A SECURITY FRAMEWORK FOR AN ERP SYSTEM

Marnewick, C[1] and Labuschagne, L[2]

Academy for Information Technology, University of Johannesburg

University of Johannesburg, PO Box 524, Auckland Park, 2006, South Africa.

[1]E-mail: cmarnewick@datacentrix.co.za

Tel.: (011) 461-2000

Fax: (011) 461-2050

[2]E-mail: LL@rau.ac.za

Tel.: (011) 489-3335

Fax: (011) 489-2138

ABSTRACT

This article provides an information security framework that can become an integrated process within an ERP system to support corporate governance.

A generic information security framework serves as a starting point to develop a specific ERP security framework because most security managers are familiar with the framework. The generic information security framework consists of three components: people, policy and technology. These three components are extended and enhanced to better fit ERP systems. The ERP security framework is applied to an ERP model to illustrate how the three components can be incorporated into it.

The ERP security framework guides management in integrating information security into the ERP system. This security framework is both product and vendor independent.

The ERP security framework ensures that information security forms an integral part of the design, implementation and operation of an ERP system, so the information provided by the system is reliable.

KEYWORDS

Information security, Enterprise resource planning, ERP model, ERP security framework.

A SECURITY FRAMEWORK FOR AN ERP SYSTEM

1 INTRODUCTION

Information is one of the most important assets of any organisation, so it should be appropriately protected[i]. Information security combines systems, operations and internal controls to ensure the integrity and confidentiality of data and operation procedures in an organisation. Availability of the information is also important to the organisation[ii]. If the integrity of the information is above board and the information is confidential, but it is not available to authorised users, it is of no use.

Enterprise resource planning (ERP) system security must be governed by the same principles as conventional information security. An ERP system controls all the business related information of an organisation as well as information relating to customers and suppliers. It is necessary to protect this information from the opposition as well as to ensure that the information within the ERP system conforms to auditing standards such as Sarbanes-Oxley[iii]. The security and protection of the information within the ERP system is therefore crucial to the existence of the organisation. The purpose of this article is to provide an ERP security framework that will enable an organisation to include security as an integral part of an ERP system and not as an afterthought.

According to Dhillon[iv], information security has traditionally been an afterthought, even within ERP systems. Because of businesses' increased dependence on information, security is increasingly being considered proactively[v]. While designing, developing and implementing systems, there are enthusiastic discussions of the relevance of certain controls and the hindrance of such controls to the conduct of business and the efficiency of certain security tools. Many ERP systems ultimately do not conform to corporate and IT governance requirements.

The process used to provide a solution to the above problem is as follows:

1) A generic security framework is analysed to determine the aspects that are applicable to ERP systems.

2) The shortcomings of this security framework are identified in the context of an ERP system.

3) An ERP security framework is developed that conforms to corporate and IT governance requirements.

The first section of the article focuses on the generic security framework and the three components that form part of this framework. The components are discussed with regard to how they relate to each other, IT and corporate governance. In the second section of the article, the security framework is mapped to an ERP model. This is done to determine the shortfalls of the security framework. The third and last section of the article provides an ERP security framework that can be used to ensure that security is integral to an ERP system and not just an add-on.

2 THE GENERIC SECURITY FRAMEWORK

Figure 1 below shows a generic information security framework. The framework is divided into three components: people, technology and policy, which are interdependent[vi]. Any change to one of these components will affect the other two.

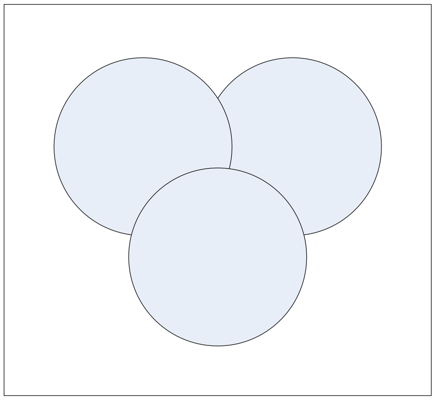

Figure 1. Security framework

2.1 People Component

The people component is divided into two groups. The first group comprises people who put security in place and support the process. A few key roles include senior management, security administrators, IT administrators and auditors. The second group is the actual users of the systems. They must be aware of the reasons why security is in place as well as the consequences if they breach the security.

