AN EVALUATION OF SECURITY FEATURES OF SAP R/3

by

DANIEL CHRISTIAAN MOOLMAN

Short Dissertation
submitted in partial fulfillment for the degree

MASTER OF COMMERCE

in

COMPUTER AUDITING

in the
Faculty of Economic and Management Sciences
at the
Rand Afrikaans University

STUDY LEADER: PROF. A. DU TOIT

Johannesburg
November 1997

ACKNOWLEDGEMENTS

The opinions expressed and conclusions made in this dissertation are those of the author and should not be seen as the opinions and conclusions of authors referred to as part of the literature survey conducted.

A word of special appreciation to the following:

Prof. du Toit and Prof. Boshoff, for their assistance and support during the two years of study.

My colleagues at work.

Friends and family - for their understanding and support, especially my brother Kobus.

Study group, Jannie, Elmarie, Markus and Louis for the teamwork and friendship during the past two years.

A special word of thanks to Delene Slabbert for editing and formatting.

To almighty God, all the glory.

INDEX

CHAPTER		PAGE
	Opsomming in Afrikaans	iii
	Synopsis	xi
1.	Introduction	2
2.	Security and Audit	17
3.	Security Features of SAP R/3	34
4.	Security Audit Program for SAP R/3	69
5.	Conclusion	84
	Bibliography	88

OPSOMMING IN AFRIKAANS

EVALUASIE VAN DIE SEKURITEITSKONTROLES VAN SAP R/3

deur

DANIEL CHRISTIAAN MOOLMAN

Opsomming van die skripsie ingedien
vir die graad

MAGISTER COMMERCII

In

REKENAAROUDITERING

aan die
Fakulteit Ekonomiese en Bestuurswetenskappe
aan die
Randse Afrikaanse Universiteit

STUDIELEIER: PROF. A. DU TOIT

Johannesburg
November 1997

OPSOMMING

EVALUASIE VAN DIE SEKURITEITSKONTROLES VAN SAP/R3

Die doel met die opsomming is om agtergrond, metodiek en gevolgtrekkings van die navorsing oor die evaluasie van die sekuriteitskontroles van SAP R/3 weer te gee. Hierdie opsomming is onder die volgende hoofde uiteengesit:

1. **Probleemomskrywing en doel met die skripsie**
2. **Navorsingsontwerp en -metodiek**
3. **Omvang en beperkings**
4. **Resultate**
5. **Gevolgtrekking**

1. PROBLEEMOMSKRYWING EN DOEL MET DIE SKRIPSIE

SAP R/3 is 'n ten volle geïntegreerde besigheidstelsel wat toegerus is vir die doeltreffende funksionering in die oopbediener-omgewing. Die stelsel bestaan uit verskillende modules en kan afsonderlik funksioneer. Die fokus van die literatuurstudie is die evaluering van sekuriteitseienskappe binne 'n oopbediener-omgewing en SAP R/3.

1.1 Probleemomskrywing

Die sekuriteit van transaksies in die IT-omgewing is 'n belangrike kwessie vir die 21ste eeu.

Vir 'n stelsel om behoorlik te funksioneer is sekuriteitskontroles noodsaaklik. Sekuriteitskontroles is onmisbaar, veral met verwysing na beramings dat teen die jaar 2000, 70% van alle transaksies deur die Internet verwerk en geproseseer gaan word.

Sekuriteitskontroles bestaan uit logiese en fisiese kontroles wat geformuleer en geïmplementeer moet word.

Met die gebruik van die Internet om transaksies te verwerk en elektroniese databasisse om inligting te stoor, moet bestuur verseker dat die sagteware stelsel in plek sy sekuriteitsrisiko's aanspreek. Sekureitskontroles moet van so aard wees dat transaksies en informasie in alle aspekte beheer en beveilig word, vir beide logiese en fisiese kontroles.

SAP R/3 het kenmerke en eienskappe wat dit geskik maak vir die prosessering van transaksies wat deur die Internet gedoen word.

1.2 Doel

Die doel van die skripsie behels die ontwerp van 'n sekuriteitsouditprogram wat die eksterne ouditeur in staat stel om die logiese sekuriteitskontroles in die SAP R/3-omgewing te kan bestudeer, spesifiek met betrekking tot twee modules binne die SAP R/3, synde die basiese sisteem en finansiële rekeningkunde sisteemmodules.

1.2.1 Doelwitte

- Evaluering van besigheidsproses-herorganisering.
- Identifisering en evaluering van sekuriteitskontroles binne 'n oopbediener-omgewing van belang vir die eksterne ouditeur.
- Identifisering en evaluering van sekuriteitskontroles binne 'n SAP R/3-omgewing van belang vir die eksterne ouditeur.
- Ontwerp van 'n sekuriteitsouditprogram wat die eksterne ouditeur in staat sal stel om logiese sekuriteitskontroles in 'n SAP R/3-omgewing te bestudeer.

2. NAVORSINGSONTWERP EN -METODIEK

Die benadering van die navorsing is om 'n sekuriteitsouditprogram te ontwikkel wat die eksterne ouditeur kan help in die evaluering van die logiese sekuriteitskontroles binne 'n SAP R/3-omgewing met betrekking tot twee spesifieke modules.

2.1 Metodiek

'n Literatuurstudie van bestaande gesaghebbende verwerkte literatuur is uitgevoer. Ander metodes as deel van die inligtingsinsamelingsproses het ingesluit gesprekke met SAP R/3 tegniese spesialiste en rondblaai op die Internet.

2.2 Navorsingsonderwerpe

- Internet en verwante transaksies
- Besigheidsproses-herorganisering
- Besigheidsukses-faktore en -praktyke
- Oudit van sekuriteitskontroles
- Beveiliging van elektroniesedata-transaksies
- Ontledings van sekuriteitskontroles
- Kenmerke en eienskappe van 'n oopbediener-omgewing
- SAP R/3-sekuriteitskontroles en -kenmerke

Alle bevindinge onderskraag die probleemomskrywing en doelwit van die skripsie.

3. OMVANG EN BEPERKINGS

3.1 Omvang

Die studie fokus op logiese sekuriteitskontroles van twee SAP R/3-modules van belang vir die eksterne ouditeur, naamlik die basiese sisteem (BC) en finansiële rekeningkunde sisteem (FI) modules. Die ander modules se sekuriteitskontroles kan ook hier ingesluit wees, maar vir doeleindes vir die detailnavorsing word dit nie bespreek nie.

3.2 Beperkings en uitsluitings

Die volgende beperkings en uitsluitings is geïdentifiseer:

- Ander SAP-sekuriteitseienskappe en kenmerke;
- Spesifieke industrie verwante sekuriteitseienskappe met betrekking tot SAP R/3 ;
- Sekuriteitseienskappe nie van belang vir die eksterne ouditeur nie;
- Alle fisiese sekuriteitsaspekte;
- Ontleding van sekuriteitskontroles op ander modules anders as die basiese sisteem (BC) en die finansiële rekeningkunde (FI) sisteemmodules;
- Die saamgestelde sekuriteitsouditprogram fokus slegs op die basiese sisteem en finansiële rekeningkunde sisteemmodules;
- Implementeringskontroles en kwaliteitsaspekte ten opsigte van die stelsel;
- Identifisering van verantwoordelikheidsvlakke binne 'n bedieneromgewing;
- Toets- en lewendige datasekuriteitskontroles;
- Onderhoud, instandhouding en implimenteringskoste- oorwegings van sekuriteitskontroles;
- Samestelling van sekuriteitskontrole-spanne;
- Koppeling van besigheids-"drivers" met rekenaartegnologie en sekuriteitskontroles binne SAP R/3;
- Studie oor die volgorde waarin SAP R/3-modules geïmplementeer moet word;

- Veranderings wat aan sekuriteitstabelle aangebring is sedert voltooiing van veldwerk van navorsing; en
- Installasie-toegangskontroles ten opsigte van SAP R/3.

4. RESULTATE

'n Sekuriteitsouditprogram is ontwikkel wat die eksterne ouditeur sal help in die bestudering van die basiese sisteem en finansiële rekeningkunde sisteemmodules in SAP R/3.

Die sekuriteitsouditprogram is 'n riglyn en moet aangepas word vir spesifieke industrieë en SAP R/3-modules in gebruik.

Die sekuriteitsouditprogram bestaan uit verskeie prosedures wat geëvalueer moet word binne die konteks van die spesifieke SAP R/3-stelsel wat bestudeer word. Elke prosedure is geïdentifiseer ten opsigte van die impak daarvan op die basiese ouditstellings van volledigheid, geldigheid, akkuraatheid en instandhouding.

4.1 Die studie het implikasies vir verdere navorsing in die volgende:

- Detail-sekuriteitstudies van ander SAP R/3 modules, BC en FI uitgesluit;
- Fisiese sekuriteitskontroles in die SAP R/3-omgewing;
- Normstelling (benchmarking) van sekuriteitskontroles teen ander IT-kontroles;

- Ontleding van die effektiwiteit van die sekuriteitskontroles ten opsigte van die voordeel wat daaruit verkry kan word;
- Studie van sekuriteitsparameters en die implementering daarvan;
- Sekuriteitprojekanalises;
- Studie van kritiese IT-omgewing-suksesfaktore; en
- SAP verwante studies.

5. GEVOLGTREKKING

Sekuriteitskontroles binne 'n IT-oopbediener-omgewing is van toepassing op SAP R/3. SAP R/3 het omvangryke sekuriteitskontroles wat geïmplimenteer kan word. As die kontroles korrek geïmplementeer word verseker dit 'n veilige omgewing, wat op sy beurt die funksionaliteit van die stelsel sal verseker.

Die sekuriteitsouditprogram wat ontwikkel is, is 'n handleiding vir die eksterne ouditeur wat aangepas moet word vir die spesifieke industrie wat bestudeer word waarbinne SAP R/3 funksioneer.

Die sekuriteitsouditprogram dui al die prosedures se impak op die ouditstellings aan, en daarvolgens kan die ouditeur sy studie fokus op aspekte wat van belang en van toepassing is in 'n bepaalde situasie.

SYNOPSIS

AN EVALUATION OF SECURITY FEATURES OF SAP/R3

1. DEFINITION OF THE PROBLEM AND OBJECTIVE OF THIS SHORT DISSERTATION

SAP R/3 is a fully integrated system equipped to function in an open server environment. The system consists of different modules that can operate independently. The focus of the literature study is the evaluation of the security features within an open server environment and SAP R/3.

1.1 Definition of the problem

Securing transactions in the Information Technology (IT) environment is the key issue for the 21st century.

Proper security controls are essential for the effective operation of a system, especially given the fact that by the year 2000 an estimated 70% of all transactions will be processed via the Internet.

SAP R/3 has features and characteristics which makes it suitable for the processing of all types of transactions on the Internet. It is therefore important to understand the security risks involved, both internal and external. All transactions and information must be secured and controlled.

1.2 Objective

The objective of this dissertation comprises the development of a security audit program to enable the external auditor to evaluate the security controls in the SAP R/3 environment, especially in respect of two modules within SAP R/3, being the basic system and finance system modules.

2. RESEARCH APPROACH AND METHODOLOGY

The research is aimed at developing a security audit program to assist the external auditor in evaluating logical security controls within a SAP R/3 environment, especially in respect of two specific modules related to two modules of SAP R/3.

2.1 Methodology

The research consists of a detailed literature survey on existing authoritative textbooks and other literature. Other mediums in gathering information include surfing the Internet and discussions with technical SAP R/3 specialists.

All findings support the definition of the problem and objectives of the dissertation.

3. SCOPE AND LIMITATIONS

The study focuses on logical access controls of two SAP R/3 modules important to the external auditor, namely the basis system (BC) and the financial accounting systems modules (FI). Some of the controls are

applicable to other modules, but these have been excluded from the discussion in the detailed research conducted.

4. RESULTS

A security audit program has been developed that will assist the external auditor in the evaluation of security features of the SAP R/3, basis system and financial accounting system modules.

