CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

Informatics

Department of Information Engineering

Diploma Thesis

Auditing and Testing Business Information Systems

Author: Lucia HASA

Supervisor: doc. Ing. Vojtěch Merunka, Ph.D.

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Department of Information Engineering

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Hasa Lucia

Informatics

Thesis title

Auditing and Testing of Business Information Systems

Objectives of thesis

The goal of this study is to introduce a set of standard techniques for auditing information systems. This will help auditors who most of the times come from non-IT profile. It is very important for an IS auditor to have IT and auditing (business) knowledge to bridge the gap between IT and auditing professions. The idea is to go through introducing the IS Auditing concept, IS Audit procedures, IS Audit techniques and standards, understanding the business needs and processes, understanding the information system (that will be implemented or that is already in place), the information system data flow and data structure and then map all them in and auditing IS project, in a prototype information system such as ERP.

Methodology

Methodology is based on the study and analysis of resources to be used for the study. An implementation of IS Audit approach based on the material introduced will be formulated. Also an IS Audit knowledge and culture survey will be analysed in order to confirm the accuracy and the completeness of the existing theories, techniques and standard introduced in the first part of the research.

The proposed extent of the thesis
60-80 pages

Keywords
Information System, Audit, IS Audit, Risk Analysis, IS Controls, ERP

Recommended information sources

ISACA. 2013. CISA Review Manual. Rolling Meadows, Ill : ISACA, 2013. 160420303005.
Information System Auditing . 2005. Robert E.Davis.
Musaji, Yusufali F. 2002. Integrated Auditing of ERP Systems. 2002.
E.Davis, Robert. 2005. IT Auditing: An adaptive process. Pleier Coporation : s.n., 2005.

The Diploma Thesis Supervisor
Merunka Vojtěch, doc. Ing., Ph.D.

Last date for the submission
March 2014

Electronic approval: March 25. 2014

Ing. Martin Pelikán, Ph.D.
Head of the Department

Electronic apporoval: March 25. 2014

Ing. Martin Pelikán, Ph.D.
Dean

Declaration

I declare that I have worked on my diploma thesis titled "Auditing and Testing Business Information Systems" by myself and I have used only the sources mentioned at the end of the thesis.

In Prague, ...

.....

Lucia Hasa

Acknowledgement

I would like to thank doc. Ing. Vojtěch Merunka, Ph.D. for his advices and supervision of my diploma thesis.

Auditing and Testing Business Information Systems

Audit a testování obchodních informačních systémů

Auditing and Testing Business Information Systems

Summary

The goal of this study is to introduce a set of standard techniques for auditing information systems. This will help auditors who most of the times come from non IT profile. It is very important for an IS auditor to have IT and auditing (business) knowledge to bridge the gap between IT and auditing professions. The idea is to go through introducing the IS auditing concept, IS audit procedures, IS audit techniques and standards, understanding the business needs and processes, understanding the information system (that will be implemented or that is already in place), the information system data flow and data structure.

Keywords

Information system, Audit, IS Audit, Risk Analysis, IS Controls, ERP

Audit a testování obchodních informačních systémů

Souhrn

Cílem této studie je představit sadu standardních postupů pro audit informačních systémů, která pomůže auditorům ve většině případů pocházejících z jiné oblasti než IT. Pro auditora informačních systémů je velmi důležité mít znalosti jak z oblasti IT, tak z oblasti podnikové (obchodní), aby dokázal překlenout mezeru mezi těmito dvěma obory. Cílem této práce bylo představení samotného konceptu IT auditu, jeho jednotlivé procedury, techniky, standardy, porozumění obchodních potřeb a procesů a informačních systémů (nově vznikajících - před samotnou implementací, či již fungujících), toky dat a jejich struktury v IS.

Klíčová slova

Informační systém, Audit, Analýza rizik, Kontrola IS, ERP

Contents

Auditing and Testing Business Information Systems 7
Summary 7
Keywords 7
Audit a testování obchodních informačních systémů 8
Souhrn 8
Klíčová slova 8
Contents 9
Tables List 10
Figures List 11
1 Introduction 12
1.1 Research Introduction 12
1.2 Research Background 13
2 Research Objectives 15
2.1 Objectives and Goal 15
2.2 Research Method 16
2.3 Outline of the Chapters 17
2.4 Scope and Limitations 18
3 IS Audit 19
3.1 Introduction 19
3.2 IS Audit Definition 19
3.3 Elements of IS Audit 21
3.4 Risk Analysis 22
3.4.1 Risk-based Approach 23
3.4.2 IS Controls 24
3.5 IS Auditor 26
3.6 Computer Assisted Audit Techniques (CAAT) 29
3.7 IS Audit Process 30
3.8 IS Audit Standards 35
3.8.1 ISACA (Information Systems Audit and Control Association) 35
3.8.2 ISO 27001 (Information Security Management-Specification with Guidance for Use) 36

3.8.3 IIA (The Institute of Internal Auditors) 37
3.8.4 ITIL (IT Infrastructure Library) 38
3.8.5 Control objectives for Information related Technology (COBIT) 38
4 ERP Audit 40
4.1 Project 40
4.1.1 Introduction 40
4.1.2 ERP Audit Phases 42
4.1.3 Risk Analyses 43
4.1.4 Controls 44
4.1.5 ERP System Development Life Cycle (SDLC) 46
4.2 Analytical Part: IS Audit Survey 56
4.2.1 Introduction 56
4.2.2 Descriptive Analysis 57
4.2.3 Analysis of hypotheses 63
4.2.4 Survey Conclusions 66
5 Conclusion 67
Bibliography 69
APPENDIX 71
Questionnaire - Interview Questions 71

Tables List

Table 1 - Chapter Outline [Author] 17
Table 2 - Control Classifications (ISACA, 2013) 25
Table 3 - IS Auditor Profile (An Information Sytem Auditor's Profile, 2006) 28
Table 4 – ISACA phases [resource] 34
Table 5 – IS audit standards [resource] 36
Table 6 – ERP SDLC (Musaji, 2002) 48
Table 7 - Author's field survey: Background [Author] 57
Table 8 - Author's field survey: Job Title [Author] 58
Table 9 - Author's field survey: Number of times included in an IS Auditing Project [Author] 59
Table 10 - Author's field survey: Education or background for an IS auditor [Author] 59
Table 11 - Author's field survey: Knowledge expected from an IS auditor with regards to IT concepts [Author] 60
Table 12 - Author's field survey: Does your company have an IS Audit Plan? [Author] 60
Table 13 - Author's field survey: Does your company comply with any auditing standards, guidelines or frameworks? [Author] 61

Table 14 - Author's field survey: Which activities from the below list are responsible for IS Audit? [Author] 61
Table 15 - Author's field survey: What Information Technology tools and techniques (CAATs) does your company use to help meet audit objectives? [Author] 62
Table 16 - Author's field survey: Do you have any qualification in IS Auditing? [Author] 62
Table 17 - Author's field survey: Does your company have the right tools and skills to perform an IS Audit? [Author] 63
Table 18 - Author's field survey: Background by Responsible activities of an IS auditor [Author] 64
Table 19 - Author's field survey: Chi-Square Tests - Background [Author] 64
Table 20 - Author's field survey: Number of times involved in IS audit by Relevant education or background [Author] 65
Table 21 - Author's field survey: Chi-Square Tests - Number of times [Author] 65
Table 22 - Author's field survey: Chi-Square Tests - Knowledge [Author] 66

Figures List

Figure 1 - Information System [audit.wa.gov.au] 13
Figure 2 - IS Audit Elements (Musaji, 2002) 22
Figure 3 – Audit Risk Based Audit Approach (ISACA, 2013) 24
Figure 4 – IS Audit Profession (An Information Sytem Auditor's Profile, 2006) 26
Figure 5 – Usual auditing process [Author] 32
Figure 6 – ERP modules [Institute of chartered accountants, 2010] 40
Figure 7 – ERP systems [resource] 41
Figure 8 – ERP systems audit [resource] 42

1 Introduction

1.1 Research Introduction

One of the most important assets of any organization is its information. Information systems and the digital technology had made a dramatic change in the way how we live and as result the way how we do and drive business. The companies are increasingly using computers to create, store and transmit their information. Nowadays in computer information systems most of the business processes are automated so they do not only record business transactions, but actually drive the key business processes of it. Companies are completely dependent on computerized information system making them the lifeblood of any large business. This new way of making business brings the need to be sure that the information is available all the time, is accurate, reliable and only authorized people (devices or processes) can access it.

Generally the more complex the business and the environment in which it operate, the more business risks increase. The enterprises are using their information systems to manage their huge amount of data. For many companies information systems such as ERP, WMS, CRM have become the basic tool on which the company has to rely on. In this case information systems improve the company business on one side but bring a lot of risks in the other side, in such a scenario, senior management and business managers do have concerns about information systems. This is why the IS auditing has become a key component in corporate governance.

The goal of this study is to introduce a set of standard techniques for auditing information systems. This will help auditors who most of the times come from non-IT profile and also the IT people who have only technological background. It is very important for an IS auditor to have both, IT and auditing knowledge to bridge the gap between IT and auditing professions.

The idea is to go through introducing the IS Auditing concept, IS Audit procedures, IS Audit techniques and standards, understanding the business needs and processes, understanding the information system (that will be implemented or that is already in place), the information system data flow and data structure and then map all them in and auditing IS project, in a prototype information system such as ERP.

1.2 Research Background

A system can be defined as a set of elements that operates together to accomplish a purpose or a goal. Also an information system is a system where the elements are people, hardware, software , procedures and data and the goal would be providing accurate information, available all the time and accessible only by authorized people.