According to Martins[vii], the people component can be divided into nine aspects:

- Policy and procedures – The information security policy dictates employee behaviour and states what is expected of employees, which in time becomes part of the information security culture.
- Benchmarking – Guidelines on information security processes can be promoted in the organisation through benchmarking. This will enable the organisation to compare itself to other similar organisations and to international standards.
- Risk analysis – Through risk analysis, threats to organisational assets and security measures can be identified to develop the information security policy.
- Budget – A financial plan is necessary to implement the issues concerning an information security culture. For instance, employees need training, technical controls need to be implemented and teams need to be enabled to assess the security of networks.
- Management – Management is responsible for information security. Management develops an organisation’s vision and strategy, which are required to protect information assets and which are implemented in the organisation.
- Trust – Information security is important in instilling trust in an IT environment. It is easier to implement new procedures and guide employees through changes of behaviour regarding information security if management and employees trust one another.
- Awareness – Since the effectiveness of information security controls depends on the people who are implementing and using them, employees need to be enabled through awareness and training to behave according to what is expected of them to ensure the security of information assets.
- Ethical conduct – Good practices form part of the culture established throughout the organisation. Employees need to incorporate ethical conduct or behaviour relating to information security as part of their everyday life in the organisation.

- Change – Technology changes involve challenges to ensure secure communication and secure use. These changes need to be managed and accepted positively in the organisation. Implementing an information security policy could also mean that employees need to change their working practices to ensure the effective implementation of information security.

These nine aspects form the basis of the people component and are comprehensive enough to address all people related issues within an ERP system.

2.2 Policy Component

Information security is a key aspect of information technology governance[viii]. Various methods are available to an organisation to make information security part of corporate governance such as international standards that include CobiT, ITIL and ISO 17799.

Figure 2 illustrates the breakdown of the policy component as guided by corporate governance requirements into the three levels of IT governance, IT management and information security management, supported by CobiT, ITIL and ISO 17799, respectively.

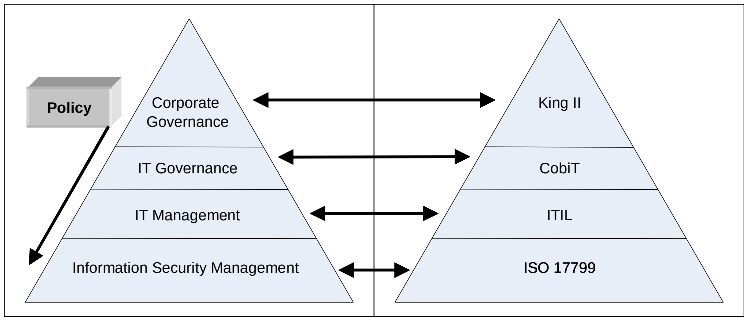

Figure 2. Policy component

- King II – The King Report on Corporate Governance for South Africa 2002[ix] is a corporate governance recommendation report published by the King Committee. It addresses the management accountability and responsibilities of organisations towards their shareholders. The King II Report covers diverse topics such as boards and directors, risk management, internal audit, integrated sustainability reporting, accounting and auditing, and compliance and enforcement.

- CobiT – CobiT is an IT governance control framework and maturity model that ensures that IT resources are aligned with the organisational vision and strategies. CobiT does not, however, include control guidelines or practices which are the next level of detail nor the process steps and tasks because it is a control framework rather than a process framework[x]. CobiT focuses on what organisations need to do, not how to do it.

- ITIL – ITIL describes and defines key processes such as problem, change and configuration management. It also provides a framework for managing the processes. By forcing a focus toward aligning and defining a specific process, the IT department can identify opportunities for improvements in efficiency which can result in the improved ability to better manage service delivery and support.

- ISO 17799 – ISO 17799 is a *de facto* international standard that provides guidelines and recommendations for security management[xi]. ISO 17799 is divided into 10 modules that are used to implement security.

King II states what must be done by the organisation, CobiT states what must be done by IT, ITIL states how it must be done and ISO 17799 focuses specifically on the detail of implementing and managing information security. These four frameworks can be used to address all policy related issues within an ERP system.

2.3 Technology Component

The technology component of information security can be broken down into five pillars[xii].