The security audit program is a guide for the external auditor, which should be tailored to meet the specific industry requirements and SAP R/3 modules in use. The study has implications for further research in various other areas.

5. CONCLUSION

The security features in an open server environment are applicable to the SAP R/3 environment. The SAP R/3 system comprises comprehensive security features, which if correctly implemented, will result in a secure environment that will enable and ensure proper functionality of the system.

The security audit program further clearly indicates the impact and implications of the procedures on the audit assertions which will assist the external auditor for focusing his approach on specific areas.

CHAPTER 1

INTRODUCTION

CONTENTS PAGE

1.1	Background	2
1.2	Definition of the problem and objective of the short dissertation	6
1.3	Scope and limitations	7
1.4	Research approach and methodology	9
1.5	Definitions	10
1.6	Conclusion	15

CHAPTER 1

INTRODUCTION

SAP R/3 is a highly modular information system that acts as a framework for an integrated business system (Ernst & Young, 1995a:3).

The research conducted resulted in the development of a security audit program for evaluating logical security features of the basis system and financial accounting system modules of SAP R/3. Only procedures of importance to the external auditor have been categorised based on audit assertions. The objective of this chapter is to provide the framework for the research conducted and the structure and layout of the dissertation.

1.1 Background

1.1.1 Business today

For businesses to be successful today, proper software solutions and secure IT controls are required.

As the IT environment changes rapidly, businesses need to continuously reassess their position of operating in this technology environment. Specific decisions regarding dealing with the change and management of the business need to be made and implemented. A company can either expand, shrink or shift as a method of embracing change.

Figure 1.1: Embracing change in the 21st century (SAP Expo April,1997).

Expand:	Shrink:	Shift:
■ Market share ■ Customer base ■ Organisational boundaries	■ Infrastructure ■ Time ■ Costs	■ Industry boundaries ■ Costs and revenues ■ Economics ■ Balance of power

The choice of a software solution has a direct impact on business today, business processing and the future viability of the company. The key issue is to secure the software to such an extent that the business is secured and that all the areas indicated in figure 1.1 are addressed.

When deciding upon a particular software solution, all areas of embracing change such software impacts upon must be considered and combined in the decision process. Exposure and questions on how to deal with change and security necessitate minimising high exposure to competitors and customers in this environment as most people use EDI (electronic data interchange) and the Internet. If a security system is not set up accurately, the company may suffer substantial financial losses or even close down. For this reason, the network security functionality is a critical issue in the implementation and operation of the system.

1.1.2 Introduction to SAP R/3

SAP stands for the German phrase "Systeme Anwendungen und Produkte in der Data verarbeitung". It is an integrated real-time software with modules to support almost all business processes.

It is difficult to choose the correct software solution. The right choice depends on detailed studies and information on the needs and potential of the business. Once a solution has been evaluated and selected, it must be maintained and ensured that it is operational. Management's decision on the software solution is a holistic business decision that affects all areas of the business (SAP R/3 - it's more than software it is a strategic solution; Ernst & Young,1995b:3).

> "Companies must respond to the challenge of rapid change with dynamic strategies. The ability to adapt immediately to new customer needs and market opportunities is a decisive competitive factor. Adapting requires a powerful, open infrastructure that provides optimum support for current business operations and allows flexible adaptation to change and progress. The answer to these challenges is the SAP R/3 system, the most frequently used standard business software for client/ server computing world-wide" (Ernst & Young, 1995a).

SAP R/3 has a revolutionary concept of enterprise wide computing and is at the leading edge of client/server technology with capabilities and functionalities to cope with all types of connectivity related issues (Ernst &

Young, 1997b). The applications in SAP R/3 are modules for opening up performance potential in a company. They link separate operational steps together to form automated workflow chains.

The system controls the flow of information from one department to another and links the company with its customers and vendors. One of the implications of this process-oriented operation is increased productivity. Each business can further customise its implementation, which makes the system flexible and desirable.

Furthermore, the entire system need not be implemented at once (SAP Expo April, 1997:51).

The impact of the highly control-driven, real-time system is a sophisticated internal control environment, an environment that can now ensure integrity and continuity of on-line business. Recently in a South African environment SAB, BMW and SAA, to name but a few, have changed to this dynamic software solution (Anon., 1997).

1.1.3 External auditor's role in the IT environment

The choice regarding a software solution impacts the external auditor in the way that he needs to understand the decision-making process and the set-up of the system, as well as to fully comprehend the new system's capabilities and the financial reports and transactions the system will produce. The impact on the business and the audit needs to be understood and evaluated

against general accepted auditing standards to enable the external auditor to deliver client service and report under the specific requirements of the attest function.

There are different auditing approaches in computer auditing; from auditing around the computer, auditing through the computer and auditing with the computer. The preferred option is to audit with the computer.

This method requires a knowledge and comprehension of the system that includes an understanding of general computer controls and application controls. The security features in any computer environment can have a direct impact on the audit approach followed by the external auditor. In the SAP R/3 environment, the security features which pertain specifically to the SAP R/3 environment and that are important to the external auditor, will be evaluated in respect of two modules. A security audit program has been developed addressing security features of the basis system and the financial accounting system, which impacts the overall audit approach followed by the external auditor in auditing and performing the attest function.

1.2 Definition of the problem and objective of the short dissertation

1.2.1 Definition of the problem

The key issue in the 21st century will be securing the transactions and the environment in which management tends to operate their business. It is estimated that by the year 2000, 70% of all transactions will be processed via the Internet.

1.2.2 Objective

The objective of the dissertation includes the following:

- Evaluating business process re-engineering;
- Identification and evaluation of security controls within the open-server environment;
- Identification and evaluation of security features in SAP R/3 of importance to the external auditor; and
- Development of a security audit program for the use of the external auditor regarding logical security controls in a SAP R/3 environment for the basis system and the financial accounting system modules.

1.3 Scope and limitations

1.3.1 Scope

It is important to fully comprehend what the SAP R/3 comprises before discussing its scope. In essence, the system comprises

- an operating and development environment that deals with general controls issues; and
- an application system that deals with application controls.

These two components are different and have different controls. In certain instances, the security features and program developed can deal with both components. However, the database is the more important area. The controls and security features can be assessed as a whole or by means of logical access path. For the purpose of the research conducted it has been evaluated as a whole with specific reference to two particular modules, namely the basis

system and the financial accounting system modules, with significant audit implications and of importance to the external auditor.

1.3.2 Limitations and exclusions

Due to SAP R/3 's vast field the following limitations and exclusions have been made:

- Security features of previous SAP versions:

  There are different versions of the software. For the purpose of the dissertation, the R/3 version and the findings relating to the security features of this specific version have been evaluated and all other versions excluded;
- Specific industry-related security features regarding SAP;
- Unimportant security features for the external auditor;
- All physical security features;
- The security audit program compiled only deals with the basis system and the financial accounting system modules;
- Implementation controls and costs as well as quality aspects thereof;
- The identification of responsibility levels within the client server environment;
- Test and life data security controls;
- Service, maintenance and implementation costs regarding security controls;
- Security controls teams;
- Linking of business drivers with computer technology, security controls within SAP other modules;

- The sequence of SAP R/3 module implementation;
- Updates to tables and information after the completion of the research have been ignored; and
- Installation access controls regarding SAP R/3.

With the above limitations and exclusions established, it was possible to focus the study on the important and significant audit assertions in developing an security for security features of the basis system and financial accounting system modules.

1.4 Research approach and methodology

The research consisted of a detailed literature survey on authoritative textbooks and other literature. Other mediums included in the gathering of the information are the Internet and discussions with various persons acquainted with the technical aspects of SAP R/3.

The research included topics on the following:

- The Internet and transactions regarding with the Internet;
- Business process re-engineering;
- Best business success factors and practises;
- Audit security controls;
- Securing of electronic data transactions, paperless transactions;
- Open server environments characteristics; and
- SAP R/3 security features.

All findings support the definition of the problem and objectives of the dissertation.

The findings and conclusions reached are based on information at a specific time. From the information obtained in the literature survey, a security audit program has been developed for evaluating specific audit related security features which are significant to the external auditor.

1.5 Definitions

The following definitions have been identified and will be referred to throughout the dissertation:

Audit and management

With expanded user access, administrative and operational requirements for security requires a proper mix of preventive, detective and corrective management controls at all levels of security and audit policies. Audit and management refer to the controls and policies that are in place (Ernst & Young, 1995a).

Strategic planning

The company's organisational structure and data flow needs to be understood before implementation. In order for networks to operate at the highest level of reliability, they must run in a controlled environment. Strategic planning is key to this and requires early involvement by audit and management (Ernst & Young, 1995a).

Evaluation

Analyses of findings regarding security related aspects (Ernst & Young, 1995a).

Client/server security

Client server operating systems should provide both physical and logical security for all components of the system. The security referred to in general therefore includes both types of security. For the purpose of this dissertation, logical controls have been separately referred to (Ernst & Young, 1995a).

Encryption

Encrypted, not readable by eye, passwords stored and controlled: this is a feature of technology that ensures controlled transmission, however it does not guarantee secure communication (Ernst & Young, 1995a). Refer PGP (good privacy) as leading software in the data scrambling software market.

Authentication

Verification of information from and to users (Ernst & Young, 1995b).

Network analysis

Measures the efficiency, reliability and performance of the network. For this you need to understand the core business goals and the business processed supported by the network (Ernst & Young, 1995a).

Completeness

To ensure that data is not lost or erroneously or maliciously deleted (Lubbe, 1995:7).

Accuracy

To ensure that data is reliable and not corrupt and that data is used in processing as intended (Lubbe, 1995:7).

Validity

To ensure that only authorised users, data and transactions are allowed (Lubbe, 1995:7).

Maintenance

To ensure that programs, data files and transactions are not subject to unauthorised changes and duplication. This control encompasses all of the above (Lubbe, 1995:7).

The traditional approach of auditing computer systems has been "around" the computer, where the computer is generally ignored. With reference to SAP R/3 this approach will not be sustainable and the concept of using technology to control technology will be used. The audit objectives have remained unchanged. The security features of SAP R/3 will be discussed in more detail in Chapter 3 (Ernst & Young, 1995b).

Abap/4

A fourth generation language designed specifically for SAP R/3. Much of the system is written in ABAP/4 and users are able to customise the system by modifying or writing their own ABAP/4 programs (Deloitte & Touche, 1997).

Abap/4 query

Report-writing software that allows users to generate reports quickly and easily without programming knowledge (Deloitte & Touche, 1997).

Authorisation objects

Tests defined in the system that are used to determine whether a user is authorised to perform a particular function (Deloitte & Touche, 1997).

Authorisation profile

Profiles contain a list of authorisation value sets. Profiles, which are allocated to users, determine their access capabilities (Deloitte & Touche, 1997).

Authorisation value sets

A list of the authorised values for a particular authorisation object (SAP, 1997b).

Authority check

An ABAP statement that can be used to check whether a user is authorised for a particular authorisation object (SAP,1997b).

Basis system

This is the primary component of SAP that provides the basic capabilities of the system. These capabilities include maintaining the database, providing security, providing standard mechanisms for user dialogues, and the ability to customise and modify the system (SAP, 1997b).

Client

The highest level of authorisation in SAP. This would usually be for an entire group or corporation (SAP, 1997b).

Client/Server

A system in which the processing is split up between different computers on the network (Introduction to Auditing Electronic Data Interchange. Ernst & Young, 1997a).

System profiles

Files containing run time settings for configuring the SAP R/3 system (SAP, 1997).

Tables

All data in the SAP system is stored in tables. This includes master file transactions and control data. Entering data into the control tables can customise the functionality of the system (SAP, 1997b).

User master record

A record that contains information about a user including his password and references to authorisation profiles (Deloitte & Touche, 1997).