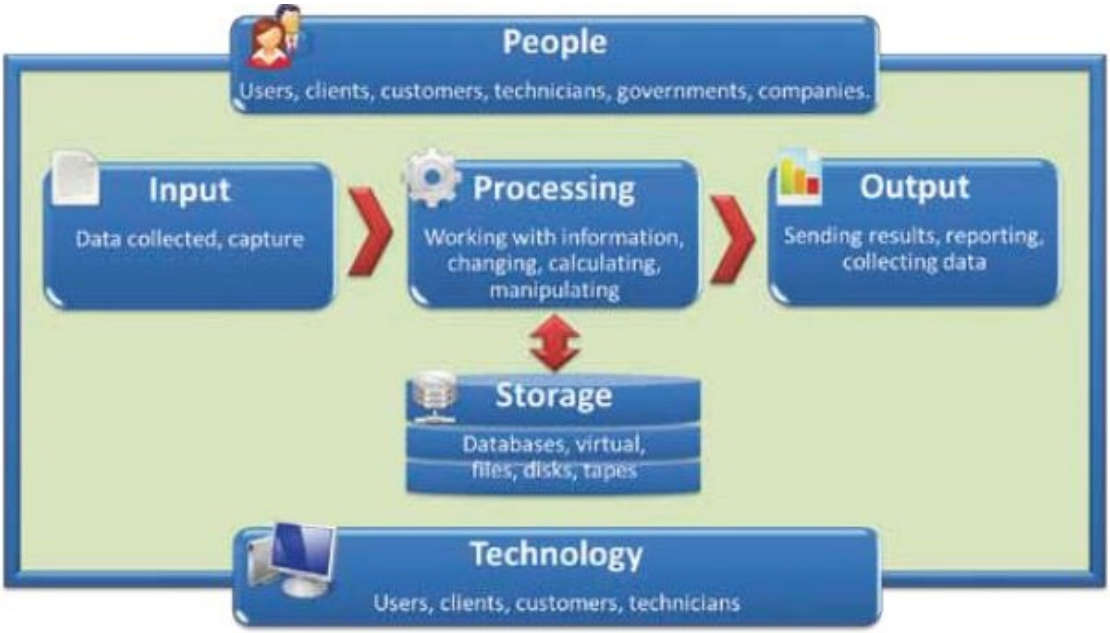

Figure 1 - Information System [audit.wa.gov.au]

"*Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision*". (Davis, et al., 1985)

As mentioned before, companies are completely dependent on computerized information system making them the lifeblood of any large business. They not only store data but they drive the business. Information helps companies in:

- Effective decision-making
- Controlling their functionalities or processes.
- Surviving in a competitive environment
- Right decision at the right time
- Innovative ideas for solving critical problems

In such a situation the managers do have concerns whether the information systems and related resources are reliable. The following typical questions arose from this:

- How to be sure that the information system is adequately safeguarding their assets?
- Is their information system maintaining data and system integrity and availability?
- Does it provide relevant and reliable information to achieve organizational goals effectively?
- Does it have internal controls that provide reasonable assurance that the business, operational and control objectives will be met?
- Does it have internal controls insure that undesired events will be prevented, or detected and corrected, in a timely manner?
- Does it consume resources efficiently?
- Who will be a good candidate to perform IS audit assignments, someone with an IT or an audit background?
- What IS audit tools and techniques are used in assisting IS auditors to perform?
- IS audit evaluations and assessments?
- Which is controlling all the above issues?

The main concerns that a company can have for its information system can be grouped:

1. *Availability*: Will the information systems on which the business is heavily dependent be available for the business at all times when required?

2. *Confidentiality*: Will the information in the systems be disclosed only to those who have a need to see and use it and not to anyone else?

3. *Integrity*: Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to the data or the software in the systems?

2 Research Objectives

2.1 Objectives and Goal

The goal of this study is to introduce a set of standard techniques for auditing information systems. This will help auditors who most of the times come from non-IT profile. It is very important for an IS auditor to have IT and auditing (business) knowledge to bridge the gap between IT and auditing professions.

Derived from the above questions the major objectives of this research are to:

- Define what is an IS Audit.
- Describe an IS audit assignment and the steps in performing and IS audit assignment.
- Reduce the semantic gap between audit and information system.
- Describe the role and the responsibilities of and IS Auditor, IT and audit (business) knowledge required to successfully perform and IS Audit.
- Construct a relationship between IS Audit and system analysis and system design documents.
- Introduce the main audit standards and techniques used more often to assist in IS.

The final purpose is to map and structure all this information to conduct an audit IS assignment in a business which already has in place or is considering implementing an ERP system.

Also a study will be performed based on survey. The aim of this survey is to study IS Audit knowledge and to confirm the accuracy and the completeness of the existing theories, techniques and standard introduced in the first part of the research.

2.2 Research Method

The process of this research will be divided into three parts:

In the first part in order to be able to introduce IS Audit concept, IS Audit assignment and techniques, a construction research method will be conducted. ” A construction research method is the structural framework linking a number of concepts into a much more comprehensive concept, mega-concept, of a phenomenon that is not directly observable or measurable”. (Page, et al., 2000). A review of results of the existing literature regarding IS Audit will be introduced in order to set the direction of the research. Available online database of ISACA (Information Systems Audit and Control Association) as well as published articles, relevant textbooks and Internet will be used to conduct the literature review.

In the second part an implementation of IS Audit approach into a real system will be done in order to prove that the mechanism is feasible.

In the third part of the study an IS Audit knowledge and culture survey will be analysed. The selection of the population will be based on judgmental samples. “Judgmental sample consist on respondent who, in the judgment of the researcher, will best supply the necessary information” (Page, et al., 2000) . In order to be able to get the needed information it will need to rely on interviewers that has at least been part of an IS Audit assignment. The population will be selected based on background (IT or Auditing) and experience in IS Auditing. The aim of this survey is to confirm the accuracy and the completeness of the existing theories, techniques and standard introduced in the first part of the research.

2.3 Outline of the Chapters

CHAPTER OUTLINE	DESCRIPTIONS
Chapter 1	Introduction Introduction to the research, a description of the significance of the study, the methodology used and the structure of the research study.
Chapter 2	Research Objectives In this chapter the research background will be described, identify questions and research methods of this research.
Chapter 3	IS Audit Part of this chapter will be a collective references of IS Audit, IS Audit process, IS Auditor, IS Audit Standards, Risk Analysis and IS Standards.
Chapter 4	ERP Audit In this chapter an implementation of IS Audit approach into a real system will be done in order to prove that the mechanism is feasible.
Chapter 5	Survey In this chapter an IS Audit knowledge and culture survey will be analysed.
Chapter 6	Conclusion Outline the summary of the conclusions and suggest area for future research.

Table 1 - Chapter Outline [Author]

2.4 Scope and Limitations

IS auditing is a new field and the main scope of this research is to provide a framework bridging the gap between auditing and IT. The scope is providing an IS Audit body of knowledge which will specify the main skills and knowledge needed to understand the concepts and demands from both sides (IT and audit) to successfully execute and IS audit assignment. We will introduce a general framework because there is impossible to have a unique framework used in different IS Audit assignment. The way how to perform and IS Audit assignment depends on IS, type of business goal, time , cost etc.

3 IS Audit

"While creativity and innovation are what drive new technology, they are also what must secure it." (Champlain, 2003)

Jack J. Champlain

3.1 Introduction

Enterprises are using their information systems to manage their huge amount of data. For many companies their information systems are the basic tool on which the company has to rely on. In this case information systems improve the company business on one side but bring a lot of risks in the other side, in such a scenario, senior management and business managers do have concerns about information systems. This is why the IS auditing has become a key component in corporate governance.

A review of the existing literature regarding IS Audit will be introduced in order to set the background for this research. This literature review will help to understand IS Audit concept and to define the framework, the aim of which is to bridge somehow the gap between IT and audit. In order to achieve this we will go through IS Audit definition, IS Audit process, techniques, tools (CAAT) knowledge, responsibilities and well known standards.

3.2 IS Audit Definition

"*Auditing can be defined as a systematic process by which a qualified and team or person objectively obtains and evaluates evidences regarding assertions about a process for the purpose of forming an opinion about and reporting on the degree to which the assertion is implemented*." (ISACA, 2013)

IS auditing is one type of general auditing which is focused on IS governance, IS controls and risks. It is focused in how the IS systems works, including here SDLC (system development life cycle) IS design, IS developing, IS configuration , IS testing, IS implementing , IS using , IS management and maintenance.

There is no single definition for IS Audit. Below will listed some of the definition from different sources.

"*IS audit can be defined as any audit that encompasses review and evaluation (wholly or partly) of automated information processing, related no automated process and the interfaces between them*." (ISACA, 2013)

"*IS Audit is the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently*." (Weber, 1988)

"*The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole."* (Institute of Charted Accounts, 2010)

"*The independent examination of records and other information in order to form an opinion on the integrity of a system of controls and recommend control improvements to limit risks*" (Hinson, 2006)

Performing an IS Audit means evaluating the strength and the weaknesses that a system has and present them together with recommendation for fixing them, in an objective manner. The scope of IS Audit is to insure that IS complies with related enterprise policies or guidelines.

An IS audit is conducted to safeguard and maintain:

- Information System Assets/Resources,
- Data Integrity,
- System Effectiveness,
- System Efficiency

This is done by evaluating the existence and the effectiveness of the IS controls and IS performance, as under.

- Data
- Application systems
- Technology
- Facilities
- People

The Information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas.

3.3 Elements of IS Audit

Today's information systems are complex and have many components which together make a business solution. The Audit of an information system can be obtained by evaluating all components. The major elements of IS audit can be broadly classified:

1. Physical and environmental.
2. Operating System.
3. Security software.
4. Data integrity.
5. IS system

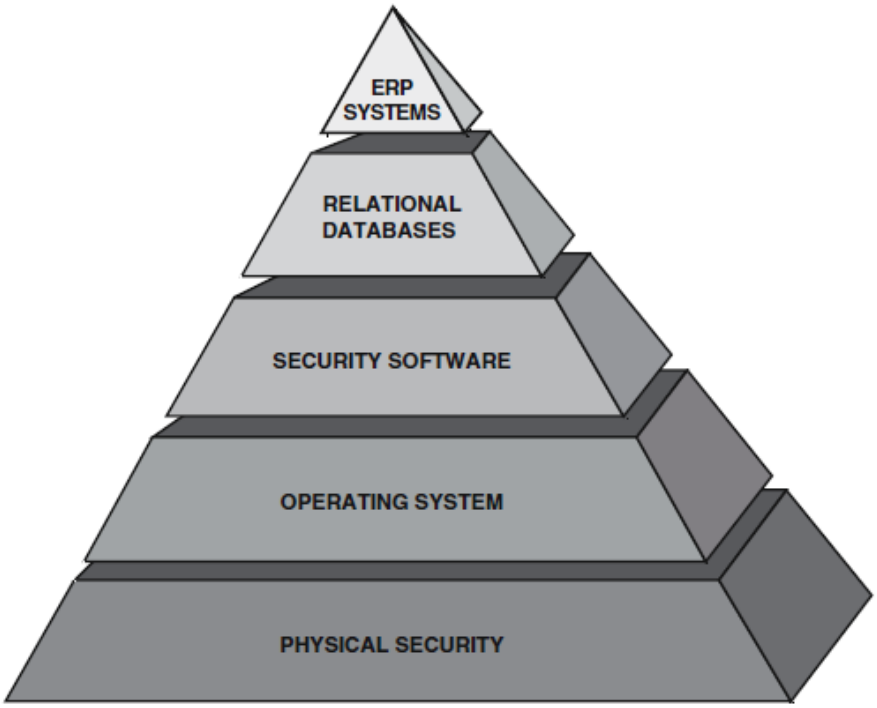

Figure 2 - IS Audit Elements (Musaji, 2002)

In this research we will be focused only in the top of the pyramid, in the last 2 levels.