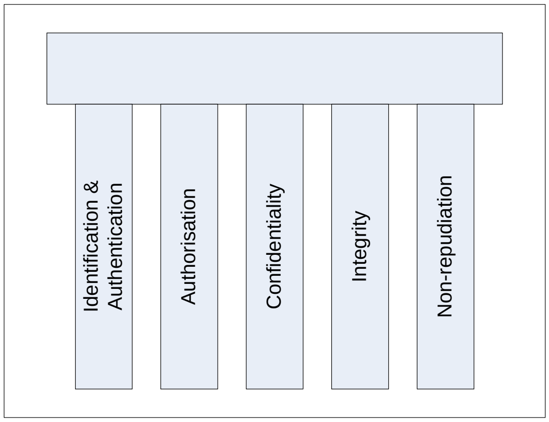

Figure 3. Five pillars of information security

- Identification and authentication – The first responsibility of information security within an ERP system is to ensure that the ERP system is only accessed by legitimate, authorised users[xiii].
- Authorisation – One of the most critical aspects to consider within ERP security is to restrict the access rights and actions of the users within the ERP system[xiv]. The access rights of a user are controlled by the authority assigned to the user ID.
- Confidentiality – Protecting the confidentiality of data implies the assurance that only authorised people are able to view specific data sets[xv].
- Integrity – Integrity means that only authorised users can modify the data of the ERP system. Modification refers to the update, deletion and creating of data within the ERP system.
- Non-repudiation – The organisation ensures that a transaction that is done is legitimate and can be proven as such in case of a query or dispute. Organisations can make use of digital signatures or public key encryption to enforce valid and legal transactions[xvi].

The five pillars of Von Solms and Eloff do not address the following two specific issues within an ERP system:

- Availability – ERP systems need to remain available 24/7 for business continuity. Organisations must be prepared to restore the system and data and reduce the need for system downtime, maintenance and management. Particular problems include scheduling background jobs, distributing and balancing workloads, monitoring the performance of ERP applications, databases, operating systems and networks, generating alerts and customer-tailored performance thresholds and analysing exceptions.
- Auditing – System design auditing should be performed as early in an ERP implementation as possible. When resources are stretched and deadlines short, audit issues can easily be overlooked. Unfortunately, this can lead to an insecure system

with poorly designed controls. Once the system is deployed, auditing requires a risk-based systems review supported by detailed checklists and practical experience in designing controls. This sort of review will not only uncover weaknesses but also support a redesign, if necessary, to improve security levels.

The five pillars can be extended to seven pillars to include the issues of availability and the auditing of the system. Figure 4 below illustrates the seven security pillars in relation to an ERP system.

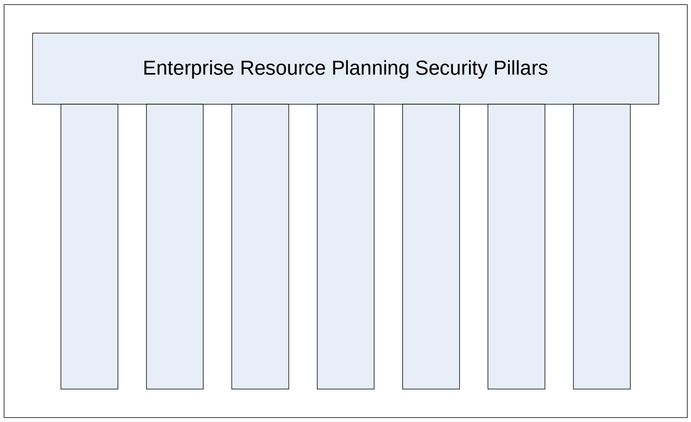
Enterprise Resource Planning Security Pillars
Identification & Authentication
Authorisation
Confidentiality
Integrity

Figure 4. Seven pillars of ERP security

The next section links the above ERP security framework to a generic ERP.

3 INTEGRATING INFORMATION SECURITY WITHIN AN ERP SYSTEM

It is important to understand how an ERP system is structured. This will ensure that the adapted security framework is mapped in a proper and consistent manner onto the ERP model. The ERP model consists of four components that are implemented through a methodology and is illustrated in figure 5[xvii].

