to have special security settings added to their user master record that identifies them as information owners. In addition, the information they are responsible for is also identified, as well as the users they should be permitted to administer. This solves two problems, namely the ability of information owners to be able to configure and maintain security objects within the system, and the restriction of the information owner to being able to operate only within a set information area of the organization.

Technically, ERPSEC requires information areas to be defined. In the simplest sense, an information area is a portion of the ERP system that corresponds to an area of the real-world organization. Examples of information areas are manufacturing, shipping and financials. Depending on the size of the organization, more information areas may exist; as an example, an organization with a global presence may have manufacturing capacity in various countries. It is unlikely that a single individual would be able to perform the task of information owner for the all manufacturing divisions worldwide. Hence, information areas may be created for each manufacturing location. Regardless what the information areas are deemed to be, ERPSEC associates the information areas with relevant users in that location or information area. The assigned information owner is the only individual other than the security administrator who is able to maintain and configure access restrictions for those users. The assignment of users to information areas and the creation of information areas themselves are tasks that can be completed by the security administrator. This task is not technically complex and does not involve detailed knowledge of business

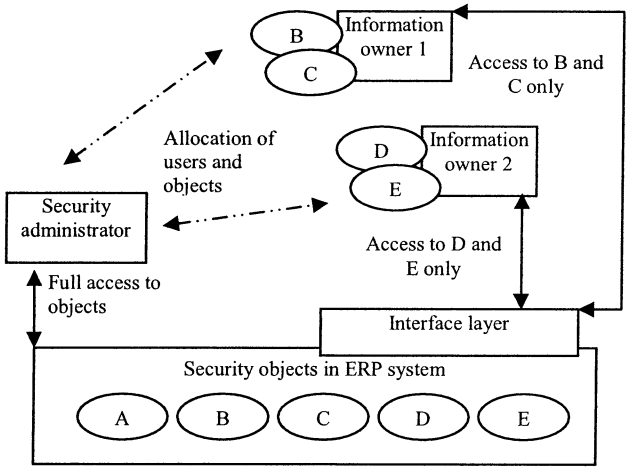

Figure 5. ERPSEC compartmentalizes users and information areas

processes. This information can be gleaned from the organization's structure.

Figure 5 attempts to represent the restricted access of the information owners. Note that the interface layer is responsible for ensure that the access to all security objects takes place in a compartmentalized fashion. In technical terms, the security subsystem may contain a number of tables that list all information owners with their associated information areas. A second table contains the information owner and allocated system users. The ERPSEC framework performs numerous checks whenever access to a security object is required by any user. In the case of an information user, ERPSEC verifies that the user in question is identified as an information owner. Once this check has successfully been completed, ERPSEC queries the table containing the information areas for that information owner. Access is not permitted to any object that is not within the list permitted for that user. At a higher level, ERPSEC ensures that no information area is accessible by more than one information owner. This ensures concurrency control and integrity.

5.5 Maintaining integrity

The concept of integrity has been briefly mentioned above. Integrity is a very important concept that has to be adhered to. As has been discussed, ERPSEC changes the traditional centralized security model to a decentralized one. In this decentralized approach, more than one user is able to modify security settings for ordinary system users. In effect, ERPSEC proposes multiple security administrators with one significant difference: each information owner is restricted to a very narrow set of users and security objects that may be configured and maintained.

Integrity is maintained within the ERPSEC framework by controlling the allocation of information areas to information owners. As discussed previously, it is very important that each information area be allocated to a single information owner. The structure of ERPSEC ensures this by providing a list of available information areas that have been configured, and by permitting the allocation of each one to only a single information area. If required, a single physical user could be the information owner for more than one information area. This is a matter of preference and does not compromise the operation of ERPSEC. However, the combination of information areas for a single information owner reverts back to the traditional centralized approach with most of its inherent problems. For this reason, a single information owner for each information area is recommended.

The allocation of information areas to individual information areas is performed by a security administrator. Once this has been completed, security objects within the ERP system that belong to that information area have to be allocated to that information area. This is not a trivial exercise and must be performed by the information owners.