3.4 Risk Analysis

The use of information systems has benefited enterprises in terms of significantly increased quality and delivery of information but from the other side the widespread use of information technology and the Internet suffers from risks. Management is the primary responsible for establishing, implementing and maintaining a framework and design IT controls to meet the internal control objectives.

The primary question that comes in mind before proceeding to an audit case are what to audit, where and how frequently. The best answer to this is directing our resources where the risk is greatest. That is why having knowledge about business risk and technology risk for an auditor is a must. They should be able to identify the risk and evaluate or suggests controls used to avoid it.

Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. (IEC, ISO, 2011)

3.4.1 Risk-based Approach

More and more organizations are moving to a risk-based audit approach. This approach is used to assess risk and to assist with an IS auditor's decision to do either compliance or substantive testing. Audit risk can be defined as the risk that information may contain a material error that may go undetected during the course of audit.

There is a great amount of information system nowadays in the market, and even if some of them are using the same the way how it was implemented in order to meet business requirement can be different. Each enterprise or parts of enterprises are facing different types of risks. By understanding the nature of the business, identifying business objective, information assets and information systems, IS auditors can identify and categorize the types of the risks that will better determine the risk model or approach in conducting the audit.

After identifying the critical information assets, a risk evaluation is performed. During this risk evaluation are determined threats and the probability that these threats will occur. The next step in this approach will be identifying the controls that will mitigate the identified risk. Identifying the controls does not mean putting them in action. A cost- benefit analysis should be performed in this way a level of acceptable to management will be added next to each risk. In this way the IS auditor can put priorities in the IS Audit process. The analysis can be based on the cost of risk mitigation comparing to the benefits, the level of risk that the company is prepared to accept and the preferred risk mitigation method (terminating, minimizing or transferring the risk).

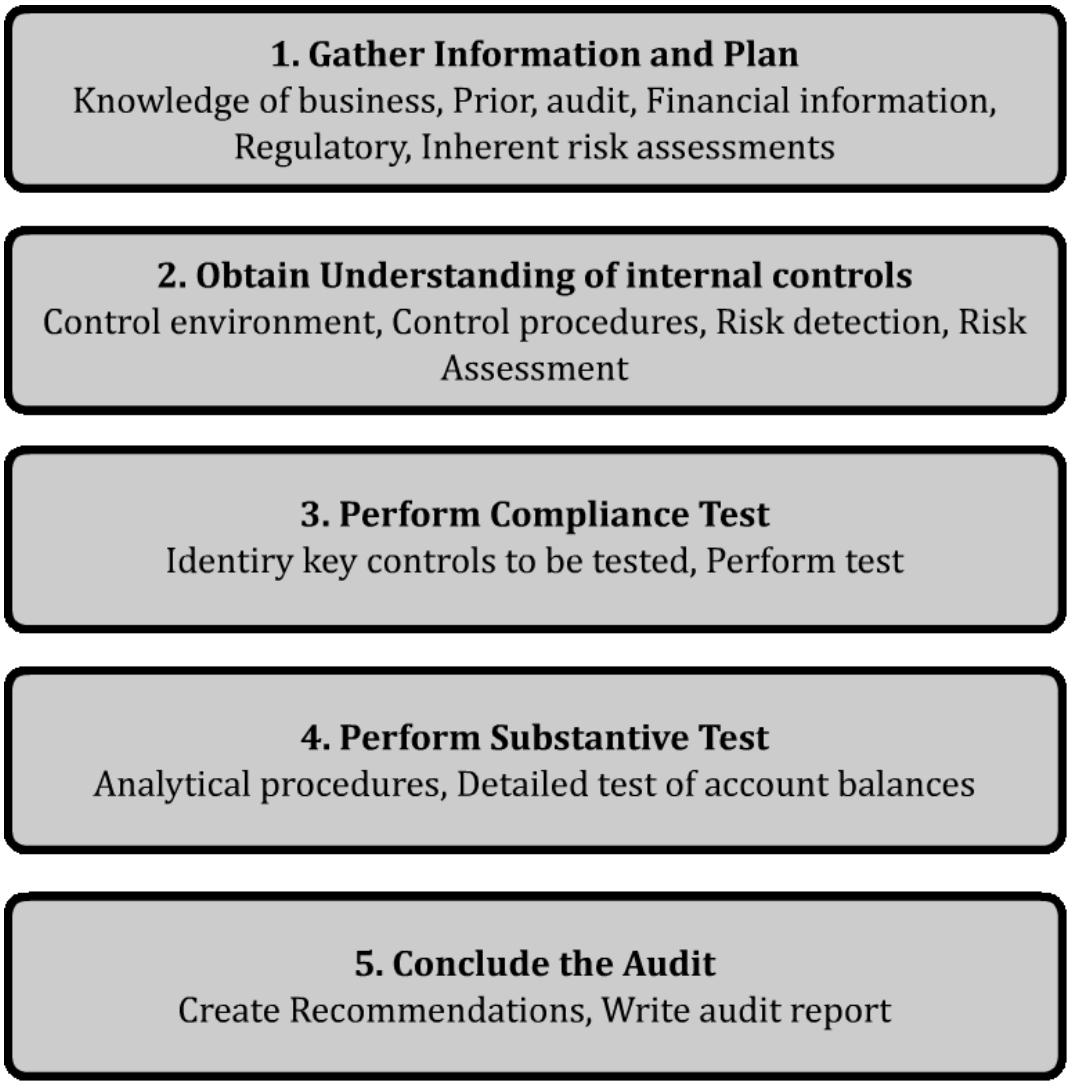

Figure 3 – Audit Risk Based Audit Approach (ISACA, 2013)

3.4.2 IS Controls

Controls are defined as "*The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected*". (ISACA, 2013)

These controls can be manual or automated (driven by automated computer resources). According to ISACA in their yearly publication of CISA review manual controls are classified as preventive, detective and corrective.

In the below table the function and examples for each control classification are defined.

Control Classifications		
Class	Function	Examples
Preventive	Detect problems before they arise. Monitor both operations and inputs. Attempt to predict potential problems before they occur and make adjustments. Prevent and error, omission or malicious act from occurring.	Employ only qualified personnel. Segregate duties. Control access to physical facilities. Use well-designed documents. Establish suitable procedures for authorization of transactions. Complete programmed edit checked. Use access control software that allows only authorized personnel to access sensitive files. Use encryption software to prevent unauthorized disclosure of data.
Detective	Use controls that detect and report the occurrence of an error, omission or malicious act.	Hash totals. Check points in production jobs. Echo controls in telecommunications. Error messages over tape labels. Duplicate checking of calculations. Periodic performance reporting with variances. Past-due accounts reports. Internal audit functions. **Review of activity logs to detect unauthorized access attempts.**
Corrective	Minimize the impact of threat. Remedy problems discovered by detective controls. Identify the cause of the problem. Correct errors arising from a problem. Modify the processing system(s) to minimize future occurrences of the problem.	Contingency planning. Backup procedures. Rerun procedures.

Table 2 - Control Classifications (ISACA, 2013)

This was a summary of introduction to IS controls; ISACA has published also a leading framework for governance, control and assurance for information and related technology. This leading control framework is called COBIT (Control Objective for Information and related Technology and will be introduce later in the IS Audit standards (2.8 IS Audit Standards).

3.5 IS Auditor

The increasing use of information system changed not only the way how we are doing business but also the way of auditing them, as result the audit profession has changed also.

"The use of computers in business Information Systems has fundamental effects on the nature of business transactions, the procedures followed, the risks incurred, and the method of mitigating those risks". (GLEIM, 2004)

Two professions need to be integrated into a profession, relying on the knowledge, skills, expertise and experience from both the audit and IT professionals

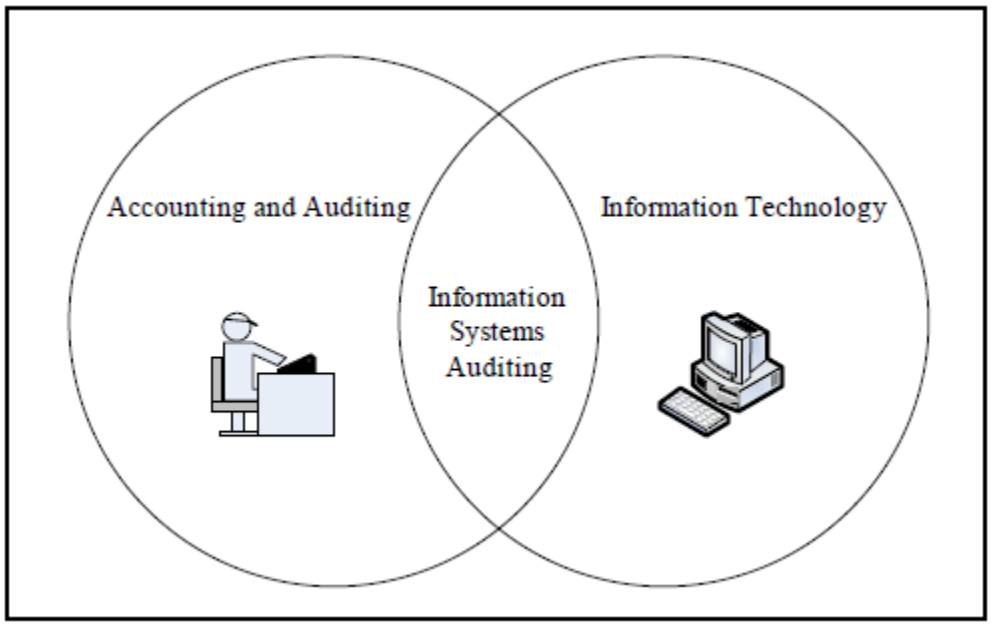

Figure 4 – IS Audit Profession (An Information Sytem Auditor's Profile, 2006)