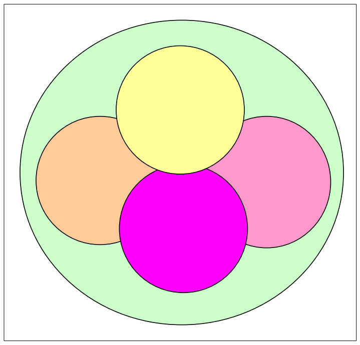

Figure 5. ERP model

- The software component – The software component of the ERP model is the most visible to the users and is often seen as the ERP product. This includes modules such as General Ledger, Supply Chain Management and Customer Relationship Management.
- Process flow – The second component is the process flow within an ERP system. Process flow deals with the way in which the information flows among the different

modules within an ERP system. This forms a very important part of understanding ERP systems.

- Customer mindset – The third component addresses the resistance to change that could kill an ERP project. A proposed ERP system may hold great promise, but often fails to consider how the users are likely to view this so-called improvement[xviii].
- Change management – Change management plays a major role in the successful implementation of an ERP system and is the fourth component in the ERP model. Change needs to be managed at all levels of the organisation.
- ERP methodology – Methodology refers to a systematic approach to implement an ERP system that will ensure the proper integration of the four components.

The alignment of the ERP model and the security framework will enable an organisation to implement an ERP system that will conform to international security standards. It will also ensure that once security is implemented, it will be an ongoing function within the ERP system and will not be neglected.

The next section focuses on mapping the ERP security framework onto the ERP model components.

3.1 Software Component of the ERP model

3.1.1 Policy Component of the Security Framework

The policy component focuses on the policies and procedures that must be in place to manage and enforce security. Although the software component only deals with the software modules within an ERP system, CobiT and ITIL guide how the software is to be implemented. CobiT dictates to the Supplier Relationship Management (SRM) module how security must be managed with a customer. ISO 17799 affects the software module as follows:

- Security policy – A policy needs to be defined on how the ERP system will function and will include all relevant information.
- Asset classification and control – Although an ERP system is perceived as software, it also includes hardware and networking infrastructure. All these assets need to be classified and controlled. It also includes intellectual capital such as customisation of the ERP system.
- Physical and environmental security – The physical ERP servers need to be hosted in a secure environment. Access to the system and premises must be controlled.
- Communications and operations – Operational procedures must be in place, e.g. the frequency of backups and the protection of the ERP system against unlawful access.
- Information access control – Access to the ERP system and even some modules and functions must be controlled.
- System development and maintenance – This module will define the security within each software module and how the data will be encrypted.
- Business continuity – The ERP system must be available for transacting and business continuity plans must be defined and tested to ensure that the ERP system can function in the event of a disaster.
- Compliance – The ERP system must comply with standards and legislation.

Almost all the aspects of ISO 17799 must be taken into consideration except personnel security. The software component does not dictate who gets employed by the organisation.

3.1.2 People Component of the Security Framework

Although people are going to use the ERP system and will be affected by the security surrounding it, the software component is not affected that much by the people component. The issues influencing the people component are mostly soft issues such as trust and ethical conduct. The following are some of the hard issues involved:

- Budget – The organisation must spend money on training to ensure that the users of the ERP system understand how it works, the effect of security on their work and the issues surrounding ERP security.
- Management – The users of the ERP system will only enforce security if it is encouraged by management.
- Change – The implementation of the ERP system will have an effect on the users since it will bring change into their lives. The organisation must know how to deal with this change.

3.1.3 Technology Component of the Security Framework

The seven pillars can be applied to the software component. The identification and authentication pillar determines who has access to the software components, while the authorisation pillar determines the type of access and the modules within the software component to which access is granted. The information supplied to the user by the software modules must be integrated as well as confidential. This means that information must flow from one side of the ERP system - such as the SRM module - right through to the printing of the invoice without any user intervention. It also means that special deals loaded by the supplier, for example, are not visible to outsiders and thus remain confidential.

Non-repudiation plays an important role, especially in the SRM and Supply Chain Management (SCM) modules. All the software modules must always be available, especially for the interaction and flow of information between the different modules, as well as for customer and supplier convenience. All aspects must be auditable and it is very important that the software comply with auditing standards.

The second component of the ERP model is the customer mindset component. This deals with how the users perceive the ERP system: typically as either a threat or a mechanism to assist them in their work.