1.6 Conclusion

A security audit program has been developed that will assist the external auditor in the evaluation of related SAP R/3 basis system and financial accounting system modules. The security features required in an open/server environment are applicable to the SAP R/3 environment. Furthermore, the SAP R/3 system has a comprehensive list of security features that can be implemented. The security features if correctly implemented, will result in a secure environment that will ensure the proper functionality of the system. The security audit program identifies key issues. The external auditor, in turn, must ensure that these key issues do in fact exist. The program needs to be made applicable for all individual client needs and environments. The controls in the development and application system can differ from one another and the key controls that need to be addressed relate to the database.

It has further been established that the external auditor can cope with the changes in this technology environment if he ensures that a self-training program is maintained whereby the knowledge of SAP R/3 is updated and maintained. The security audit program developed can be used as a guideline in developing programs for individual tailored versions of SAP R/3 applications that are in use.

CHAPTER 2

SECURITY AND AUDIT

CONTENTS **PAGE**

2.1	Objective	17
2.2	Nature of the literature survey	17
2.3	Scope, limitations and exclusions	18
2.4	Business process re-engineering and impact on security	19
2.5	Security objectives, security features and relevant exposures in an open server environment	21
2.6	Server and workstation security features and controls over data movement	26
2.7	Conclusion	29

CHAPTER 2

SECURITY AND AUDIT

Introduction

2.1 Objective

In order to achieve the most benefit from the literature survey, the objectives have been defined.

The objectives of this chapter are the following:

- To study the process business process re-engineering;
- To evaluate the security objectives in an open server environment;
- To understand the security features in an open server environment; and
- To understand the movement of data between server and client.

Establishing an understanding of the audit implications as part of the security audit program to be developed in chapter 4.

2.2 Nature of the literature survey

To ensure credibility and acceptance of the findings and proposals of this short dissertation, the underlying concepts should essentially be based on authoritative views and generally accepted among computer auditing professionals. Theory based on an individual's experience without considering

those generally accepted professional views might be subject to personal bias. Other factors that could introduce bias are the individual's background and the absence of formal research. To avoid these problems, references have been restricted to those published by auditors and auditing firms and to authoritative technical books by computer experts. The authors selected represent experts in this field, with good knowledge and practical experience.

The main categories of authors/ publishers are:

- large audit firms: Deloitte & Touche; Ernst & Young; Coopers & Lybrandt; and
- software manuals on SAP.

The security audit program that has been developed represents a guideline and is dependent on the type and amount of modules that have been implemented. The amount of modules that can be implemented solely depends on the needs of the specific client, as SAP R/3 modules can be implemented in phases. The security audit program developed will be discussed in chapter 4.

2.3 Scope, limitations and exclusions

A variety of literature was studied for relevant references. This was used as a foundation for the research as part of formulating the events to be audited in a client server environment. The combination of the events and the security features of SAP R/3 in chapter 3 form the foundation of the security audit program developed.

The following limitations and exclusions were placed on the scope of the literature survey:

- Security issues in an open-server environment that would be relevant to the external auditor have been studied;
- Security objectives only relevant to the external auditor have been studied;
- Data movement issues only relevant to the external auditor have been studied;
- Events to be audited only relating to logical security issues have been identified; and
- Audit implications regarding logical security, not all audit-related implications have been reviewed.

2.4 Business process re-engineering and impact on security

2.4.1 Business process re- engineering

Business process re-engineering as such is a very comprehensive issue. Because it has a significant impact on security issues that in turn have audit implications, it is part of the study conducted (Deloitte & Touche and SAP SA, 1994).

Business process re-engineering encompasses some form of shift or change. When the change or shift occurs, it indicates a form of business re-engineering. There are different versions and levels of complexity of business process re-engineering.

Business process re-engineering as defined by Capon (1997) is the optimising and fit between business strategy, business practises and the technology infrastructure, which include all security related issues. It entails finding and supporting the essential elements for business success and building a comprehensive repository with business reference models and their relation to business.

It has further impact by simplifying and streamlining the implementation of business infrastructure and configuring and managing business change, which include all technology and IT related issues. Therefore the integration of IT with business today has developed to such an extent that the IT part of business is the driving force in the process and the result of business change (Capon, 1997). With the above statements in mind, the impact on security is clear and management needs to ensure that proper security is in place.

At a SAP R/3 presentation in Johannesburg in 1997, George Oertel, Managing Director SAP South Africa, said: "The capability gap between current business processes and those required by shifts in the business approach, requires a realignment of business investments".

Businesses in the 21st century will therefore undergo some form of change that will impact IT and IT will impact the business. This process is called business process re-engineering. Before the process of business process re-engineering can take place, business drivers must be established first.

2.4.2 Business drivers

Business drivers are the essence (success factors) of the business: those factors that allow the business to survive and that render it profitable. Examples are globalisation, customer service, product quality, market share and response time to the market.

A business driver without the need for change has no meaning. Management must define the scope of the change, i.e. the ultimate action plan, which encompasses the "what we do" (formulated strategy), the "how we do it" (process) and "what we do it with" (required infrastructure).

The above indicates the impact of change required affecting the business model, the people the process and technology including security. It is therefore essential that the entire business model be holistic, complete and integrated.

From the above it is clear that change is certain. Furthermore, the direction of this change has also been established. The final step is developing the business model, which must include all the relevant security features.

2.5 Security objectives, security features and relevant exposures in an open server environment

As business systems become architecturally more distributed, so communication links become increasingly important. The client server technology ensures that critical information is passed through complicated communications links. To ensure consistent minimum levels of security

consisting of physical and logical controls over software and hardware, security standards must be documented and implemented. These standards should be well known by all users and the documentation must be widely and freely available. Without uniform standards, inconsistencies can occur within different areas of an organisation thereby increasing security risk. IT is an integral part in the entire process of any organisation's infrastructure. It is therefore important to establish the objectives of information security.

2.5.1 Objectives and exposures of information security

The objectives and exposures of information security focused upon which are important to the external auditor deals with the following:

Table 2.1 below has been developed based on the security features and objectives identified by Coopers and Lybrandt. It has been linked to assertions by the author and exposures have been identified for each of the assertions.

Table 2:1 Security objectives, security features and exposures (Coopers & Lybrandt, 1994)

ASSERTION	OBJECTIVE	SECURITY FEATURES	EXPOSURE
Completeness	To ensure integrity	Account, passwords, directory, file, supervisor and other	General attacks, hijacking of information, specifically in the Internet connections environment
Validity	To ensure confidentiality protecting sensitive information from unauthorised disclosure	Account, passwords, directory, file, supervisor, and other	General attacks, hijacking of information, specifically in the Internet connections environment
Accuracy	To ensure integrity, safeguarding of information	Account, passwords, directory, file, supervisor, and other	General attacks, hijacking of information, specifically in the Internet connections environment
Maintenance	(Also referred to as availability and can include accountability - ensuring information and vital services are available to users when required	Account, passwords, directory, file, supervisor, and other	Hijacking of user authentication information

In addition to the above network, logons and remote access have to be valid and accurate, as they are exposed to hijacking of user authentication information (Coopers & Lybrandt, 1994).

With the above in mind, it is important that the security objectives are in place throughout the entire process of implementing business process re-engineering.

Having established the objectives, security features can now be assessed.

2.5.2 Security features

Once the objectives have been identified, the features included in the system must be evaluated. Ensure that these features meet the objectives that have been established, as well as the exposures identified. If the security features meet the requirements of the security objectives, it will create a sound, secure environment.

The terms pertaining to security features are explained below:

2.5.2.1 Account level security feature: (main objective addressed: validity)

A user may be automatically logged out or prevented from logging in as the result of the account been disabled, the account expiration date has passed, the log time restriction has been abled, the connection limit has been exceeded or an intruder has been detected. The situation will only be restored once the cause has been identified and rectified (Lubbe, 1995:12).

2.5.2.2 Password level security feature: (main objectives addressed: validity, accuracy and maintenance)

This optional policy can be set ensuring password changes are enforced regularly with specific day intervals. The password security feature can also include the different types of passwords as well as password encryption whereby passwords are encrypted before being stored on the hard disk (Lubbe, 1995:12).

2.5.2.3 Directory level security feature (main objectives addressed: validity and maintenance)

Within the directory rights, the following can be set:

- Read rights - to read the contents of existing files;
- Write rights - allows you to change or add to the contents; and
- Create rights - to copy files to a directory and saving a worksheet and erase command right to delete or erase a file (Lubbe, 1995:12).

2.5.2.4 File level security feature (main objectives addressed: validity and accuracy)

File level security allows access to the files for which a user has been granted a right to use and are flagged according to the user right that has been allocated (Lubbe, 1995:12).

2.5.2.5 Supervisor deletes and writes rights feature (main objectives addressed: validity and completeness)

No transaction can be deleted without approval from the supervisor of the system (Lubbe, 1995:13).

2.5.2.6 Other features (main objectives addressed: all)

In addition to the above, security features can be divided into an entire host of components relating to data centre and operations security. These security features referred to can be local or host-based, network or remote-access based (Priest, A 1997).

Other security features include the following all general interconnectivity issues, including strategic planning; client server security; encryption and authentication and audit and management and network analysis. For changing management systems further separate security features also exist.

Having identified the above security features, we will now examine the specific environment in which security features operate, i.e. server and workstation applications.

2.6 Server and workstation security features and controls over data movement

2.6.1 Server and workstation security features

In a server and workstation environment the security features as identified by (Coopers & Lybrandt, 1994) are expanded to included security over the following:

- Domains, groups, users, permissions and access rights;
- Users manager for domains, user account security, built-in accounts, user account properties, user profiles, home directories- private storage;
- Groups: local, global groups, special groups;
- Pass-through validation; and

- Security structures through file set up, printer security and server manager security, ensuring data is prevented from disaster events.

The subsystem can include features such as local, reference monitor authority checks or security components. The process can be defined to specifically address the log-on process, discretionary access control, access tokens and establishing access control lists.

All the above indicate the various possible forms of security features that need to be implemented. The most important issue however is to ensure that whatever the feature, it addresses the objectives and the exposures identified.

Now that we understand objectives, features, application environments and applications, we need to look at the actual movement of the data. Without the data being moved around the various applications, workstations, servers and connections with the outside vendors, there would not be any security risk.
The movement of data and how such movement is controlled, is set out below.

2.6.2 Controls over data movement

With the concept of features understood, the movement of data must now be evaluated. In an open-server environment, which the SAP R/3 is part of, different issues have to be assessed. For this reason, the link and the impact of data transfer between servers and clients must be fully comprehended.

From here, the link to the audit and the impact on the external auditor can be determined by studying the events that have to be audited in this environment. The study will form the basis for evaluating the security features in SAP R/3 in chapter 3. The basis for the security audit program is designed in chapter 4. Data in an open-server environment is a very important asset, often not recognised in the accounting records. The importance can not be under estimated and the value of the asset is unmeasureable. If this data is exposed to the wrong users, it can lead to a non-viable organisation.

The data between the server and client must be secured and freed from any unauthorised changes. This is not only a technical issue, but involves an entire mindset change from all the users involved, ensuring they become accountable for their own actions. To effect change, users require training (Coopers & Lybrandt, 1997).

To ensure the safeguarding of data, a global security structure has to be implemented that should include formalised, documented policies and procedures.

Bearing all the above in mind, we can now conclude and pull together a thought process for what should be included in a global security feature structure, linking them with audit objectives to address the needs of the auditor after establishing the security audit objectives and applications. This will be used for application in the SAP R/3 environment and to establish a security audit programme for the SAP R/3 financial and basis system.

2.7 Conclusion

2.7.1 Areas to be included in a global security feature structure

The following areas have to be covered as part of the global security features structure, including remote access: (Sapphire International, 1994 and SAP Expo, 1997) .

- Security policy regarding the operating software, the application software and third party software;
- Acknowledgement of messages, transactions and data;
- Physical protection measures of all IT hardware and software;
- Digital protection;
- Encryption for all messages and transactions;
- Passwords changes, uses and length;
- Communications software valid and updated;
- Network technology, network components and devices functional and secured;
- Personal computers and workstations secured and functional;
- Network technology constructs; and
- External access maintained and controlled.