Defining the roles and responsibilities of an IS Auditor is one of the key steps in the direction of a successful IS Audit assignment. In order to perform an IS audit through the defined roles and responsibilities, IT and audit knowledge are required, IS audit tools and techniques are required to enable and assist the IS auditor to perform these responsibilities and a certain set of soft skills are needed to drive the successful completion of the audit. (An Information Sytem Auditor's Profile, 2006)

IS auditors are therefore faced with the challenge of being involved in the planning and organising of IT projects, implementation of proposed solutions, delivery and support of Information Systems and the monitoring of the process, the controls, assurance and evaluation. (Kimpton, et al., 2001)

Carol listed the above mentioned in here research in defining a IS Auditor Profile

<table>
<tr><td colspan="2">Skills</td></tr>
<tr><td colspan="2">Analytical / systematic
People's person / people knowledge
Communication skills
Project Management (Managing people, resources, time and budgets (leadership))
Good listener
Passion for auditing
Understand client environment / business
Team player
Conflict resolution
Constant learning
See the "bigger picture"
Strength of character</td></tr>
<tr><td>Audit Knowledge</td><td>IT Knowledge</td></tr>
<tr><td>Understanding of the concept of risk;
Knowledge about applicable standards and best practices;
Audit planning;
Audit testing methods;
Understanding of the concept of control;
Understand basic accounting principles;
Business understanding;
Obtaining and interpreting relevant audit evidence; and
Independence.</td><td>Application programs / ERP systems;
Basic Information Systems and information;
Technology general concepts;
Programming languages and procedures;
Computer communications and networks;
Data structures and databases;
Information security;
Information System Management / IT Governance;
Operating Systems;
System analysis, design, development, testing, implementation and maintenance (SDLC);
Business Continuity and Disaster Recovery planning;
Information Systems Operations; and
Specialized areas.</td></tr>
<tr><td colspan="2">Generalized audit software;
Specialized analysis tools;
Audit methodologies, standards, guidelines and audit programs;
General applications.</td></tr>
</table>

Table 3 - IS Auditor Profile (An Information Sytem Auditor's Profile, 2006)

3.6 Computer Assisted Audit Techniques (CAAT)

"*CAATs are tools/utilities to help auditors select,gather, analyse and report audit findings*". (Hinson, 2006)

As entities increase the use of information systems to record, transact and process data, the need for the IS auditor to utilise IS tools to adequately assess risk becomes an integral part of audit coverage. The use of computer-assisted audit techniques (CAATs) serves as an important tool for the IS auditor to evaluate the control environment in an efficient and effective manner. The use of CAATs can lead to increased audit coverage, more thorough and consistent analysis of data, and reduction in risk.

CAATs include many types of tools and techniques, such as generalised audit software, customised queries or scripts, utility software, software tracing and mapping, and audit expert systems.

CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Penetration testing

CAATs may produce a large proportion of the audit evidence developed on IS audits and, as a result, the IS auditor should carefully plan for and exhibit due professional care in the use of CAATs.

IS audit tools and techniques, currently available, fall into the following main categories:

- *Generalised audit software* (GAS) (ACL, IDEA, Microsoft Excel, SQL queries)
- *Security analysis tools*: These tools are used to assist in auditing auditor of security settings of operating systems and networking.
- *Application analysis tools* (used to ensure that proper validation and controls are implemented at application or database level);

- *Audit Methodologies* (assisting the auditor in all areas of the audit by means of evaluating organisational controls against control objectives, audit guidelines and best practices); and
- *General applications* (includes document management and planning management and enabling the auditor to create work papers, reports and other relevant documentation e.g. Microsoft word, Microsoft projects).

Examples of such tools are ACL (Audit Command Language), IDEA (Interactive Data Extraction and Analysis), Microsoft Excel and SQL queries. Hinson (2006:18) further elaborates and states that "information security applications such as intrusion detection systems, penetration testing and vulnerability assessment tools could also be considered CAATs since they can be used by auditors to find information security control weaknesses".

3.7 IS Audit Process

In order to perform an IS audit the adequate knowledge and planning are very important. The audit process requires the IS auditor to gather evidence, evaluate the strengths and weakness of controls based upon the evidence gathered through audit tests and prepare and audit report that presents those issues in an objective manner. In this process the auditor collects and evaluates evidences to determine whether the information systems and related resources adequately safeguard assets, maintain data and system integrity and availability, provide relevant and reliable information, achieve organizational goals effectively, consume resources efficiently, and have internal controls that provide reasonable assurance that the business, operational and control objectives will be met and that undesired events will be prevented, or detected an corrected, in a timely manner.

An audit does not fellow or has a specific number of steps but as minimum it will perform in such a way in order to gain an understanding of the entity that is being audited, to evaluate and test the control structure.

The main activities during an IS Audit may include one or both of the following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency.

The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilisation of resources).

Different audit organizations go about IT auditing in different ways and individual auditors have their own favourite ways of working. It can be categorized into six stages:

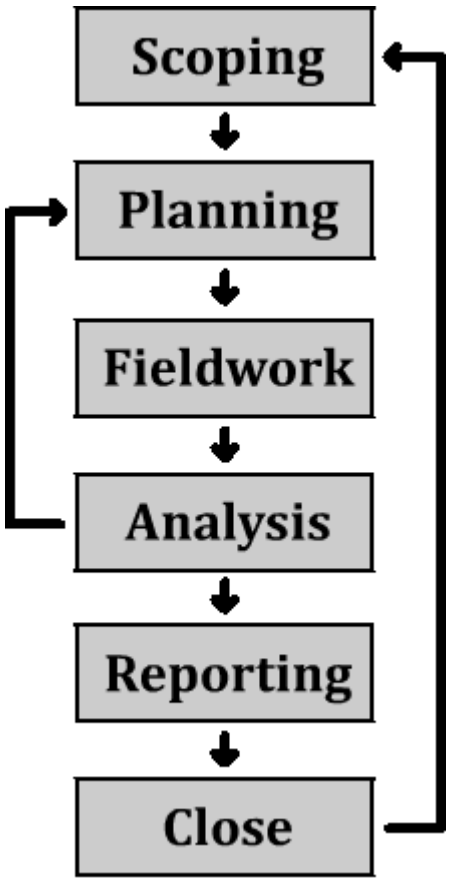

Figure 5 – Usual auditing process [Author]

Scoping and pre-audit survey: The auditors determine the main areas to focus based normally on some form of risk-based assessment.

Planning and preparation :During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

Fieldwork: Information like background, previous audit reports, interviewing staff and managers, reviewing documents, printouts and data, observing processes are use in this phase.

Analysis: This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, and Treats) or PEST (Political, Economic, Social, and Technological) techniques can be used for analysis.

Reporting: Reporting to the management is done after analysis of data gathered and analysis.

Closure: In this phase notes for future audits and following –up management to complete the actions needed to performed after the audit assignment.

The default audit phases according to ISACA in CISA (Certified Information System Auditor) are:

ISACA – Audit Phases	
Audit Phase	• Description
Audit Subject	• Identify the area to be audited.
Audit Object	• Identify the object of the audit. For example, and objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
Audit Scope	• Identify the specific systems, functions or unit to the organization to be included in the review. For example , in the previous program changes example , the scope statement might limit the review to a single application system or to a limited period of time.
Preaudit Planning	• Identify technical skills and resources needed. • Identify the source of information for test or the review such as functional flow charts, policies, standards, procedures and prior audit work papers. • Identify locations and facilities to be audited
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines to review. • Develop audit tools and methodology to test and verify controls
Procedures for evaluating the test or review results	• Organization –specific.
Procedures for communication with management	• Organization –specific.
Audit report preparation	• Identify follow-up procedures. • Identify procedures to evaluate/ test operational efficiency and effectiveness. • Identify procedures to test controls. • Review and evaluate the soundness of the documents, procedures and policies.

Table 4 – ISACA phases [resource]

3.8 IS Audit Standards

IS auditors need guidance in order to meet needs of performing a professional IS Audit assessment. During the IS Audit process assessment in planning the audit in the best way is needed, identifying and prioritizing risk is needed and in evaluate and assess the severity of errors found.

The objective of IS Audit standards is to approach IS Auditors in their challenge and provide assurance and the skills needed to perform such a process. IS audit standards provide audit professionals a clear idea of the minimum level of acceptable performance in order accomplish their responsibilities effectively .The purpose of this Auditing and Assurance Standard is to establish standards on procedures to be followed when an audit is conducted in a computer information systems environment. ((AAS), 2003)

Bellow we will list well known organizations who have contributed in giving such a frameworks in IS Audit:

3.8.1 ISACA (Information Systems Audit and Control Association)

ISACA (Information Systems Audit and Control Association) is a global leader in information governance, control, security and audit. ISACA developed the following to assist IS auditor while carrying out an IS audit. IS auditing standards:

ISACA issued 17 auditing standards which defines the mandatory requirements for IS auditing and reporting.

Standards for IS Audit and Assurance	Effective Date
1001 Audit Charter	1 November 2013
1002 Organisational Independence	1 November 2013
1003 Professional Independence	1 November 2013
1004 Reasonable Expectation	1 November 2013
1005 Due Professional Care	1 November 2013
1006 Proficiency	1 November 2013
1007 Assertions	1 November 2013
1008 Criteria	1 November 2013
1201 Engagement Planning	1 November 2013
1202 Risk Assessment in Planning	1 November 2013
1203 Performance and Supervision	1 November 2013
1204 Materiality	1 November 2013
1205 Evidence	1 November 2013
1206 Using the Work of Other Experts	1 November 2013
1207 Irregularity and Illegal Acts	1 November 2013
1401 Reporting	1 November 2013
1402 Follow-up Activities	1 November 2013

Table 5 – IS audit standards [resource]

IS auditing guidelines: ISACA issued 42 auditing guidelines which provide a guideline in applying IS auditing standards. IS auditing procedures: ISACA issued 11 IS auditing procedures which provide examples of procedure an IS auditor need to follow while conducting IS audit for complying with IS auditing standards.