3.2 Customer Mindset Component of the ERP Model

3.2.1 Policy Component of the Security Framework

The policies and standards of the organisation will have an effect on how users perceive the ERP system. The users should not perceive security as a burden, but rather as a necessity to ensure the integrity and confidentiality of information. A few modules of ISO 17799 play a role in the customer mindset component. One is the security organisation that determines the roles and responsibilities within the organisation. Another is the personnel security module that determines who gets employed.

3.2.2 People Component of the Security Framework

The people component and the customer mindset both deal with the way the user interacts with the ERP system. These two components influence each other and are interdependent. A comparison of the two follows:

- Policy and procedures – The policy and procedures instilled by the organisation will influence the employees of the organisation. The way they work will be governed by the policies and procedures.

- Benchmarking – The organisation can use benchmarking to compare itself to other organisations. This comparison will enable the organisation to determine where it is lacking in security and how it measures as an organisation in terms of the rest of the industry.
- Risk analysis – The employees of the organisation must be involved in the day-to-day risk analysis. This will ensure that security policies are up to date and will make users aware of any security breaches.
- Budget – The organisation must train the users in the impact of security on their lives and the way they work. The implementation of security affects the way users work and interact with the ERP system, so the budget should allow for education in this regard.
- Management – The management of the organisation should make security a way of life by enforcing and implementing it themselves.
- Trust – The users of the ERP system must be trusted by the organisation to interact with the ERP system and to enforce the security rules and regulations.
- Awareness – The users must be aware of how confidentiality, integrity and availability are impacted if they do not abide by security policies.
- Ethical conduct – The integrity of the ERP system will be affected by the ethical code and conduct instilled by the organisation. For example, users must be aware that they cannot work on the information from home.

These aspects of the people component will influence the way users interact with the security surrounding the ERP system. The next component is the technology component and the impact it has on the users' mindset.

3.2.3 Technology Component of the Security Framework

Identification and authentication play a vital role in the customer mindset component. If the users do not abide by the rules of the technology component, the security will have no effect. For example, the users must understand what the consequences are if they pass their username and password on to someone else. This also affects the authorisation pillar and the consequences can be far-reaching. The ERP system must also be audited to ensure that the users comply with the policies and procedures of the organisation.

The ERP system cannot be implemented within an organisation if change does not take place. The following section will discuss the change management component of the ERP model.

3.3 Change Management Component of the ERP System

Change management not only deals with the changes that the ERP system enforces on the organisation, but also with system changes once the system is implemented and business process changes.

3.3.1 Policy Component of the Security Framework

Changes to the ERP system cannot be made without considering the policies and standards of the organisation. The deployment of new versions of software will be managed by ITIL, which will ensure a smooth upgrade. During the lifetime of an ERP system, the business process will change, having an impact on security. Certain aspects of security might change and this should take CobiT into consideration. ISO 17799 plays a role in the implementation of the ERP system and will manage the security aspects during the changes that are instilled by the system. Changes to the security policies will be addressed by the security policy component and the new roles and responsibilities will be addressed by the security organisation component.

3.3.2 People Component of the Security Framework

Certain aspects of the people component have an impact on the change component of the ERP model. Policies and procedures will change during the implementation of an ERP system and awareness regarding the system will change to accommodate new ways of doing things. The management of the organisation must also ensure that the users are aware of these changes to the policies and the necessary education must be provided.

3.3.3 Technology Component of the Security Framework

System and business process changes have an effect on the following four pillars:

- Confidentiality – The system or business process changes must not affect confidentiality. The information must still only be accessible to authorised users.
- Integrity – The information must not be compromised during changes and must still be intact after the changes to the ERP system.
- Availability – The ERP system must be available for transacting, which makes it difficult for system administrators to implement changes. Careful planning is needed to minimise the effect of downtime.
- Auditing – After system or business process changes, the ERP system must still pass all audits.

3.4 Process Flow Component of the ERP System

The process flow component of the ERP system deals with the way information flows between the different software modules.

3.4.1 Policy Component of the Security Framework

ISO 17799 will affect the way the different components interact with each other. It will also determine the level of information that flows between the different software components.