An overall security strategy should include not only adequate host-based security for the network and the workstations, but network protocols. All interconnectivity issues must be addressed.

The global security structure must ensure that objectives, features and exposures as discussed are secured in the entire process of data being transmitted between servers and clients.

2.7.2 General audit objectives

From an audit perspective, the external auditor must meet the requirements of general accepted auditing standards and furthermore, give his or her opinion on the financial results and position of the company. According to Van Rensburg (1992:36), the general audit objectives are listed below:

- Reviewing, monitoring and documenting relevant information systems;
- Assessing the policy on protection of integrity, confidentiality, continuity and availability of the information;
- Analysis of hardware and software, including in-house developments;
- Assessing technology controls and testing network communications;
- Assessing physical security and operational security;
- Reviewing back-up and restoring policies;
- Checking log on and log off, and file and object access procedures;
- Checking user and group management security;
- Reviewing policy changes, restart/shut down and system boot policies as well as domain access;
- Transfer of information into or out of the system;
- Account modifications and account and group authorisation;
- Identification, rights, file and object, access;
- Changes in audit status and utility auditing; and

- Changes in trust relationships and system initialisation, program installation as well as account modification.

The audit approach forms the foundation of the audit. The organisational structure, nature of resources, services that are provided and all applications and processes associated with the business needs to be fully understood and developed into a tailored audit approach.

The methodology to test the adequacy of manual and automated internal controls, ensuring the reliability and integrity of financial and operating data must be written and formalised. The process of formalising an efficient audit approach and methodology should include proper preliminary analysis and assessments.

The audit concerns as to whether the hardware and software communications architecture meets the needs of the organisation and whether it provides thorough accounting records and audit trails must be assessed. The audit type i.e. due diligence, system review security review must be customised and organised around the size and requirements of the client.

2.7.3 Security audit objectives/ implications

The following as identified by (Ernst & Young, 1997a) are security audit objectives/ implications:

- Validity and completeness (Integrity) implies that data and programs are changed only in response to properly authorised transactions and processing;
- Accuracy (Confidentiality) implies that corporate data is available only to properly authorised personnel;
- Validity (Continuity) implies that only authorised transactions and processes change data, once it is stored on a network medium; and
- Maintenance (Availability) implies that data, software programs and hardware assets are always available to authorised users of the network.

2.7.4 Summary

From the above the concerns and issues regarding the security and audit have been identified. In order to understand the impact it has on SAP R/3, security features must be assessed.

The concerns and issues in chapter 2 will be used to evaluate the security features of SAP R/3. The definitions established will be used as part of the study conducted in chapter 3.

In conclusion, a network security refers to the control over the connections specifically to and from other hosts. These controls cover internal and external organisations. As a result of the increased exposure, the auditing feature is important. This will be discussed specifically regarding SAP R/3 in chapter 4 in the security developed.

CHAPTER 3

SECURITY FEATURES OF SAP R/3

CONTENTS **PAGE**

3.1	Objective	34
3.2	Nature of the literature survey	34
3.3	Scope, limitations and exclusions	35
3.4	Background	35
3.5	SAP R/3: the different modules and how SAP R/3 operates	36
3.6	Specific SAP R/3 security features, with specific reference to access controls	48
3.7	Operation and maintenance of SAP R/3 security features	66
3.8	Conclusion	68

CHAPTER 3

SECURITY FEATURES OF SAP R/3

Introduction

In the previous chapter the security objectives, exposures and relevant security features in general were discussed. This chapter is dedicated to the study of security features pertaining to SAP R/3. The literature survey for security features of SAP R/3 is set out under the following headings:

3.1 Objective

The objective of this chapter is to obtain a thorough understanding of the security features within SAP R/3, which are of importance to the external auditor.

3.2 Nature of the literature survey

To ensure credibility and acceptance of the findings and proposals of this short dissertation, it is essential that the underlying concepts should be based on authoritative views and be generally accepted among computer auditing professionals. Theory based on an individual's experience without considering generally accepted professional views may be subject to personal bias.

Other factors that could introduce bias are the individual's background and the absence of formal research. To avoid these problems, references have been restricted to those published by auditors and auditing firms and to authoritative

technical books by computer experts. The main categories of authors/ publishers used Deloitte & Touche, Ernst & Young, Coopers & Lybrant and SAP. These authors represent experts in this field, with good knowledge and practical experience.

From the literature survey conducted and the combining of findings of security and audit as discussed in chapter 2, and the security features of SAP R/3 as discussed in this chapter a security audit program has been developed. This program, which is used by the external auditor, will be discussed in chapter 4. The security is a guide and is dependent on the type and amount of modules that have been implemented, and should be tailored accordingly. This will be discussed in more detail in chapter 4.

3.3 Scope, limitations and exclusions

SAP R/3 has been studied and conclusions have been made from that. For the purpose of the research, all previous SAP versions have been excluded.

3.4 Background

Before the security features are evaluated, the concept, which specifically pertains to the re-engineering for business solutions regarding SAP R/3, must be fully understood.

SAP R/3 ensures a process-oriented organisation. The effects of SAP R/3 can be summarised in the following mindset and changes in the operation (Ernst & Young, 1996; D A Consulting, 1996):

- Customer-oriented aims vs. an attitude of the customer considered a nuisance;
- Flexible organisation structure vs. rigid organisational structure;
- Emphasis on actual behaviour vs. emphasis on structure; and
- Workflow managers enable flexible process control vs. co-ordinating managers control processes.

The remainder of the chapter focuses on the different general security features in an open/server environment and applying them specifically related to SAP R/3. The main purpose is to ensure that data and transactions are protected.

3.5 SAP R/3: the different modules and how SAP R/3 operates

SAP R/3 is a highly integrated software solution that uses electronic data interchange processing between trading partners. This process effects the direct transmission of data from computer to computer over telephone lines and data communications links (Deloitte & Touche, 1997).

SAP R/3 solutions are hard at work in various vertical industries, for instance automobile manufacturers use SAP R/3 to build flow factories, where just-in-time materials and assemblies flow from the vendor into production and then as finished products to the customer. Retail companies use SAP R/3 to achieve consumer response, while wholesale businesses use the system to speed up the processing of business processes from the vendor to the

customer. This enables the simultaneous and optimal calculation of wholesale and consumer prices (Ernst & Young, 1996; D A Consulting, 1996).

SAP R/3 is the fastest growing software solution of this decade. It supports industries such as: (SAP ,1993; SAP , 1994)

- Automotive;
- Banking and insurance;
- Chemical and pharmaceutical industries;
- Consumer goods;
- Healthcare;
- High-tech and electronics industries;
- Machinery and heavy construction;
- Oil and gas;
- Project-oriented manufacturing;
- Public administration and education; and
- Retail telecommunications and utilities.

In essence, SAP R/3 has achieved a high performance, on-line standard software solution for on-line interactive applications. It has immediate access to all relevant information at workplaces, doing away with the multiple entry of data at different sites and increasing the company's competitiveness.

The SAP R/3 applications bring together people who are working on common tasks inside a single company, different people working in a network set up of

several companies, and customers and suppliers at other different locations. The modules in SAP R/3 can be used individually or as a fully integrated system although the true benefits of using SAP occur through broad implementation. SAP includes financial reporting and offers powerful management information capabilities. According to Ernst & Young (1996) and D A Consulting (1996) the use of a common database enables extensive data analysis.

The number of workstations included with SAP R/3 in a client/ server solution is determined by individual needs. It can vary from 30 end users to 3000 end users. The R/3 System runs under various versions of the Unix operating system (e.g. IBM's AIX, Digital's ULTRIX, Hewlett-Packard's UX) and has been launched for the Windows NT, AS/400 environments (Ernst & Young, 1996; D A Consulting, 1996).

SAP R/3 offers standard application software in open-system environments, open hardware platforms and client/server architectures. The key aspect of SAP R/3 is its process-oriented operations - it connects what belongs together with convenient access to all information. The workflow management is integrated with up-to-date, consistently integrated information. The applications are all integrated under one umbrella (Priest, A , 1997).

The software, as dictated by actual needs, can mirror the entire business process. Vertical links generate compressed data for planning and control functions. Enterprises with foreign subsidiaries work within the context of a

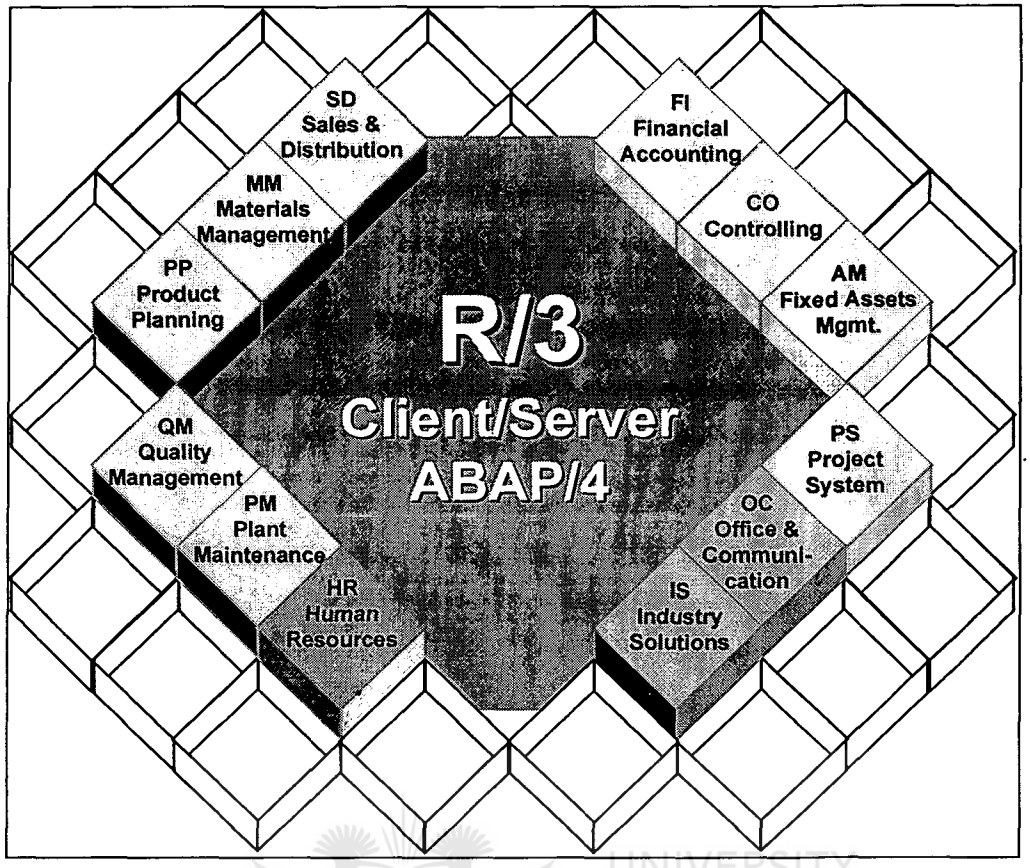
single, international network of consistently designed and smoothly interacting applications.

The SAP R/3 workflow management strengthens the individual responsibility and independence of employees. The system is flexible to change and progress, and runs on the hardware platform of the leading international manufacturers as well as integrated customers' in-house applications. The business processes contained in the R/3 system set new standards, applications are open to allow the integration of third party solutions and by disclosing the architecture and structure it offers complementary software that is easy to interface (Ernst & Young, 1996; D A Consulting, 1996).

3.5.1 The modules in SAP R/3

SAP R/3 consists of different modules as illustrated in figure 3.1 below.

Figure 3.1 Overview of all SAP R/3 modules (Deloitte & Touche, 1997).



The functions of each module are described briefly below:

BC Basis system is the heart of SAP R/3, as illustrated above "R/3 Client-server ABAP/4".

NOTE: This module is included in the audit security program.

FI Financial accounting collects all the data relevant to accounting complete documentation and comprehensive information and is at the same time an up-to-the-minute basis for enterprise-wide control and planning (Ernst & Young, 1996; SAP, 1997b:45).