3.8.2 ISO 27001 (Information Security Management-Specification with Guidance for Use)

ISO 27001 (Information Security Management-Specification with Guidance for Use) a global standard issued by ISO (The International Organization for Standardization)and IEC (The International Electro technical Commission) in October 2005. It helps to establish and maintain an effective information management system, using a continual improvement approach. It implements OECD (Organization for Economic Cooperation and Development) principles, governing security of information and network systems. ISO/ IEC 27001:2005 is designed to ensure the selection of adequate and proportionate

security controls that protect information assets and give confidence to interested parties. IT helps organizations in identification and clarification of existing information security management, formulating security requirements and objectives, managing security risks in cost effectively manner, to ensure compliance with laws and regulations, to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons and implementation of business-enabling information security.

3.8.3 IIA (The Institute of Internal Auditors)

IIA (The Institute of Internal Auditors) is an international professional association. This association provides dynamic leadership for the global profession of internal auditing. IIA issued Global Technology Audit Guide (GTAG) GTAG provides management of organisation about information technology management, control, and security and IS auditors with guidance on different information technology associated risks and recommended practices. Following is the list of GTAG developed by IIA.

- GTAG 1 : Information Technology Controls
- GTAG 2 : Change and Patch Management Controls : Critical for Organizational Success
- GTAG 3 : Continuous Auditing : Implications for Assurance, Monitoring, and Risk Assessment
- GTAG 4 : Management of IT Auditing
- GTAG 5 : Managing and Auditing Privacy Risks
- GTAG 6 : Managing and Auditing IT Vulnerabilities
- GTAG 7 : Information Technology Outsourcing
- GTAG 8 : Auditing Application Controls
- GTAG 9 : Identity and Access Management.

3.8.4 ITIL (IT Infrastructure Library)

ITIL (IT Infrastructure Library) is the best practice in IT Service Management, developed by OGC and supported by publications, qualifications and an international user group. It gives a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures that can be tailored to any IT organization. ITIL provides a systematic and professional approach to the management for IT services. ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organisations growing dependency on IT and embodies the best practices for IT Service Management. Information System Audit and Control Association (ISACA) has long recognized the importance of information security and control and offers a wide range of products and services on the topic. Most significantly, in 2002 ISACA introduced the Certified Information Security Manager (CISM) certification, recognizing the special role played by those who manage an enterprise's information security program.

3.8.5 Control objectives for Information related Technology (COBIT)

The Information Systems Audit and control Foundation (ISACA) developed the Control Objectives for Information and related Technology (COBIT) COBIT is a framework of generally applicable information systems security and control practices for IT control. The framework allows management to benchmark the security and control practices of IT environments, users of IT services to be assured that adequate security and control exist, and auditors to substantiate their opinions on internal control and to advise on IT security and control matters. The framework addresses the issue of control from three dimensions:

Business Objectives. To satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements for information. The criteria are divided into seven distinct yet overlapping categories that map into the COSO objectives: effectiveness (relevant, pertinent, and timely), efficiency, confidentiality, integrity, availability, compliance with legal requirements, and reliability.

IT resources, while include people, application systems, technology, facilities, and data.

IT processes, which are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession. It is helping managers learn how to balance risk and control investment in an information system environment. It provides users with greater assurance that the security and IT controls provided by internal and third parties are adequate. It guides auditors as they substantiate their opinions and as they provide advice to management on internal controls.

COBIT – IT Governance Model

COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management. The underpinning concept of the COBIT Framework is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes.

4 ERP Audit

4.1 Project

4.1.1 Introduction

Enterprise Resource Planning (ERP) is a solutions that seek to integrates operation processes and information flows in the company. " An ERP system is a fully integrated business management system that integrates the core business and management processes to provide an organization a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable real-time information." (Institute of Charted Accounts, 2010) An ERP system integrates various business processes as shown below:

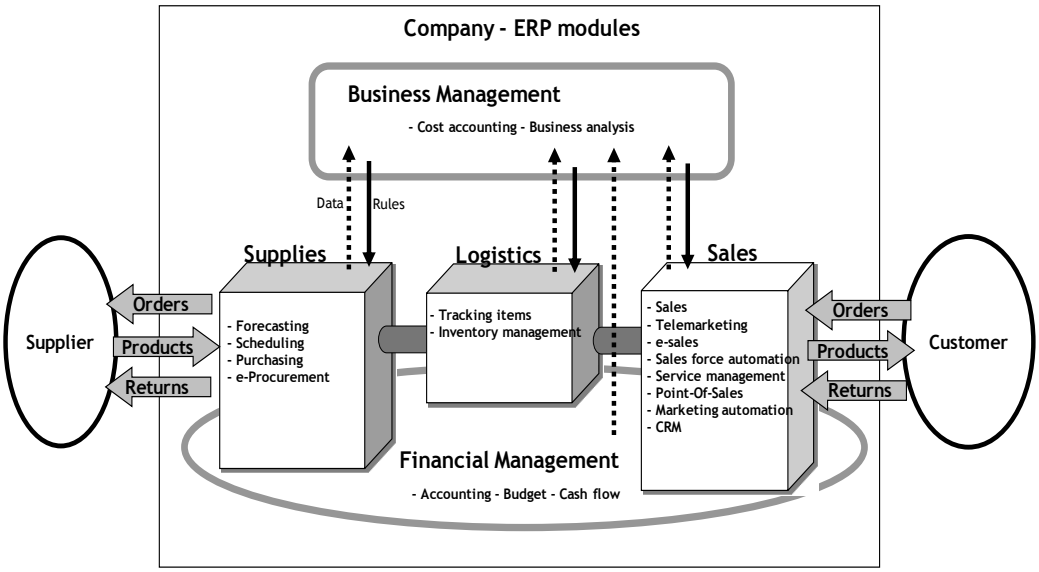

Figure 6 – ERP modules [Institute of chartered accountants, 2010]

ERP system can be thought as the engine that automates the business process of the company. Implementing an ERP system for a company is adopting the best business practice on it, this why in most of the cases the existing business processes are reengineered.

An ERP system avoids managing information flows manually. ERP systems have the capability of integrating virtually all business processes by installation of program

application modules for sales, marketing, accounting, finance, production and materials management, and human resources. (Jacobs, et al., 2002)

ERP systems has a common database for all accounting and operating information instead of working with different data resources as was the case in old fragmented systems. ERPs are usually client-server networks that operate across multiple platforms.

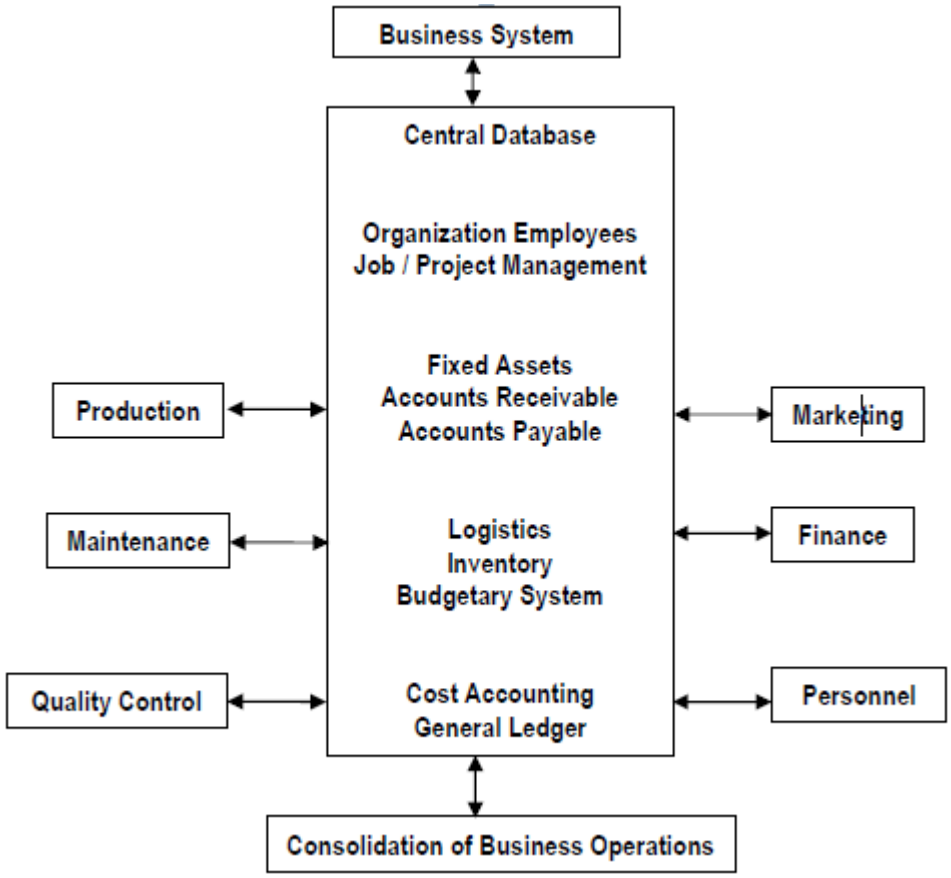

Figure 7 – ERP systems [resource]

This integrated nature of this system has change the way auditing them, the auditors are aware that the approached used till before this systems came along, auditing around the computer is not sufficient. New techniques and knowledge are required to move from auditing around the computer to auditing through and with computer.

The main objectives for the auditors is to understand the business processes and to insure that the ERP system reflect them accurately and effectively.

In this part we will evaluate the audit process in an ERP environment, the risk and

the recommended approaches for controlling it.

Auditing the business process and its internal control will become the focus of the audit.

4.1.2 ERP Audit Phases

Auditing in an ERP can be categorized into:

- Auditing of ERP systems under implementation
- Auditing of operational ERP systems.

Depending in which of this two types of environment the audit is executed a different approaches are used.