- Asset classification and control – This component will determine the protection between the different modules and will ensure that the different software modules do not influence each other in a negative way.
- Communications and operations – During the flow of information between the different modules, this component will provide the guidelines to ensure that the information is intact and not tampered with.

An aspect that must be considered during the process flow is the access control and the system maintenance of the ERP system.

3.4.2 People Component of the Security Framework

The people component does not play a significant role because all information flow happens in the background of the ERP system. The only aspect that must be taken into consideration is that the users must be aware of how the system works and the impact their actions might have later on.

3.4.3 Technology Component of the Security Framework

The flow of information between the different software components must be controlled by the following pillars:

- Confidentiality – Information should remain confidential as no user directly interacts with the information as it flows from one module to another. The less user interaction, the better the confidentiality of the information.

- Integrity – The information that flows from one software module or even within a module must be the same when it reaches its destination. The information must not be altered during the process flow.
- Availability – The ERP system must be available to ensure that information can flow between the different modules. If some modules are not available, it can lead to corrupt data or the recapture of data.

The next section addresses the integration of information security into the ERP methodology.

3.5 Methodology Component of the ERP System

3.5.1 Policy Component of the Security Framework

It is the responsibility of the programme manager to ensure that CobiT and ITIL are adhered to during and after the implementation of the ERP system. This adherence to international standards and guidelines ensures that customers are content to deal with the organisation because they know that the organisation and systems are adhering to the standards. The policies of the organisation take precedence over the policies of the ERP system, that is, the ERP system must be adapted to accommodate the policies of organisation and not the other way around.

3.5.2 People Component of the Security Framework

The people component will determine who within the organisation is responsible for the security aspects of the ERP system. These responsibilities will be derived from the overall people component of the security framework and will be incorporated into the ERP system security. If a person's responsibility is to implement password policies for the organisation, then that same person must be responsible for the password policies of the ERP system. The programme manager responsible for the implementation of the ERP system must ensure that all the relevant people are involved and incorporated into the project team. This will facilitate security being implemented from the beginning of the implementation and not just as an afterthought[xix].

3.5.3 Technology Component of the Security Framework

The seven pillars of ERP security must be incorporated in the ERP system. These pillars form the foundation of ERP security and determine what users and customers are allowed to do within the system. These pillars also ensure that the confidentiality, integrity and availability of the information are above suspicion. The programme manager must ensure that these pillars are addressed during the design of the ERP system and that they form part of the overall project plan. The seven pillars must be part of the design and process flows of information between the different software modules.

The above sections mapped the ERP model to the ERP security framework to determine how it can be used to implement and manage security within an ERP system.

Table 1 provides a summary of this mapping process.

Table 1. Mapping of ERP model to security framework

	Policy Component	**People Component**	**Technology Component**
Software Component	• CobiT • ITIL • ISO 17799 o Security policy o Asset classification & control o Physical & environmental security o Communications & operations o Information access control o System development & maintenance	• Budget • Management • Change	• Identification & authentication • Authorisation • Confidentiality • Integrity • Non-repudiation • Availability • Auditing

	o Business continuity o Compliance		
Customer Mindset	• CobiT • ITIL • ISO 17799 o Security organisation o Personnel security	• Policy & procedures • Benchmarking • Risk analysis • Budget • Management • Trust • Awareness • Ethical conduct • Change	• Identification & authentication • Authorisation • Auditing of the people
Change Management	• CobiT • ITIL • ISO 17799 o Security policy o Security organisation o Communications & operations o Information access control o System development & maintenance	• Policy & procedures • Budget • Management • Awareness • Change	• Confidentiality • Integrity • Availability • Auditing
Process Flow	• ISO 17799 o Asset classification & control o Communications & operations o Information access control o System development & maintenance o Compliance	• Awareness	• Integrity • Availability • Confidentiality
Methodology	• ITIL • ISO 17799 o Personnel security o Communications & operations	• Policy & procedures • Risk analysis • Management • Awareness • Change	• Identification & authentication • Authorisation • Confidentiality • Integrity • Non-repudiation • Availability • Auditing

It is clear from table 1 above that an ERP system cannot be implemented or managed without taking the security framework into consideration. The security framework provides the project manager and system administrator with guidelines, policies and standards to implement and manage the ERP system.