NOTE: This module is included in the audit security program.

TR Treasury is a complete solution for efficient financial management that ensures the liquidity of your company world wide, structures financial assets profitably and limits risk (Ernst & Young, 1996; SAP, 1997:45).

CO Controlling is a complete system of compatible planning and control instruments for company-wide controlling systems with a uniform reporting system for co-ordinating the contents and procedures of your company's internal processes (Ernst & Young, 1996; SAP, 1997b:45).

EC Enterprise controlling continuously monitors your company's success factors and performance indicators on the basis of specially prepared management information (Ernst & Young, 1996; SAP, 1997b:45).

AM Fixed assets management offers integrated management and processing of fixed assets measures and projects from planning to settlement, including analysis and depreciation calculations (Ernst & Young, 1996; SAP, 1997b:46). This module has been updated and is now part of FI.

PP Production planning provides comprehensive processes for all types of manufacturing: from repetitive, make-to-order and assemble-to-order production through process; lot and make-to-stock manufacturing; process oriented manufacturing with functions for extended MRP II, and electronic kanban, plus optional interfaces to PDC, process control systems, CAD and PDM (Ernst & Young, 1996; SAP, 1997b:46).

MM Materials management optimises all purchasing processes with workflow-driven processing functions, enables automated vendor evaluation, lowers procurement and warehousing costs with accurate inventory and warehouse management, and integrates invoice verification (Ernst & Young, 1996; SAP, 1997b:46).

PM Plant maintenance provides planning control and processing of scheduled maintenance, inspection, damage related maintenance and service management to ensure availability of operational systems, including plant delivered to customers (Ernst & Young, 1996; SAP, 1997b:46).

QM Quality management monitors enters and manages all processes relevant to your quality assurance along the entire supply chain, co-ordinates inspection processing, initiates corrective measures and integrates laboratory information systems (Ernst & Young, 1996; SAP, 1997b:46).

PS Project systems co-ordinates and controls all phases of a project in direct co-operation with purchasing and controlling from quotation to design and approval, to resource management and settlement (Ernst & Young, 1996; SAP, 1997b:46).

SD Sales and distribution actively supports sales and distribution activities with outstanding functions for pricing, prompt order processing, and on-time delivery, interactive multilevel variant configuration and a direct interface to profitability analysis and production (Ernst & Young, 1996; SAP, 1997b:46).

HR Human resources management provides solutions for planning and managing the human resources of your company, using integrated applications that cover all personnel management tasks and helps simplify and speed up the processes (Ernst & Young, 1996; SAP, 1997b:46).

IS Industry solutions and OC office communications provides solutions for industry and office communications (Ernst & Young, 1996; SAP, 1997b).

In addition to all the different modules, the open information warehouse is responsible for and contains intelligent information systems that summarise data from R/3 applications and external sources to executive information supporting not only user department decisions and controls but also the higher level control (Ernst & Young, 1996; SAP, 1997b).

3.5.2 The operation of the SAP R/3 modules

SAP R/3 as discussed above consists of different modules, these modules function in different ways and the way they operate needs to be understood to identify the relevant logical security features the system offers.

The layers form the essence for all the movements that are processed in the system, from transactions entering the system to the final presentation. The flow is as follows, and note that a separate computer can handle each of these layers.

Figure 3.2 The layers of SAP R/3 (Deloitte & Touche, 1997)

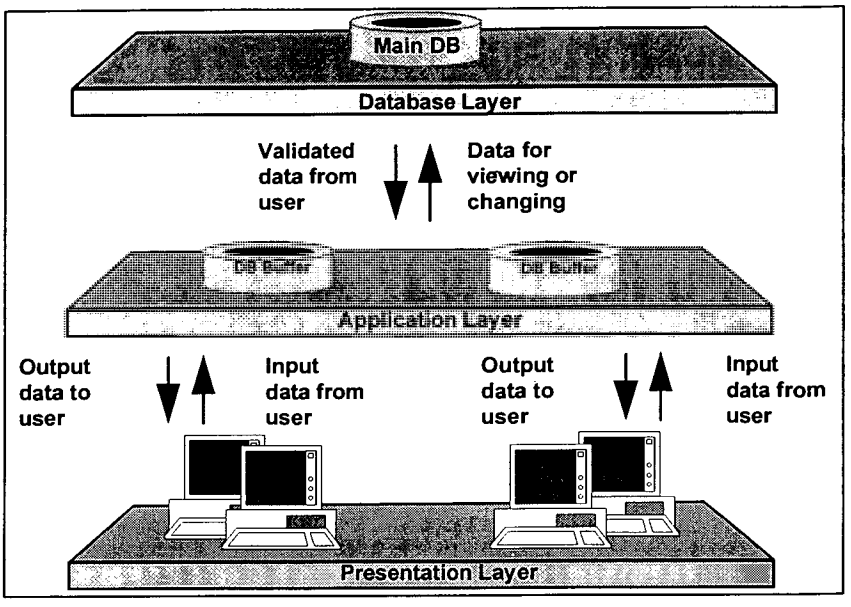


Figure 3.2 illustrates the interaction between the different layers within SAP R/3. This is the key to understanding the operation of the system and relevant functions of the individual components.

The individual layers can be explained as follows:

3.5.2.1 Database Layer

The database layer is the database system used by all application servers. The database server processes the SAP-SQL requests from the application programs, converts them to "standard" SQL and returns the requested data. The following relates specifically to the database server.

Updates Each application server has update processes. If any server creates a huge number of update requests, only the local and central update processes will be used.

Enqueuing A server that manages the locking for SAP objects. The lock server allows multiple users and multiple application servers to synchronise their access to database objects.

Spooling The process that formats data for printing and passes it to a spool system or a SAP spool transfer process.

3.5.2.2 Application layer (Server Layer)

The server layer consists of the SAP System servers. Within SAP there are application servers and associated servers (Deloitte & Touche 1997).

a) Application Server

The heart of a SAP System is one or more application servers and the associated servers that process requests for SAP services. Each application server takes on part of the SAP System workload.

An application server is the SAP System kernel, which runs ABAP/4 programs and therefore can run SAP applications that manipulate data obtained from the user and the database. An application server consists of:

- A dispatcher task: the responsibility of the dispatcher task is to manage the queues of processing requests; and
- One or more work processes: the responsibility of these is to carry out the processing requests.

The dispatcher receives user inputs from the presentation layer and requests for services from other application servers as well as from work processes themselves that he then allocates for services to its work processes, which carry them out.

b) A work process has four components: (Deloitte & Touche 1997)

- TSKH: The task handler, which communicates with the dispatcher and oversees execution in a work process;
- DYNP: The dynamic program (dynpro) processor, which executes the logic in SAP screen programming;
- ABAP: The ABAP/4 processor, which executes ABAP/4 programs; and
- DB-SS: The database interface, which converts SAP Structured Query Language (SQL) instructions into SQL requests to the database.

c) Associated Servers (Deloitte & Touche 1997). Support services provided to the application servers by associated servers include:

Dialogue Management	User transactions are divided into dialogue steps. Each time a user presses the enter key or a function key or selects a menu item, the dialogue server sends a dialogue step to a dispatcher.
Background Processing	The background processor executes programs submitted for background execution.
Messages	The message server routes messages and service requests between application servers. All active application servers of a system are registered with the message server.

Gateway Services	The gateway server communicates with external systems using the Common Programming Interface-Communication (CPI-C) protocol. An R/3 system can use CPI-C requests to obtain services from and exchange data with another R/3 system, a R/2 system or a CPI-C partner. The gateway server is the only server that communicates with external systems.

3.5.2.3 Presentation Layer

The function of the presentation layer is to display information to users and transfer data entered by the users to the application server layer (Deloitte & Touche 1997).

Personal computers or workstations on which SAPTEMU has been installed support presentation services. The processors are connected to the SAP host computer by a local area network (LAN) or wide area network (WAN).

Having established a background about SAP R/3, we will now look at some characteristics and benefits prior to later analysing the security features. The security features can only be analysed if a understanding of the system has been established.

The openness strengthens the independence and protects the investment for the long term. It grows with the technical development and with hardware changes R/3 change. The R/3's application link enabling (ALE) incorporates autonomous application systems located at various sites in an enterprise. It ensures wide network communication of distributed business.

In short the SAP R/3 modules automatically inform purchasing when minimum stock levels are reached and recommend an order volume based on the upcoming production requirements. It is more than information exchange between sales and production; its modular structure enables the user to link all business processes in a company across all hardware platforms and operating systems to achieve optimum use of resources.

The BC basis component is the central SAP component that provides the support and the link for the other modules. The BC module is the single most important module of the modules (Deloitte & Touche 1997).

3.6 Specific SAP R/3 security features, with particular reference to access controls

With the different modules understood and the way the information is moved between the different layers within SAP R/3, the specific security features can now be evaluated. Within SAP R/3, the security can be broken down: security as a result of the installation and security as a result of controls over access.

As noted in chapter 1, the installation controls fall outside the research conducted and the access controls will be discussed further. Access controls, security features regarding the BC (basis system) module (Ernst & Young, 1996; SAP, 1997b).

The SAP R/3 system runs on among others Unix and Windows NT operating systems in a client server environment. Security features can be built into the host and other operating systems but this is beyond the scope of this

dissertation. The security in the system therefore depends on the logons, set-ups of information and tables - referred to as access controls.

3.6.1 Access controls

Access controls can be divided into the following (which will be discussed individually):

- Log on procedures, including passwords, and log on process;
- User master record, including user ID, password and user group and period of validity;
- TSTC table, including table entries, transaction tables, number ranges, procedures and tables to be secured;
- Authorisation value sets;
- Authorisation profiles;
- Program security;
- Accessing production programs- including module pools, accessing dynpros, accessing queries and types of authorisations; and
- General.

3.6.1.1 Log on procedure

Log on procedure checks the users ID and password and ensures that only valid users can access the system. The log on procedure is used to identify and authenticate users. At first log on, the system forces the user to change his initial password. (The authorisation object, authority check for transaction code)

To improve password integrity by making passwords more difficult to guess, the system requires passwords: These passwords must be at least three, and at most, eight characters long. Furthermore, the passwords cannot:

a) begin with three identical characters or an exclamation mark;

b) contain a space within the minimum length specification;

c) commence with any sequence of three or more characters that occur in the user ID;

d) be PASS or SAP; and

e) cannot be any of the user's previous five passwords.

Parameters for user logons (Ernst & Young, 1996; SAP, 1997b). The system profile parameters can be used to set passwords, characteristics, incorrect log in limits and the default client. The parameters can specify the following regarding the passwords: (Ernst & Young, 1996; SAP, 1997b) expiry date, minimum characters, lock facility, number of times an incorrect password can be entered. The system tests access parameters for each log on and authenticate their identity.

Log on process: At log on, users identify themselves to the system and a password is used to authenticate their identity. The user ID and encrypted password are stored in table USR02. System profile parameters are used to set password characteristics, such as the following (Ernst & Young, 1996; SAP, 1997b).

a) Log in/min-password-lng vv: Minimum password length. The default is three characters. Any value from three to eight can be used. The typical recommendation is a minimum length of six characters.

b) Log in/password-expiration-time-hange frequency. The number of days after which a password must be changed. The default is zero, which never requires the user to change the password. The typical recommendation is at least every 45 days.

c) Log in/fails-to-end. Failed log on attempts. Based on the default setting, the user can enter an incorrect password three times before the system ends the log-on attempt. While SAP allows any value from 1 to 99, the typical approach is to permit three attempts.

d) Log in/fails-to-user-lock. Failed log on attempts with lock out. This is the number of times a user can enter an incorrect password before the system locks the user out. Locked users are automatically released at midnight. The default value is 12. The typical recommendation is a value of three.

e) Log in/system-client. Specifies the default client that is automatically filled in on the system log-on screen. The user can type in a different client.

f) Zcsa/system-language. Specifies the default language in which the log on screen appears. The user can change the language.

g) Log in/no-automatic-user-sap*. Disables the SAP* user even if the user-id has been deleted.

h) Rdisp/gui-auto-log out. Automatic terminal log out. This parameter represents the seconds of inactivity before logging out a user from the session (zero = no log out). We typically recommend 15 minutes. These parameters are globally effective when defined in the default system profile, DEFAULT.PFL. They can be made instance specific by being defined in the profile of each application server in the SAP System.

i) Cannot begin with three identical characters, a question mark or an exclamation mark, have the first three characters that occur in the user ID, contain a space with a minimum length, cannot be PASS or SAP or any previous five passwords.