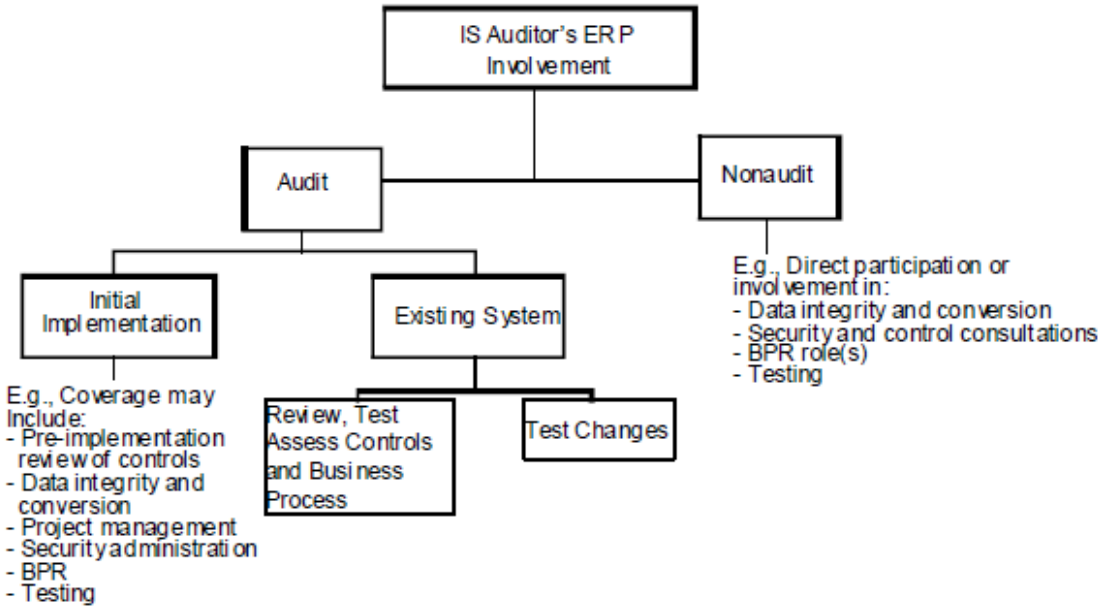

Figure 8 – ERP systems audit [resource]

Auditing of ERP systems under implementation: During the implementation of the ERP system we don't have an operational system in place and as result there are no output data to be analysed or audited. In this phase the auditor become familiar with the business goal, system and base on this evaluates the controls needed without having the processing results. The main goal in this phase is to be sure that all the procedures needed are properly implemented. Vulnerabilities that are identified in this phase are easier to be

avoided than after having implementation.

Auditing of operational ERP systems: Auditing an ERP system in place or operational ERP systems is to evaluates the adequacy and effectiveness of the system and system controls by analysing the operational results. During this phase vulnerabilities can be identified also but it is very costly to fix them. It is 50—100 more expensive and costly to correct them after implementation.

There is no defined method in implementing an information system in our case an ERP system. It will always vary depending on business requirements, costs and time. Audit involvement during the implementation is very important. As we all know changes after the implementation are very difficult, costly on most of the time impossible after ERP implementation. The same logic applies to auditing; retrofitting controls is also difficult and costly after the fact. This is why it is very important that the audit should have an active role during the implementation.

The cost to retrofit controls into a system increases during the progress of the system life cycle. This is the reason why it so important (especially in this type of the system) the implementation approach of the controls. It is very important to evaluate how the controls are addressed, implemented and also documented for future references. Building a healthy system of controls during the ERP implementation leads to a fine tuning of controls in audit operational phase.

4.1.3 Risk Analyses

A risk analysis of an organization's ERP systems, their existing controls, and their vulnerabilities results in the loss potential for the system, with an estimated likelihood of occurrence. This loss potential in damages must be represented in terms of dollar value. A risk analysis of an ERP system performs two important functions: Searches out an ERP system's vulnerabilities and the probabilities of threats materializing to exploit these vulnerabilities. Calculates the damage or loss to its assets that could be produced by the resulting damaging events.

An ERP system environment's vulnerabilities and set of threats should be assessed to arrive at some estimate of possible damaging events. Such an assessment

would also review the strengths of existing controls. A vulnerability assessment is conducted as part of a risk analysis. The vulnerability assessment is a major assessment of the adequacy of an ERP's system. Organizations must first identify vulnerabilities and threats; and then determine whether controls are adequate to reduce the resulting risks to an acceptable level.

The risks in an ERP environment include both those present in a manual processing environment and those that are unique or increased in an ERP environment. The use of ERP systems clearly introduces additional risks into the system environment. These additional risks include problems associated with:

- Improper use of technology.
- Inability to control technology.
- Inability to translate user needs into technical requirements.
- Illogical processing.
- Inability to react quickly (to stop processing).
- Cascading of errors.
- Repetition of errors.
- Incorrect entry of data.
- Concentration of data.
- Inability to substantiate processing.
- Concentration of responsibilities.

For each of this risk the appropriate controls need to be identified and evaluated.

4.1.4 Controls

In this phase main controls and deliverables expected from the system to be fulfilled will be defined. The goal of the controls is to ensure that the ERP system functions have the appropriate controls and security and also that these controls are efficient and effective. This control will define a clear path for the auditor in order to define whether the ERP system is working properly and fulfils the business requirements. Controls can be

different depending the scope of the audit but the main concerns during an ERP implementation can be grouped:

- Transactions are properly authorized (Authorization).
- Transactions are recorded on a timely basis (Timeliness).
- Transactions are accurately processed (Accuracy).
- All existing transactions are recorded (Completeness).
- All recorded transactions are valid (Validity).
- Transactions are properly valued (Valuation).
- Transactions are properly classified and posted to proper accounts and subsidiary records (Classification).
- Transactions are properly summarized and reported (Reporting).
- System and data integrity is maintained (Integrity).
- System availability is assured (Availability).
- System usability is assured (Usability).
- System economy and efficiency are maintained (Efficiency).

Each control objective is met by one or more control techniques. These techniques are the ways and means that management uses to control the operations; they are varied in nature and exist as:

- Procedures and policies.
- Physical controls.
- Segregation of duties.

As was mentioned before an ERP system can be thought as the engine that automates the business process of the company. This automation is realized through an integrated user interface and the integrated database.

ERP systems are not new but achieving a successful implementation is still an issue for most of the companies who are using them. Understanding the system is a key factor in to a successful Audit. We will go through each implementation phase, defining principal participant, key activities and deliverables. This will make easier to understand key system controls in each phase and their implementation. This controls or deliverables will become the framework or the target of audit process.

There is no defined method in implementing an ERP system, it will always vary. Audit involvement during the implementation is very important. As we all know changes after the implementation are very difficult, costly on most of the time impossible after ERP implementation.

Enterprise Resource Planning (ERP) System implementation consists of planning, implementation, and continuous maintenance.

It is very important to understand structured methodologies in the implementation of ERP systems. The basic steps of structured methodologies are:

- *Business Requirements Definitions*. Defining the terms of reference, determining user needs and system constraints, generating a functional specification and a logical model for the best solutions.
- *External Design.* Detailing the design for a selected solution, including diagrams relating all programs, subroutines, and data flow.
- *Internal Design*. Building, testing, installing, and tuning software.
- *Pre-implementation.* Evaluation and acceptance
- *Implementation.* Implementing systems.
- *Post-implementation.* Evaluation of controls and debugging.

4.1.5 ERP System Development Life Cycle (SDLC)

The first step in developing audit assignment is accessing and understanding the data. Experience has shown that the traditional application system ERP (Enterprise Resource Planning) can cover only 30% of the company needs in the first setup and 70% of the work is customization. So the heterogeneity it is not only because of applications are developed in different periods of time and from different vendors but even between the same systems implemented in different businesses.

As result this makes preparing the data for the first time during an audit process faces difficulties no matter the great number of audit software in market.

Preparing the data asks a great amount of knowledge business related and also technical background.

Audit software can access ERP tables directly or use open database connectivity to access ERP and legacy systems. After accessing and understanding the data, auditors can import standard reports into Excel or a similar program. Whether the auditor is using a series of standard reports, a continuous controls monitoring system, or an audit software and computer modelling program, the important thing is to start by understanding the main business systems, key controls, and emerging risk areas from a data perspective.

The System Development Life Cycle (SDLC) framework provides system designers and developers to follow a sequence of activities. Being part of SDLC is crucial for and auditor to understand the business goals, business process and the ERP system.

Audit should also ensure that the organization has followed the structured steps involved in implementation of an ERP, such as Project Planning, Business & Operational analysis, Business Process Reengineering, Installation and configuration, Project team training, Business Requirement mapping, Module configuration, System interfaces, Data conversion, Custom Documentation, End-user training, Acceptance testing and Post implementation/Audit support.

This feature of the SDLC is critical to the successful management of an IS project. The SDLC can also be viewed from a more process oriented perspective. This emphasizes the parallel nature of some of the activities and presents activities such as system maintenance as an alternative to a complete re-design of an existing system.

The System Development Life Cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

Phase	***Activity***
1.Preliminary Investigation	• Determine and evaluate the benefits of the system and ensure that solution fits to business strategy.
2.Systems Requirements Analysis	• Analyzing the system base on user requirements
3.System Design	• Design interface, database and functions
4.System Developing	• Programing the system
5.System Testing	• Testing
6.System Implementation	• Final testing, quality controls and acceptance.
7.Post implementation Maintenance	• Continuous evaluation and maintenance of the system in the live environment.

Table 6 – ERP SDLC (Musaji, 2002)

From the perspective of the IS Audit, the following are the possible advantages:

- The IS auditor can have clear understanding of the various phases if the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
- The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

ERP audit approach

ERP implementations can be very complex systems consisting of thousands of configuration items with many individual modules. And audit assessment in such a complex system can seem like an impossible mission.

The only way to manage such an assignment if by splitting the system in manageable subsystem that supports the objectives of the audit.

People

The interaction of the users with the system is one of the main concerns regarding to the security of the ERP system. Data integrity in ERP environments is highly dependent on how well lower-level employees who enter the data understand their jobs and the system. For this reason, time should be spent interviewing these employees and documenting their ability to deal with regular and irregular work situations. Because ERP systems are highly sophisticated, employee training procedures should be reviewed including the proficiency level of employees, training schedules, and how system changes and new modules are introduced. (Monk, et al., 2006)

ERP systems require greater training to master duties and responsibilities and can represent a significant investment for employers. For this reason, employees are often undertrained which can introduce opportunities for errors and fraud. Data accepted by the system is posted through all accounts immediately and errors become pervasive. Employees must be trained to deal with "*nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates*". (IT Governance Institute, 2004)

Functionality Requirements and Workflow Integration

ERP system can be thought as the engine that automates the business process of the company. The main workflows of the system should be identified and documented. This will be used from IS Auditor to match the ERP aspect that fulfils this business workflows

This comparison is done in order to ensure that the functionalities requirements are met. If this requirement are not met this brings to weakly controlled business or weak internal controls.