The advantage of the ERP security framework is that it provides an organisation with a framework to ensure that security forms an integral part of the ERP system right from the start. The main disadvantage is that organisations that use any other standard must build their specific standards into the framework as the framework does not cater for them.

4 CONCLUSION

The article focuses on security within an ERP system. It provides a security framework that can be used to address all relevant security aspects within an organisation and to ensure that it forms an integral part of an ERP system. The security framework is mapped onto the ERP model to provide the organisation with a clear understanding of which security issues must be addressed within which ERP component.

It is clear given the above that security must form an integral part of an ERP system and that it will be difficult to add it on once the ERP system is already implemented. If security is added after implementation, the ERP system will have difficulty adhering to IT and corporate governance requirements. An ERP system is also an integral part of the organisation and cannot be treated as an independent system without taking the organisation's policies and procedures into consideration.

This article provides an organisation with a framework to ensure that all aspects surrounding IT and corporate security are built into an ERP system. The organisation can quickly determine where the ERP system is at fault regarding security and this fault can be rectified before it causes major problems.

Another aspect that must not be forgotten is that ERP security is an ongoing process. The official process starts with the pre-implementation phase where security is designed and built into the ERP system. The official process stops with the implementation of the ERP system. However, this is not where everyone's responsibilities end. As the system is kept up to date and new technologies emerge, security must be addressed as an everyday event to keep the information intact.

5 REFERENCES

[i] Hong, K-S. et al. 2003. An integrated system theory of information security management. Information Management & Computer Security. Volume 11. Number 5. pp 243 – 248.

[ii] Scott, D. & Krischer, J. 2002. Real-time enterprise: business continuity and availability. Gartner. 24 September.

[iii] Blosch, M. & Hunter, R. 2004. Sarbanes-Oxley: an external look at internal controls. Gartner. August.

[iv] Dhillon, G. 2004. Guest Editorial: the challenge of managing information security. International Journal of Information Management. Volume 24. pp 3 – 4.

[v] Von Solms, R. & Von Solms, B. 2004. From policies to culture. Computers & Security. Volume 23. pp 275 – 279.

[vi] Pal, R. & Thakker, D. Defining an enterprise-wide security framework. http://www.networkmagazineindia.com/200211/guest.shtml

[vii] Martins, A. 2003. Information security culture. Masters thesis. Johannesburg: Rand Afrikaans University.

[viii] CobiT Security Baseline. IT Governance Institute. http://www.itgi.org

[ix] King Committee on Corporate Governance. 2002. King Report on Corporate Governance for South Africa. Institute of Directors. ISBN 0-620-28851-5.

[x] Mingay, S. & Bittinger, S. 2002. Combine CobiT and ITIL for powerful IT governance. Gartner. 10 June.

[xi] Hoekstra, A. & Conradie, N. 2002. PriceWaterhouseCoopers LLP. CobiT, ITIL and ISO 17799: How to use them in conjunction.

[xii] Von Solms, S.H. & Eloff, J.H.P. 1997. Information security. Department of Computer Science, Rand Afrikaans University. Johannesburg.

[xiii] Yang, Y., Wang, S., Bao, F., Wang, J. & Deng, R.H. 2004. New efficient user identification and key distribution scheme providing enhanced security. Computers & Security. Volume 23. pp 697 – 704.

[xiv] McLean, N. 2000. Matching people and information resources: authentication, authorisation and access management and experiences at Macquarie University, Sydney. Electronic Library & Information Systems. Volume 34. Number 3. pp 239 – 255.

[xv] McMillen, D. 2004. Privacy, confidentiality and data sharing: issues and distinctions. Government Information Quarterly. Volume 21. pp 359 – 382.

[xvi] Bell, T., Thimbleby, H., Fellows, M., Witten, I., Koblitz, N. & Powell, M. 2003. Explaining cryptographic systems. Computers & Education. Volume 40. pp 199 – 215.

[xvii] Marnewick, C. & Labuschagne, L. 2005. A Conceptual Model for Enterprise Resource Planning (ERP). Information Management and Computer Security. Volume 13. Number 2.

[xviii] Maurer, R. 2002. Plan for the human part of ERP. Workforce Online. September.

[xix] Posthumus, S. & Von Solms, R. 2004. A framework for the governance of information security. Computers & Security. Volume 23. pp 638 – 646.

.

.