3.6.1.2 User master record

The user master record contains the information about a user such as user ID, password, user groups, user type, period of validity and references to authorisation profiles. Each user requires a master record for each client that access is needed. The user master records contain references to

authorisation profiles that specify the authorisation details. While user master records can be deleted, this deletes the audit trail of transactions entered by that user. The preferred approach is to lock the records when they are no longer required.

A user master record as identified by Deloitte & Touche (1997) includes the following information (important to the external auditor):

a) **User ID**: The default user type for the normal interactive user is "dialogue". Other user types are needed for special types of processing, such as batch input. The period of validity for the user ID should be specified for anyone who is being given temporary access to the system, such as consultants, temporary staff or auditors.

b) **Password**: The user ID and password (stored in encrypted format) are used in the log on procedure. Only valid users are allowed access.

c) **User group**: User group refers to the authorisation that and administrator has to change master records. If the user is not allocated to a user group then any user administrator can alter the user master record. User groups are defined as part of the access control approach for tables, reports and programs. They must be established if the maintenance of user access, is divided among several security administrators. When a user is assigned to a group, only the administrator authorised to maintain that group can alter the user's

master record. If no group is specified, any user administrator can change the user's master record.

d) **Period of validity**: Period for which access is valid.

3.6.1.3 TSTC table

Table of all the transactions available in the system. It defines the authorisation of all users to run each transaction. If a transaction is marked as not requiring and authorisation check, all users can run that transaction with the appropriate menu option (Ernst & Young, 1996; SAP, 1997b).

The tables that control the SAP System processing and hold the security information reside in the database that also holds the programs and data. If users are able to access the database directly outside the SAP System, security may be significantly compromised. It is most important that operating system and database management system controls are defined and implemented in such a way that the SAP System controls are supported. Section 5-C includes a list of tables that must be secured.

SAP does not include any encryption technology. R/3 stores all data in one database. The passwords are, however, coded using a proprietary one-way hash function. While this algorithm is not published by SAP, it is fixed rather than key-driven. This may not be sufficient for highly security conscious companies. SAP provides an interface between R/3 and external security systems such as Kerberos.

a) Table Entries

SAP is delivered with some standard system table entries, not all of which are necessarily used in the installation. The unused entries should be removed. If they remain in the system there is a risk they will be used for other than the intended purpose. Additionally, deleting these entries may improve the user friendliness of the system, since the user will not have to view irrelevant data. The removal of the unused entries must be handled with care. It is possible that one business area will regard the entries as unused while another area may need them. Appropriate procedures should be followed to ensure that entries are not removed until all relevant areas have concurred in their removal.

b) Transaction Table

When a user selects a menu entry or enters a transaction at the command line, the authority of the user to initiate the transaction is verified. Table TSTC lists the transactions in the system. It notes additional authorisation tests to be performed when a user runs a transaction. If a transaction is marked as not requiring an authorisation check, all users with the appropriate menu option can run that transaction.

The field admin functions in object system admin functions must be set to TCOD to allow a user to add, alter or delete the additional authorisation tests.

c) Number Ranges

Number ranges are used to assign numbers to individual database records that belong to a business object. For example, numbers can be assigned to orders, operations or material master records. The numbers are part of the key that identifies a database record in the system and do not have any built-in significance.

A number range contains a set of characters or numbers which may be either:

- External: Numbers, assigned manually by the user; or
- Internal: Numbers, assigned automatically by the system.

The set of characters in the number range is defined by an interval. The number range interval consists of numbers or alphanumeric characters and is limited by the fields From Number and To Number. Number ranges can be maintained using transaction SNRO or from within a SAP application. The number ranges are stored in the TNRO table.

Typically, number ranges are assigned during system implementation and an approach is developed for expanding the ranges. Once the system is in production, number ranges should not be changed, since

this could cause significant problems. The number ranges must be accessible to only appropriately authorised users in order to prevent incorrect changes to the ranges. The system uses the Number Range Maintenance authorisation object to test access to the functions for managing number ranges.

d) Procedures

Policies must be developed that specify which users are permitted to make table changes. Various levels of table changes must be identified and the procedure specified for making each type of change. For example, the process for adding a new general ledge account number should be very different from the process for changing a global system parameter.

Changes to the tables can be logged. The system uses change document objects to specify which tables are logged and the level of logging performed on each table. A list of the tables whose changes can affect the structure of the system should be developed. For these tables, all changes should be logged and the logs reviewed on a regular basis.

e) Tables to be secured

Table 3.1 indicates all the tables that must be accessible to only appropriately authorised security administration personnel.

Controlling the tables is specifically important to the external auditor. These tables are important to the system that needs to be secured but are not all the tables that should secured; others have been excluded from the research conducted.

Table 3.1: List of tables to be secured (Deloitte & Touche ,1997; Ernst & Young , 1997c; Ernst & Young, 1996; SAP, 1997b)

TABLE	Description
DD02V	List of Tables and Descriptions
TACT	Activities that can be Protected
TACTT	Activities that can be Protected with Descriptions
TACTZ	Authorisation Objects and Valid Activities
TBRG	Authorisation Objects and Authorisation Groups
TBRGT	Auth. Objects and Auth. Groups with Descriptions
TDDAT	Table Authorisation Groups
TOBJ	Authorisation Objects
TOBJT	Authorisation Objects and Descriptions
TOBC	Authorisation Object Classes
TOBCT	Authorisation Object Classes and Descriptions
TSTC	Transaction Listing
TSTCA	Values for Transaction Code Authorisations
TSTCT	Transactions with Description
USR01	User Master Records
USR02	User ID and Passwords
USR03	User Address Data
USR04	User Master Authorisations
USR05	Field Defaults by User
USR06	User Address Information
USR07	Objects/values of Last Failed Authority Check
USR08	Table for User Menu Entries
USR09	Entries for User Menus

Table 3.1: List of tables to be secured (Deloitte & Touche ,1997; Ernst & Young , 1997c; Ernst & Young, 1996; SAP, 1997b)

USR10	Authorisation Profiles
USR11	User Master Profiles and Descriptions
USR12	User Master Authorisation Values
USR13	Authorisation Descriptions
USR30	Additional Info for User Menu
USRMM	User Settings: Material Master
USH02	Change history for log on data
USH04	Change history for authorisations
USH10	Change history for authorisation profiles
USH12	Change history for authorisation values

3.6.1.4 Authorisation value sets

Authorisation value sets: for each authorisation object an authorisation value set containing the specific values for which the user is authorised is also required. An unlimited number of access privileges can be defined for each authorisation object. An authorisation value set is a list of set permissible values for each field in an authorisation object.

3.6.1.5 Authorisation profiles

Authorisation profiles: the profile concept used to grant authorisation for value sets. The user master record refers to profiles and the profiles in turn refer to value sets that determine the access capabilities of the user (Ernst & Young, 1996; SAP, 1997b). A profile applies for each workplace. The ability to allocate the same profiles to different users and to allocate the same authorisation value sets to different profiles is possible within SAP R/3. More

than one profile can be assigned to a user, which is done by task therefore reducing the risk of performing functions not intended.

3.6.1.7 Program security

Executing Programs: SAP's approach to controlling the execution of programs (ABAPs) is to establish authorisation groups. ABAPs are assigned to groups and users are authorised to groups. An ABAP can be run only by users authorised to that ABAP's group.

S-PROGRAM is the object used to define whether a user can submit an ABAP/4 program. It identifies the groups of programs that can be accessed. It also restricts the types of activity performed on the program groups. As delivered, ABAPs are not assigned to authorisation groups. Any user may run ABAPs that are not assigned to an authorisation group with authorisation for object S-PROGRAM. Any user who can execute transaction SA38 can run any of the standard ABAPs. It is essential that each ABAP is assigned to an authorisation group so only users authorised to that group can run it. Users should be given authorisation to only those groups needed for their job functions.

The S-PROGRAM authorisation object that allows users to run ABAP/4 programs contains two fields:

1. Program Group-Names of the program groups for which a user is authorised.

2. Activity -The types of activities the user can perform on programs in the program group(s).

Possible activities include (Ernst & Young, 1996; SAP, 1997b):

- SUBMIT: Start programs interactively;
- BTCSUBMIT: Submit programs for background processing;
- EDIT: Maintain attributes and text elements, use utilities for copying and deleting reports; and
- VARIANT: Maintain variants (parameters passed to an ABAP program).

SAP provides additional protection related to program execution: (Ernst & Young, 1996; SAP, 1997b)

- The database interface uses the AUTHORITY-CHECK instruction to check if the user is authorised to access or change the information needed by an ABAP; and
- Table TSTC lists the transactions in the system and notes additional authorisation tests to be performed when a user runs a transaction.

3.6.1.7 Accessing Production Programs

Most of SAP is written in ABAP/4 and unauthorised changes to the SAP System must be prevented. The ability to write or modify ABAP programs requires strict control.

Access to production programs is available to anyone with the right authorisation. Not anyone should be given the right to directly change production source code within the production environment. All program changes should be made in a test environment and tested, reviewed and approved before being migrated to production.

SAP's approach to controlling the creation/modification of programs is to establish authorisation groups. ABAPs are assigned to groups and users are authorised to groups. An ABAP can be modified only by users authorised to that ABAP's group.

As delivered, ABAPs are not assigned to authorisation groups. Any user may change ABAPs that are not assigned to an authorisation group with authorisation for object S-DEVELOP.

The S-DEVELOP object allows users to create and modify programs. Authorisations using this object must be closely monitored. The object contains the following two fields:

1. Program Group: Names of the program groups for which a user is authorised; and
2. Activity: The types of activities the user can perform on programs in the program group(s).

Possible activities are:

- SHOW: Display a program in the editor or a screen in the screen painter; and
- EDIT: Change a program using the editor or a screen in the screen painter.

The developer of a newly created ABAP/4 program must include appropriate authorisation checking instructions in the program. Procedures must be in place to verify such programs and ensure the necessary security checking is performed.

a) ABAP/4 SQL Statements

ABAPs may contain ABAP/4 open SQL statements or possibly native SQL statements. These do not trigger authorisation checks at run time, which means they provide unrestricted access to the database (Deloitte & Touche, 1997).

This lack of control can be overcome by including the AUTHORITY-CHECK statement in the ABAP to check at run time the user's authority for the objects. This control should be included in every ABAP containing SQL statements and procedures should exist to ensure the inclusion occurs.

b) Module Pools

A module pool is a set of ABAP/4 programs that check and process the user's entries. It is the framework for a transaction and stores the

associated screens, menus and function keys. These programs form a unit with the transaction code and the screens (dynpros) and can not be run on their own.

c) Accessing Dynpros

It is possible to make major changes to the system by changing dynpros. Therefore, tight controls must be in place to ensure that changes to dynpros are authorised, tested and approved before the changed dynpros are placed in production (Ernst & Young, 1997b).

The S-DEVELOP object allows users access to the screen painter. Authorisations using this object must be closely monitored.

d) Accessing Queries

ABAP/4 Query user groups must be defined so those users permitted to run or change queries can be appropriately authorised. The user group defines the functional areas and names of the people authorised to run or change the query (Ernst & Young, 1996; SAP, 1997b).

These user groups are not defined in the standard profiles and authorisations. They represent an additional set of information to be updated when users' jobs change. Procedures must be in place to ensure the user group information is changed.