Operations

The policies and practices associated with an ERP system are essential elements of governance. Furthermore, insufficient operational aspects of an ERP system can raise questions regarding effectiveness or existence of information assurance controls claimed to be implemented. An auditor's review of the operational aspects of an ERP system can identify significant security deficiencies not considered previously.

Working Papers and Documentation

A system with insufficient documentation is difficult to assess. The documentation for a system undergoing rapid changes is likely to become outdated quickly. Detailed, accurate and complete documentation is a good indicator of a system that is properly managed. Reviews of documentation should consider if it contains sufficient: The documentation should provide enough depth of detail so that implementation elements of the ERP system can be duplicated or evaluated by those not familiar with the system. Auditor's working papers should include documentation of the company's business processes that are captured by the ERP and legacy systems. Documentation may consist of narratives, flowcharts, and graphics such as data-flow-diagrams, entity-relationship diagrams, and resource-event-entity models. It is important that auditors have an understanding of the graphical methods in order to determine if the described relationships and processes accurately reflect the actual processing of information. Furthermore, it is necessary in order to determine if individual user rights and privileges reflect the appropriate segregation of duties. (Cooke, 2004)

The use of intelligent work papers can save time in documenting responses to internal control questionnaires wherein answers are automatically logged and potential weaknesses identified in a section of the audit report.

Good documentation serves a variety of purposes. It is the basis for employee training, it provides IT programmers and analyst's information for future modifications, it provides auditors with support for evaluation of internal controls, and it helps to assure that the systems design specifications were correctly implemented. (Bodnar, et al., 2004)

Security Requirements

Laws, regulations, policies and standards form the basis for the security requirements of a system. An ERP application should support existing security requirements. An auditor should determine if a system sufficiently supports all security requirements. The inability of an ERP system to support a particular requirement should be counteracted with at leastone of the following:

- Compensating controls
- Acceptance of risk

Management may choose to accept risk when a security requirement is difficult or impossible to meet.

Good documentation serves a variety of purposes (Bodnar & Hopwood, 2004). It is the basis for employee training, it provides IT programmers and analysts information for future modifications, it provides auditors with support for evaluation of internal controls, and it helps to assure that the systems design specifications were correctly implemented.

Change Management

Organizations that customize their ERP systems will need to maintain an effective change management process. Changes that are not properly controlled may introduce weaknesses into the security posture of the ERP system. It is also likely that applications will need periodic vendor updates to the deployed modules. The consequences of poor change management can introduce new weaknesses when they are not properly controlled or allow a known weakness to persist when they are not implemented in a timely manner.

An auditor can look into recent changes to determine if they were:

- *Authorized* - The change was agreed upon prior to deployment and permitted by management.
- *Controlled* - A process of changing systems' aspects is documented and followed and provides separation-of-duty assurances.
- *Validated* - Follow-up with regard to the change was conducted by those not responsible for implementing the change.

The validation of the change provides assurance that only the targeted aspects of the change were affected, while other parts of the system were not altered.

Changes to program code should be authorized and documented internally within the code as well as externally. Controls should separate program coding changes from program execution and access to related data files. Testing of all changes should be documented and reviewed before the revisions are placed into production. If testing is not given high priority, errors might go undetected causing serious weaknesses in the accounting information systems and in financial reporting.

Configurations

An ERP system may contain thousands of individual configuration items. These items impact the workflow and handling of information through the system. Misconfigurations may impact the confidentiality, integrity or availability of the information. Other supporting parts of the system, including operating systems, networking devices and databases, also need explicit configurations to support security in the ERP system. Configurations should be documented and periodically validated. An auditor can assess ERP configurations by matching configuration documentation with actual settings in the system. A lack of sufficient documentation for settings is another point of view an auditor should consider.

Technology

ERP systems are often very complex and may contain components from multiple vendors. Furthermore, an ERP system often relies on commodity operating systems and databases that increase overall complexity. The extent the technological components integrate or work tightly together can affect the overall security of the ERP system.

Access Control

Mechanisms that allow or deny access according to a policy are core security components. Access control mechanisms must support the security policy designated for the ERP system. Often, access control mechanisms from different vendors do not integrate easily. The access control mechanisms for the operating system, database and ERP application may not integrate well. The auditor needs to review the implementation of each access control mechanism to determine if weaknesses exist. It may be possible for a user to bypass controls in the ERP application through either the database or operating system if there is a mismatch in the access control implementations in either case. Security is a major control risk for ERP systems and auditors should determine whether the security standards framework for the ERP system meets the standards for the firm's security policy (IT Governance Institute, 2004). ERP security audits should focus on physical access, system access, and segregation of duties. Physical access is the easiest to ascertain and includes access to data centres, data libraries, and servers.

Audit Logs

Detecting ERP misuse is an important security management activity. The auditor should review audit settings and implementations to assess if audit logs have the capability or capacity to capture events that could be analyzed to detect ERP misuse. Correlation of audit activity in the ERP system with external audit events through the operating system or networking equipment should also be examined to determine if sufficient details are collected to detect misuse and support user accountability.

Automated quality-assurance testing is available for every transaction without disruptions caused by traditional auditing methods. Many audit programs run concurrently with normal processing to capture audit data and identify errors as they occur (Taylor, 2006).

Benefits of ERP are numerous. Most ERP systems integrate data from legacy systems. Auditors must have an understanding of the process and know the source of the data, the points of processing, and the points of integration. Some systems provide for the use of embedded audit routines that the user can customize. Snapshots can be used to provide detail about specific processing functions. Auditors must verify the existence and effectiveness of backups of output and disaster recovery plans. Off-site backups should occur at regular intervals and training for disaster recovery should be evaluated.

Control requires continuous monitoring of system access and a log of all access activities. The functions of development, testing, and production should be separated. Development, other than routine maintenance, should be initiated and approved outside of the IT function. Personnel responsible for modifying code should not be able to place code into production or execute production code. Similarly, access to data libraries should be separated from operations to prevent fraudulent changes to data (Perry, 1985). All changes to code should be tested, documented and reviewed prior to placing it into production (Adint, 2002).

In addition to auditing through the system, audits around the system should ensure that results from ERP processing are reconciled to external information such as bank statements. High priority should be given to vulnerable areas such as accounts payable. Controls for responsibility accounting centres must be reviewed and the authorization

process for nonroutine transactions.

ERP systems can be implemented for any size company and the underlying control environments can be unique and complex. Examination of various internal checks such as the use of check digits, cross-field checking, limit tests, table lookups, and default values can help to establish data integrity (Hahn, 1999). Attention must also be given to the specific points of data entry including automated entry at point-of-sale and EDI. Data entered from purchase requisitions, purchase orders, invoices, and invoices are posted immediately throughout the system and correction of errors will be more pervasive than with stand-alone legacy systems (Brady, et al., 2001).

IT audits, particularly in ERP environments, require the retrieval of significant amounts of data from the firm's files. Some data may reside on direct access data devices such as hard drives. One approach is to use commercial products designed for data retrieval. Further technical assistance may be necessary where these products are not adequate for all applications. Some auditors rely on the use of query languages such as SQL which can be tailored to the firm's data files if the technical expertise is available.

Longitudinal analysis using CAATs has the advantage of revealing trends, patterns, and shifts in the data.

Automated Workflows

The ability of an ERP system to automate manual processes is the core purpose of the system. When workflows are automated through the ERP, a possibility exists that certain processes may become orphaned—that is, they are erroneously left out of the system. Orphaned processes can seriously affect the ability of the ERP system to provide timely or accurate information. An auditor should review the automated processes to ensure that all workflows intended to be automated are actually implemented or have sufficient documentation indicating the supplemental manual processes. At the other extreme, an automated process may introduce weaknesses that affect other controls such as separation of duties. Furthermore, a process without sufficient checks and balances may enable a user to perpetrate a fraud. Audits of ERP workflows should include a determination of whether automated processes violate separation of duties or introduce the ability for workers to perpetrate a fraud, which means the system is not enforcing separation of

duties.

Transaction authorization is vital to data integrity in ERP systems. The benefit of the tightly integrated modules creates potential problems for transaction authorization. Because of the real-time nature of processing, controls must be present to validate transactions before they are accepted by the system. Many of the controls are programmed within the system and the challenge to auditors is to gain a detailed understanding of the controls and ensure they are being used (Hall, et al., 2005).

Conclusions

ERP implementations can be very complex and critical IT investments. The complexity of auditing such a system can be managed by decomposing system aspects into the people, operational and technical security countermeasures.

Auditing an ERP system is really complex and time consuming. The auditor should invest sufficient time and effort of gathering background knowledge and understanding of the organisation's existing/planned development and gaining control of the ERP system. Audit of ERP solutions is not just an audit of technology but of the business process. The aim of ERP system is to integrate people, business functions through information technology. This is why the best approach in auditing such a system is decomposing them according to these aspects.

Audit should also ensure that the organisation has followed the structured steps involved in implementation of an ERP, such as Project Planning, Business & Operational analysis including Gap analysis, Business Process Reengineering, Installation and configuration, Project team training, Business Requirement mapping, Module configuration, System interfaces, Data conversion, Custom Documentation, End-user training, Acceptance testing and Post implementation/Audit support.

4.2 Analytical Part: IS Audit Survey

4.2.1 Introduction

This chapter analyses data collected from the sampled population in line with objectives and hypothesis set for the study. The sample is selected based on background (IT or Auditing) and experience in IS Auditing. The analyzed data has been presented in tables and graphs for easy assimilation. Questionnaires were formulated and administered by interview to respondents who have been part of an IS audit. The survey was conducted between August to December 2013 Tirana, Albania. The aim of this survey is to confirm the accuracy and the completeness of the existing theories, techniques and standard introduced in the first part of the research.

This part has been apportioned into two parts: Descriptive analysis of responses based on objectives and analysis based on hypothesis. The hypotheses addressed in this part are:

- The responsibilities of an IS auditor is impacted by the background of the individual.
- The number of times one is involved in an IS audit has a bearing on the educational qualification of an IS auditor.
- Knowledge of IS audit and job title have a close correlation.