5.6 Extending information areas to include security objects

Figure 3 briefly introduced the notion of allocating security objects to individual information owners. To facilitate the transfer of functionality to ordinary users within the system, the information owner must be able to allocate physical security objects to users. The concept of allocating such security objects is similar to the allocation of information areas to information owners. In the case of security objects, the organization determines which functional blocks within the ERP system belong to which information area. As has been determined in the study of existing ERP systems, a large number of function or menu codes are present in an ERP system. The ERPSEC framework assumes that all functions within an ERP system can be represented by function codes. In technical terms, a function code can be a menu item, shortcut or text entry that is linked to a particular program or functionality within the software system. Once the user selects a menu item or enters the function code, that program or functionality is executed. In this way, the user is able to perform tasks such as the entry of an order or the creation of an invoice.

To provide information owners with the ability to distribute the required functionality to the users within their information area, the information owner must be able to allocate function codes to relevant users in the system. It is logical to assume that function codes can be grouped to form segments of basic functionality within an ERP system. This fact is supported by the study of existing ERP systems: groups of function codes represent functionality within a particular module of the ERP system. In this way, all material management functions are associated with a particular group of function codes, for example. Hence, the allocation of function codes to individual information areas and hence to information owners is not an impossible task.

In the ERPSEC framework, the information owners determine which function codes belong to their information area. There may be cases where the ownership of a particular function code cannot be determined precisely. In this case, the organization should allocate that function code to the most

likely information area. The result of this exercise within the ERPSEC framework is an additional data structure within the security subsystem that contains all function codes that have been allocated to a particular information owner. By employing the integrity and concurrency rules discussed earlier, only one information owner is able to allocate any particular function code. This has important consequences for the tightening and enhancing of security within the ERP system.

5.7 Enhancing security through ERPSEC

The operation of the ERPSEC framework has been briefly discussed in the above sections. The allocation of information areas to information owners, and the allocation of particular function codes to these information areas enhances security automatically. The reason for this is the fact that only the stakeholders or owners of the information are permitted to allocate access to it. This has important consequences for the overall security of the ERP system: as the information owner is responsible for the performance of his business unit, restricting access to only those users in the organization that require access is sensible. In contrast to the traditional centralized approach, the approach of allocating access at the information area level adds an extra layer of trust and security. As the information owner is aware of the users to whom certain function codes are being allocated, the allocation of the function codes takes place in a more secure environment. In contrast, a centralized security administrator is not always fully aware of all users within the organization and cannot determine why a certain function code may have to be allocated.

5.8 Support for segregation of duties

The fact that the information ownership approach increases support for segregation of duties has been mentioned briefly. Segregation of duties is seen to be one of the most important aspects to prevent fraud and heighten security[7].It is important to note that this requirement is becoming a legislative requirement for many organizations to adhere to. Legislation at present mandates accountability.

The ERPSEC framework assists by providing a non-technical platform for stakeholders to configure and define what security is required within their area. This in turn requires the stakeholder or information owner to accept the responsibility for the configuration and content of the resulting security object. Though it has to be stated that the ERPSEC framework

cannot guarantee increased security, the adherence to the information ownership principles provides a platform from which stricter security measures can be put in place.

6. CONCLUSION

The paper has briefly introduced the reader to the problems traditionally faced when implementing security within an ERP software environment. The most pressing problems were identified and discussed. To provide a solution to these problems, the paper introduced the concept of information ownership as a means to increasing and enhancing the security subsystem of an ERP software package. The proposed ERPSEC framework was introduced. The requirements of the ERPSEC framework to support the concept of information ownership were highlighted. It was briefly shown how ERPSEC assists in supporting the following:

- a reduction in complexity of the security configuration;
- the ability to increase responsibility and accountability within the organization;
- a faster implementation time by providing decentralized access to security objects;
- to improve the quality of the security configuration as a whole;

REFERENCES

1. M. Hertenberger, Prof. S.H. von Solms, *A framework for ERP security*, PhD study in progress, 2005
2. The Information Security Glossary, http://www.yourwindow.to/information-security
3. Internal controls, Committee of Sponsoring Organizations of the Treadway Commission (COSO), http://audit.ucr.edu/internal_controls.htm
4. Joseph R. Dervaes, *Internal Fraud and Controls*, Washington Finance Officer's Association, 48th Annual Conference, 19 September 2004
5. K. Vuppula. *BW security approaches*, http://www.intelligenterp.com/feature/2002/12/0212feat1_1.shtml, 2002
6. P. Manchester, Financial Times, 12 November 2003
7. Elizabeth M. Ready, Emerging Fraud Trends, State of Vermont, 2003
8. M. Hertenberger, Prof. S.H. von Solms, *A case for information ownership in ERP systems*, Kluwer Publishing, 2004