The system uses user group assignments and the authorisation object ABAP/4 Query to test access to the ABAP/4 Query facility.

According to Ernst & Young (1996) and SAP (1997b), three types of authorisations can be assigned:

- Run queries. A user must be assigned to the appropriate user group to run a query. No authorisation for the Query object is needed. Users can run any query defined for their own user group regardless of who wrote the query;
- Run and maintain queries. A user must be assigned to the appropriate user group. "02" Query authorisation is needed; and
- Run and maintain queries, maintain user groups and functional areas. A user must be assigned to the appropriate user group. "23" Query authorisation is needed.

The authority to maintain the user groups should be restricted to administrators. The activity field of the ABAP/4 Query authorisation object should be set to 23 (maintain environment) for these administrators.

3.6.1.8 General controls

Logging transaction SU93 and SU91 can be used to display changes made to user master records and profiles (Deloitte & Touche, 1997). Security is enhanced by locking certain critical transactions that can only be unlocked through specific authorisation object checks. All changes are logged by the

system. For each log the system reports both the old and the new version. This is available control for unauthorised changes to users access capabilities and with a regular review ensure the system function as intended.

3.7 Operation and maintenance of SAP R/3 security features

With the types of security features identified that are in place, the operation of these security features needs to be assessed.

3.7.1 A typical operation case study presents and reveals the following:

The user enters the user ID and password. The system will check the user ID and only valid users with the correct password will be allowed to enter the system. The user enters a transaction (either from menus or directly from the command line).

If the transaction does not exist (not defined in the TSTC table) it is rejected. If the transaction has been marked as locked (through transaction SM01) it will be rejected.

If an additional authorisation check has been identified in the TSTC table, the user's authorisation value set for this object is tested. If the user is not authorised for the additional check, the transaction is rejected.

The other detailed authorisations of the user (stored in profiles and authorisation value sets) are checked to determine whether the user is authorised for all required objects.

3.7.2 Maintenance in general

Restricting the ability to maintain security: Procedures are in place to ensure that the changes processed to ensure that users are able to change master records, profiles and value sets are all done and in line with procedures and according to management's guidelines. All maintenance is set per object, field and value.

The standard authorisations that are maintained are as follows:

- Authorisations in production system;
- Authorisation profiles;
- Authorisation objects; and
- Authorisation value sets.

From the above features, it is clear that vast capabilities exist within the SAP R/3 environment. The set-up is in the user's hands. The various authorisation components and their relationships are very powerful and inter-linked. In summary, the composite profiles referred to as more than one profile.

For example, a user contains a composite profile C, which is a combination of profile A and B. Each profile contains pairs of authorisation value sets and objects. The objects referred to are defined in the system and contain one or more fields that are used to test user access. The authorisation value sets are lists of all values (for each field) for which a user is authorised.

In conjunction with ABAP/4 authority check program, the system checks all authorisations that the users possesses for that object until it finds an

authorisation value that satisfies the nature of the user request, otherwise access is denied (Deloitte & Touche, 1997).

3.8 Conclusion

From the above analysis and literature survey, it is noted that SAP R/3 has a fast variety of security features. These security features have different impacts on the audit engagement. The impact on the audit and the evaluation of the security features will be discussed in chapter 4, as part of developing an audit program, to deal with the security features.

CHAPTER 4

SECURITY AUDIT PROGRAM FOR SAP R/3

CONTENTS PAGE

4.1	SAP R/3 security features impact on the audit	70
4.2	Security audit program	74
4.3	Conclusion	83

CHAPTER 4

SECURITY AUDIT PROGRAM FOR SAP R/3

In a SAP R/3 environment, the client's business applications talk directly to their trading partner's business applications, reducing costs, paper and people.

The main concern that has been identified is security. How should a message from a trading partner be tested from a security point of view to ensure that it was not sent by a disgruntled employee bypassing controls, or by an external "hacker" who penetrated their system?

Issues regarding audit and SAP R/3 were discussed in chapter 2 and 3. SAP R/3 has relevant security features and those features relevant to the external auditor now need to be identified and tested.

4.1 SAP R/3 - security features impact on the audit

SAP R/3 has many security features, and they are comparable to security features in the open server environment. The complexity of the system reveals certain challenges and implications for the auditor.

The implications and challenges directly impact the audit methodology. The audit methodology is part of the entire audit plan of finalising the security features of the modules to be tested.

The security audit program is based on all relevant findings, audit implications, challenges and the methodology developed. The program is a guide and needs further tailoring for a specific industry.

4.1.1 The auditor is faced with the following challenges:

a) The system is complex and highly integrated, and he needs to test the access to data, ensuring that only authorised users view this data.

b) The software is highly customised using thousands of tables and the auditor requires a good understanding of the tables and options that affect control.

c) Unlike traditional data processing environments, the boundaries between the users and the systems staff (programmers, operators, etc.) are not clearly defined. The risk of inappropriate segregation of duties must be defined and included in the security .

d) Users can tailor SAP R/3 to their requirements by writing routines using ABAP, a fourth generation language delivered with SAP R/3. This option has great impact on the audit approach since standard programming logic may have been changed - which makes the testing of the standard programming logic and the other versions in use very important.

e) The distributed nature of the system means that control information may be defined in more than one location, since each application server has its own parameter file. So while the database server may have appropriate settings (e.g. for password length or failed log on attempts), the application servers could have different values that would override the database server's values for the users attached to the application

server. The external auditor will need to include procedures in his security to ensure all testing is done at the various locations where all the servers are situated to address the risk.

The following audit methodology concerns must be incorporated in the entire audit process:

a) An overall assessment of the control environment as well as a detailed risk assessment must be performed.

b) Identification of all sources of information that affect the accounts must be performed.

c) Development of an audit approach which must include the following:

- Tests to ensure the tables are valid and complete;
- Tests to ensure that there is no inadequate segregation of duties;
- Testing the standard program logic in use to ascertain whether the version is current and up to date;
- Specific tests for each parameter file in use; and
- Testing the audit report writing function that is used and the reports generated by the function.

d) Execution of the audit approach.

e) Formulation of audit conclusions based on the audit approach executed and audit fieldwork findings.

4.1.3 As part of the audit work to be completed, the external auditor has a audit security report function with the following capabilities to his disposal:

- Display of detailed information on user master records;
- Display of authorisation profiles;
- Display of authorisation objects and authorisation value sets; and
- Display of all authorisation value sets and objects processed by the user.

In conclusion, this function can be used to test all users access capabilities. The testing of the report function and the reports are included in the security.

4.1.4 Summary

From a security aspect, prevention is preferred above detection and the controls are partially more important. Because of the extent of the automation of transactions, the speed and number of transactions, the loss of traditional audit trails and the increased complexity of the transactions detect controls become more difficult to implement. Detect controls are limited now to exception reports. On the other hand, SAP allows better management information. This results in high-level management controls and key performance indicators to provide overall assurance.

Based on all the information and literature survey conducted, the security audit program has been developed. The security audit program deals with all the assertions in combination and is in no specific order in dealing with the

literature survey results from chapter 2 and 3. As established the security features in the SAP R/3 environment can deal with the security issues.

4.2 Security audit program

4.2.1 Introduction

The security features in an open server environment are applicable to the SAP R/3 environment.

The SAP R/3 system comprises comprehensive security features, which if correctly implemented, will result in a secure environment that will enable and ensure proper functionality of the system.

The security audit program further clearly indicates the impact and implications of the procedures on the audit assertions which will assist the external auditor for focusing his approach on specific areas.

4.2.2 The following assertions and definitions are important:

Completeness

To ensure that data is not lost or erroneously or maliciously deleted (Lubbe, 1995:7).

Accuracy

To ensure that data is reliable and not corrupt and that data is used in processing as intended (Lubbe, 1995:7).

Validity

To ensure that only authorised users, data and transactions are allowed (Lubbe, 1995:7).

Maintenance

To ensure that programs, data files and transactions are not subject to unauthorised changes and duplication. This control encompasses all of the above (Lubbe, 1995:7).

The traditional approach of auditing computer systems has been "around" the computer, where the computer is generally ignored. With reference to SAP R/3 this approach will not be sustainable and the concept of using technology to control technology will be used. The audit objectives have remained unchanged. With this in mind the following secuirty audit program has been developed as discussed below.

4.2.3 SAP R/3 Security audit program pertaining to BC and FI modules

The program deals with all the security features and are specific for the BC and FI module. Table 4.1 lists a number of questions, instructions and statements pertaining to SAP R/3. For the purpose of the audit procedure, its impact has been evaluated and categorised as to what audit assertion is effected. The audit assertions have been abbreviated as follows:

C - Completeness
A - Accuracy
V - Validity
M - Maintenance

Table 4.1: Security Audit Program - BC, F1 Modules

AUDIT PROCEDURE	Ref Ch 3	C	A	V	M
Is the software source code for ABAP'S and Dynpro's available and encrypted?	3.6.1.1 and 3.7		X		X
Obtain a complete list of all the systems software used on hardware identified at all the different locations in use. Document any changes from previous tests conducted.	3.6.1.1 and 3.7	X			
Obtain the contingency plan document. Test how the continuity of trading capability is ensured.	3.6.1.2 and 3.7				X
Establish the relationships between the users and the information systems department, regarding the structure and set up of users in the environment.	3.6.1.2 and 3.7				X
Document the boundaries between users and system staff, discuss their functions and establish whether adequate segregation of duties do exist, in order to establish whether invalid access is possible or not.	3.6.1.2 and 3.7			X	X
Enquire as to how the financial management ensures and monitors user involvement in the development of programs including the design of internal control checks and balances.	3.6.1.3 and 3.7				X
Obtain a copy of the logical security policy documented and review the general computer controls relating to logical access controls.	3.6.1.1 and 3.7	X	X	X	X
Inquire and test the ownership structure in place, whether it is complete and comprehensive to address the necessary requirements.	3.6.1.3	X			X
Inquire and test the policies and procedures in place over the granting of user access.	3.6.1.2 and 3.7		X	X	
Test the security function of the basis systems and financial accounting system modules in place, ensuring only users have access to the life system and development access is properly controlled and separated.	3.6.1.2 and 3.7	X	X	X	X

Table 4.1: Security Audit Program - BC, F1 Modules

Obtain the program logic and audit the changes to the last versions.	3.6.1.4, 3.6.1.5, 3.6.1.6 and 3.7		X		
Test the user's rights regarding ability to change system parameters, and whether a proper rotation plan is in place for functions and responsibilities.	3.6.1.1 and 3.7	X		X	
Test the validity and completeness of procedures followed for changing system parameters.	3.6.1.2 and 3.7	X		X	
Test the parameter report for evidence of being reviewed regularly and properly followed up.	3.6.1.7 and 3.7				X
Check whether the original password for SAP R/3 been changed.	3.6				X
Obtain the audit security report generated by the system and review changes regarding authorisation profiles.	3.6.1.5 and 3.7	X	X	X	X
Obtain the audit security report generated by the system and review changes regarding user master records.	3.6	X	X	X	X
Obtain the audit security report generated by the system and review changes regarding authorisation objects.	3.6.1.4 and 3.6.1.5	X	X	X	X
Obtain the audit security report generated by the system and review changes regarding authorisation value sets and objects.	3.6.1.6	X	X	X	X
Test the procedures in place to identify lock transactions that are potentially dangerous and not normally required.	3.6.1.7 and 3.7			X	X
Test the validity of which users have the ability to lock and unlock transactions.	3.6.1.7 and 3.7			X	
Test the validity of which users are able to alter and delete the additional authorisation checks defined in table TSTC.	3.6.1.7 and 3.7			X	
Test the validity of which users have access to the ABAP/4 dictionary, and check whether their passwords are changed regularly.	3.6 and 3.7			X	
Test the right of all users to identify what control management has over the ABAP/4 dictionary to determine whether any unauthorised changes have been made.	3.6 and 3.7			X	

Table 4.1: Security Audit Program - BC, F1 Modules

Obtain a list of users who have the ability to run ABAP/4 and their access rights. Compare to prior lists to ensure terminations have been properly updated. Test other users' rights to establish the completeness of the list.	3.6.1.7 and 3.7			X	
Inquire as to whether any users on the production system have the ability to edit ABAP/4.	3.6.1.7 and 3.7	X			X
Review and inspect the sites and work stations and determine what policies are in place to prevent passwords been written down and displayed or kept at the work station.	3.6.1.3 and 3.7			X	X
Review system changes regarding passwords to ensure all password issues and confidentiality are properly communicated to the users by ensuring passwords are not displayed, are changed regularly via the system and adhere to all the password guidelines.	3.6.1.8 and 3.7			X	X
Perform test to establish whether each user has a unique ID and password.	3.6.1.4 and 3.6.1.8			X	X
Test passwords' length and expiry dates to ensure they are properly enforced.	3.6.1.5			X	X
Test and inquire whether user profiles are reviewed regularly and updated correctly.	3.6.1.5 and 3.7			X	X
Test the system to establish whether there is an ability to activate profiles and authorisations as well as being able to change profiles and authorisations by any one single person based on his rights awarded on the system.	3.6 and 3.7			X	X
Test messages for complete storage in a batch first and not directly processed by the application.	3.6.1.8 and 3.7	X			
Is the ability to modify user master records segregated from the ability to modify profiles and value sets?	3.6.1.8 and 3.7			X	X
Are security administrators appropriately restricted as to which user groups (users groups), profiles (authorisation profiles) and authorisations (authorisations) they are able to work on?	3.6.1.7 and 3.6.1.8			X	X
Is the ability to activate profiles and authorisations segregated from the ability to change profiles and authorisations?	3.6.1.7 and 3.6.1.7			X	X

Table 4.1: Security Audit Program - BC, F1 Modules

Test and inquire to what extent the client makes use of the SAP EDI facilities.	3.6.1.8			X	X
Test the validity and accuracy of the type of messages sent and check whether they contain financial information.	3.6.1.6	X	X	X	
Test the storage of messages, ensuring they are batched first or are they directly processed by the application.	3.6.1.5 and 3.6.1.6		X	X	
Test and inquire whether the sequential control numbers for EDI envelopes are in place and establish if and how a report can be generated and tested.	3.6.1.5 and 3.6.1.7		X	X	
The back of the envelope can also include a control total of the number of messages in the envelope as calculated by the sender and compared by the receiver upon received. Discrepancies can be investigated as agreed upon. Test whether the above control is in place and how management will follow up and review it for accuracy.	3.6.1.6		X	X	
Functional acknowledgement: response sent by the message recipient. However, this does not verify receipt of the envelope contents.	3.6.1.8				X
Application acknowledgement: similar as functional acknowledgement handled by the business application software layer rather than the translation software layer. This acknowledgement can confirm the widgets for the price specified.	3.6 and 3.7				X
Trading partners ID's passwords. Only authorised persons and programs have access to data and they perform specifically identified defined functions. Document the procedures in place ensuring the feature and test the reports generated by the system, regarding access obtained. Test the access paths of trading partners ensuring only access to correct applications are being allowed.	3.6 and 3.7			X	X

Table 4.1: Security Audit Program - BC, F1 Modules

Determine what procedures are in place for message authentication for both parties to confirm the message is genuine without alterations. (The sender's application however needs additional control edits or reasonability checks to detect erroneous transactions). Test the logical procedures identified.	3.6.1.4			X	
A mutually controlled pricing catalogue can control pricing. Regular maintenance and unauthorised changes to be prevented by passwords. Test the price catalogue for price changes and validity of users making the changes.	3.6.1.8 and 3.7			X	
All EDI transactions must be dated and stamped, and unread messages must be investigated. Ascertain whether the message identified is complete and how the reports can be tested. Discuss and follow up the impact on logical procedures by management and perform tests of the logical procedures.	3.6.1.4 and 3.7		X	X	
Test the classifications by testing combination of automated cross-reference tables in place.	3.6.1.3 and 3.7	X	X	X	
Inquire and document whether the software documentation on security is up to date.	3.6.1.3 and 3.7				X
Review computerised logs regarding new software revisions to ensure they are properly tested before they are put into production.	3.6 and 3.7				X
Inquire whether there are advanced automated systems controls in place and whether they are tested regularly.	3.6 and 3.7				X
Test and review computerised logs ensuring general computer controls are tested regularly.	3.6.1.8				X
Inquire as to whether a flow chart of information, in and outside the organisation at the value added networks, has been documented.	3.6 and 3.7				X
Test all program change controls and programs ensuring all changes are complete when implemented.	3.6.1.5 and 3.7				X

Table 4.1: Security Audit Program - BC, F1 Modules

Controls testing instead of substantive procedures: refer general and applications controls programs tailored for SAP R/3.	3.6.1.8 and 3.7			X	
Test the system to ensure there are adequate audit trails or logs in place.	3.6 and 3.7			X	
Obtain the history regarding the module set-up and establish whether it has been properly set up and maintained, and whether the security is intact, by accessing other modules and performing test runs.	3.6.1.8	X	X	X	X
Review all audit trails reports regarding logical access controls generated by the system. Regarding the Internet transactions, review the firewall that has been put in place as well as the local controls put in place.	3.6.1.8			X	X
Review the traffic log of unauthorised network traffic filtered out to establish any network attacks to the BC system.	3.6.1.8			X	X
Test the repository and screening system within SAP R/3 via test data, ensuring it operates effectively.	3.6.1.8			X	X
Regarding Internet transactions to be processed by the BC and FI modules, review the policies and procedures in place ensuring interception and compromise are compromised.	3.6.1.3 and 3.6.1.4			X	X
Regarding Internet transactions to be processed by the BC and FI modules, review the policies and procedures in place ensuring performance links are maintained and corruption and destruction are compromised.	3.6.1.3 and 3.6.1.4			X	X
Regarding Internet transactions to be processed by the BC and FI modules, review the policies and procedures in place ensuring proper encryption procedures are in place through testing via test data.	3.6.1.3 and 3.6.1.4	X	X	X	

Table 4.1: Security Audit Program - BC, F1 Modules

Interface of BC and FI modules: ensure and test that responsibility of daily management is properly defined and privacy is maintained.	3.6.1.6				X
Interface of BC and FI modules: ensure and test that error correction procedures are timeous and review log for correcting errors is maintained.	3.6.1.8				X
Interface of BC and FI modules: ensure and test that sender system audit trails are properly established and reviewed.	3.6 and 3.7			X	X
Interface of BC and FI modules: ensure proper auditing and archiving policy are in place (all).	3.6 and 3.7			X	X
Interface of BC and FI modules: ensure the procedures ensuring the profiles between the regions and branches are all current.	3.6 and 3.7				X
Interface of BC and FI modules: ensure by test posting entries to an old account that it is actually not possible.	3.6 and 3.7				X
Interface of BC and FI modules: ensure database corruption is followed up and timeously corrected, ensure policies are in place.	3.6 and 3.7				X
Interface of BC and FI modules: ensure payment terms on the FI module are in agreement master file. Review master file changes and verification of the payments processed.	3.6 and 3.7			X	
SAP archiving of BC and FI modules: test whether up to date. Review the procedures regarding identification audit status and utility.	3.6.1.4		X	X	
SAP archiving of BC and FI modules: test whether up to date and complete.	3.6.1.5	X			X

4.3 Conclusion

The security audit program forms the base of all tests to be conducted. If correctly used it will be a good guide in assessing the security features of the basis system and financial accounting system modules in any operation.

CHAPTER 5

CONCLUSION

CONTENTS PAGE

5.1	Introduction	85
5.2	Further areas for research	86
5.3	Conclusion	87

CHAPTER 5

CONCLUSION

5.1 Introduction

The SAP R/3 system has a far more comprehensive list of security features that can be implemented. If correctly implemented, the security features will result in a secure environment that will ensure the proper functionality of the system.

The security audit program compiled has identified key issues. However, the external auditor must ensure that these issues exist. For the planning of each specific industry, the audit methodology must be altered and tailored to ensure that there is no negative impact on the audit opinion.

It has further been established that the external auditor can cope with the changes in this technology environment if he ensures that a self-training program is sustained to maintain and update the knowledge of SAP R/3.

The security developed will be a good starting point in establishing the required understanding of the security features in place in the SAP R/3 modules relating to the BC and FI modules. These are the most important modules from an external auditor's point of view.

5.2 Further areas for research

- Detailed security study of all Modules regarding the security features that are specifically required within the modules;
- Study fields regarding the physical access controls in this global environment;
- Results of security features tested and the evaluations and listing of the most important security features for a business;
- Benchmarking security features against other IT practises;
- Cost study of the implementation of the above security features measured against the return of investment;
- The effectiveness of the security features compared to the benefits obtained;
- Initial costs and running costs of maintaining the set security features from an external auditor's point of view and from the client's point of view;
- Critical success factors of the security system, updating the system, as well as the cost implications based on the changing IT environment;
- Who to involve in the security features analysis; and
- Linking of business drivers with IT technology and security features within SAP R/3 and what modules to be implemented in what sequence.

5.3 Conclusion

The objective of the dissertation has been met. Problems and issues identified have been included in the security developed. New areas for academic research have been opened up and the security developed is a proper guide for the external auditor.

BIBLIOGRAPHY

ANON. 1997: Business Day

CAPON, N 1997: Business process re-engineering. [Online]. Available URL address: http://www.abi.inform.

COOPERS & LYBRANDT 1997: Internet audit guide: Report. U.S.A.:Coopers & Lybrandt.

COOPERS & LYBRANDT 1994: Windows NT 3.5 Guidelines for security audit and control. (A joint research project by Citibank N. A, Coopers & Lybrandt, The Institute of internal auditors and Microsoft Corporation).

DA CONSULTING 1996: Overview of SAP transactions: Report. Benmore: DA Consulting.

DELOITTE & TOUCHE 1997: SAP basis system environment assessment guide (For SAP R/3 version 3 systems): Report. Johannesburg:Deloitte & Touche.

DELOITTE & TOUCHE and SAP SA: Joint seminar SAP R/3 and business process re-engineering. (6 October, 1994: Johannesburg).

ERNST & YOUNG 1995a: Audit control and security features of SAP R/3:Report. Ernst & Young International Limited.

ERNST & YOUNG 1995b: Audit control and security features of SAP R/2: Report. Ernst & Young International Limited.

ERNST & YOUNG 1996: The solution SAP:Report. United States of America: Ernst & Young.

ERNST & YOUNG 1997a: Introduction to auditing electronic data interchange: Report. Johannesburg:Ernst & Young.

ERNST & YOUNG 1997b: R/3 System:Report. United States of America:Ernst & Young.

ERNST & YOUNG 1997c: The solution:Report. United States of America:Ernst & Young.

LUBBE, J 1995: A value-for-money audit approach to LANs, with specific reference to Novell NetWare. Johannesburg:Rand Afrikaans University. (M.Com. (Computer Auditing) Short Dissertation).

PRIEST, A 1997: SAP R/3 report provides control answers organisations the world over are seeking available. [Online]. Available URL address:http://www.rutgers.edu/Accounting/raw/iia/sapr3_pr.htm.

SAP 1993: Annual Report, March 16, 1994. Walldorf:SAP.

SAP 1994: Annual Report. March 16, 1995. Walldorf:SAP.

SAP 1997a: The R/3 System. Internal publication. Johannesburg:SAP.

SAP August 1994: SAP Info. Magazine of SAP Group. Walldorf:SAP.

SAP 1997b: R/3 System, SAP AG. Walldorf:SAP.

SAPPHIRE INTERNATIONAL 1994: Access the information highway. Walt Disney World Dolphin, Walt Disney World Swan. Florida:Sapphire International.

SAP EXPO 97: Integrated Systems and Business Strategies for the 21st Century. SBS Conference, April 97.

VAN RENSBURG, R 1992: Auditing EDI Book. Internal correspondence. Johannesburg:Ernst & Young.