These hypotheses were analyzed by using a two-way frequency procedure in table analysis. The analysis of the field data was done using SPSS software application.

4.2.2 Descriptive Analysis

Background

The background of respondents was sought. Out of the 31 respondents, 20 (64.5%) have a background on IT while 11 (35.5%) have an audit background. This signifies that the various stakeholders were consulted for the purpose of the research.

	Frequency	Percent	Cumulative %
Audit	11	35.5	35.5
IT	20	64.5	100.0
Total	**31**	**100.0**	

Table 7 - Author's field survey: Background [Author]

The data seen above signify that there was a fair representation of ideas on the subject matter; hence the findings are more reliable, credible, fair and not skewed.

Job title

Out of the 31 respondents, 9 (29.0%) respondents have a financial title, 19.4% are consultants, 12.9% are DBA, 6.5% are IT Auditors and Operational mangers and the rest of the respondents are spread among other job titles as in Table 8. From the data analyzed, it reveals that the respondents cut across all fields in the organization and therefore a panacea to crosscutting ideas on the research area.

	Frequency	**Percent**	**Cumulative %**
Consultant	6	19.4	19.4
DBA	4	12.9	32.3
Developer	1	3.2	35.5
Financial	9	29.0	64.5
IT Auditor	2	6.5	71.0
IT Support	1	3.2	74.2
Manager	1	3.2	77.4
MIS	1	3.2	80.6
MIS Assistant	1	3.2	83.9
Operational	2	6.5	90.3
Project Manager	1	3.2	93.5
System Admin	1	3.2	96.8
Tester	1	3.2	100.0
Total	**31**	**100.0**	

Table 8 - Author's field survey: Job Title [Author]

Number of times included in an IS Auditing Project

The number of times an IS auditor is included in IS audit helps to portray the depth of knowledge and experience the person has in the discipline. Asked of the number of times respondents were included in an IS audit project, the following revealing findings in Table 9 were made.

	Frequency	Percent	Cumulative %
1	11	35.5	35.5
2 to 5	10	32.3	67.7
more than 5	10	32.3	100.0
Total	**31**	**100.0**	

Table 9 - Author's field survey: Number of times included in an IS Auditing Project [Author]

From the responses above, it is clear that respondents have a depth of knowledge and experience in IS audit per the number of times they were included in IS audit.

Education or background for an IS auditor

Out of the 31 respondents, a whooping 27 (87.1%) indicated that the background or Education of an IS auditor must be in IT and Audit, while 3 (9.7%) and 1 (3.2%) indicated that it should be in Audit or IT respectively as seen in Table 10.

	Frequency	Percent	Cumulative %
Audit	3	9.7	9.7
IT	1	3.2	12.9
IT and Audit	27	87.1	100.0
Total	**31**	**100.0**	

Table 10 - Author's field survey: Education or background for an IS auditor [Author]

Knowledge expected from an IS auditor with regards to IT concepts

16 (51.6%) out of the 31 respondents believe an IS auditor must have knowledge of applications in IT concepts, 10 (32.3%) indicated it must be in security and 5 (16.1%) indicate that Databases will be ideal as in Table 11. It is obvious from the below table that a combination of the concepts will be more ideal for an IS auditor.

	Frequency	**Percent**	**Cumulative %**
Applications	16	51.6	51.6
Databases	5	16.1	67.7
Security	10	32.3	100.0
Total	**31**	**100.0**	

Table 11 - Author's field survey: Knowledge expected from an IS auditor with regards to IT concepts [Author]

IS Audit Plan

For the 31 respondents, it was shockingly revealed that 21 (67.7%) of their companies do not have an IS audit plan while 10 (32.3%) accepted that their companies have an IS audit plan as indicated in Table 12. It is apparently revealing that companies do not have an IS audit plan and yet are grossly involved IS audit. This means that the companies affected must consciously develop a comprehensive IS audit plan for IS audit purposes.

	Frequency	**Percent**	**Cumulative %**
No	21	67.7	67.7
Yes	10	32.3	100.0
Total	**31**	**100.0**	

Table 12 - Author's field survey: Does your company have an IS Audit Plan? [Author]

Complying with any auditing standards, guidelines or frameworks

From Table 13, the companies of 23 (74.2%) respondents do not comply with any auditing standards, guidelines or frameworks while only 8 (25.8%) do. Out of the 8 who comply, 5 (16.1%) comply with ISO standards while 3 (9.7%) comply with COBIT standards and guidelines. This is so intriguing and companies affected must take steps to address this anomaly to gain competitive advantage.

	Frequency	**Percent**	**Cumulative %**
COBIT	3	9.7	9.7
ISO	5	16.1	25.8
No	23	74.2	100.0
Total	**31**	**100.0**	

Table 13 - Author's field survey: Does your company comply with any auditing standards, guidelines or frameworks? [Author]

Responsible for IS Audit

The activities responsible for IS audit where tabled and majority of the respondents placed application auditing as the main activity responsible for IS audit. The rest of the activities are shown in Table 14 with corresponding frequencies and percentages.

	Frequency	**Percent**	**Cumulative %**
Application Auditing	10	32.3	32.3
Compliance Documentation	6	19.4	51.6
Compliance Testing	7	22.6	74.2
Data Analytics	4	12.9	87.1
IS General Controls	4	12.9	100.0
Total	**31**	**100.0**	

Table 14 - Author's field survey: Which activities from the below list are responsible for IS Audit? [Author]

Information Technology tools and techniques

From table 15, 24(77.4%) of the 31 respondents use Excel as the IT tool and technique for IS audit. The other tools and techniques used are indicated in the table below. This signifies that most IS audit software and tools are not embraced by the companies in IS audit.

	Frequency	Percent	Cumulative %
ACL	3	9.7	9.7
Excel	24	77.4	87.1
In house SW	3	9.7	96.8
Integrated Audit Module	1	3.2	100.0
Total	**31**	**100.0**	

Table 15 - Author's field survey: What Information Technology tools and techniques (CAATs) does your company use to help meet audit objectives? [Author]

Qualification in IS Auditing

30 (96.8%) of the 31 respondents do not have any qualification in IS audit with only 1 (3.2%) having a qualification in CISA as shown in Table 16. The result indicates that more people need to be trained in IS auditing to enhance their work in the field.

	Frequency	Percent	Cumulative %
CISA	1	3.2	3.2
No	30	96.8	100.0
Total	**31**	**100.0**	

Table 16 - Author's field survey: Do you have any qualification in IS Auditing? [Author]

Tools and skills to perform an IS Audit

On the position of whether the companies of respondents have the right tools and skills to perform IS audit, 26 (83.9%) said no while 5 (16.1%) diminutive responded in the affirmative as seen in Table 17. The huge number with a negative response signifies a wider need for the right tools and skills needed in the IS audit sector.

	Frequency	**Percent**	**Cumulative %**
No	26	83.9	83.9
Yes	5	16.1	100.0
Total	**31**	**100.0**	

Table 17 - Author's field survey: Does your company have the right tools and skills to perform an IS Audit? [Author]

4.2.3 Analysis of hypotheses

The hypotheses have been analyzed from the data of the 31 respondents. The Chi-square test was used in SPSS by the use of table analysis to test the association between two categorical variables with the significance level, $\alpha = 0.05$ and a sample size, $n = 31$. The criterion used is stated below:

If the test statistic (P) is less than the significance level (α), the null hypothesis (H_O) is rejected and the alternative hypothesis (H_1) is accepted.

The responsibilities of an IS auditor is impacted by the background of the individual.

H_0: There is no relationship between IS auditor and the background of the person.

H_1: There is a relationship between IS auditor and the background of the person.

Background	Activities					
	Application Auditing	Compliance Documentation	Compliance Testing	Data Analytics	IS General Controls	**Total**
Audit	3	4	2	2	0	**11**
IT	7	2	5	2	4	**20**
Total	**10**	**6**	**7**	**4**	**4**	**31**

Table 18 - Author's field survey: Background by Responsible activities of an IS auditor [Author]

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	.987[a]	1	.320
Continuity Correction[b]	.382	1	.537
Likelihood Ratio	.997	1	.318
N of Valid Cases[b]	31		

Table 19 - Author's field survey: Chi-Square Tests - Background [Author]

The alpha (α) value, 0.05 is less than the test statistic value, (P) of the Chi-Square test, 0.320 from above. The null hypothesis (H_o) is therefore accepted and H_1 rejected, hence conclude that the responsibilities of an IS auditor is not directly related to the background of the person. The background of an IS auditor is therefore not fully a requirement for assigning responsibilities per the data collected.

The number of times one is involved in an IS audit has a bearing on the educational qualification of an IS auditor.

H_o: The number of times one is involved in an IS audit has no direct relationship with the educational qualification of an IS auditor.

H_1: The number of times one is involved in an IS audit has a direct relationship with the educational qualification of an IS auditor.

	Relevant education or background			
Number of times involved in IS audit	Audit	IT	IT and Audit	**Total**
1	3	1	7	**11**
2 to 5	0	0	10	**10**
more than 5	0	0	10	**10**
Total	**3**	**1**	**27**	**31**

Table 20 - Author's field survey: Number of times involved in IS audit by Relevant education or background [Author]

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	8.350[a]	1	.040
Likelihood Ratio	9.421	1	.051
N of Valid Cases	31		

Table 21 - Author's field survey: Chi-Square Tests - Number of times [Author]

From the Chi-square test results, P-value (0.040) is less than alpha (α) of 0.05, hence H_o is rejected and H_1 accepted. The number of times one is involved in an IS audit has a direct relationship with the educational qualification or relevant experience of an IS auditor.

Knowledge of IS audit and job title have a close correlation.

H_o: The knowledge of an IS auditor does not play a role in the job title of the individual

H_1: The knowledge of an IS auditor plays a role in the job title of the individual

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	22.610[a]	1	.031
Likelihood Ratio	28.575	1	.005
N of Valid Cases	31		

Table 22 - Author's field survey: Chi-Square Tests - Knowledge [Author]

From the results of the Chi-Square test, P value (0.031) is less than α (0.05), hence H_0 is rejected and H_1 accepted; thus it is held that the knowledge of an IS auditor plays a role in the job title of the individual IS auditor.

4.2.4 Survey Conclusions

From the data analyses and test of hypotheses, the following summarized findings were arrived at:

- To perform creditably in IS audit, a combination of IT concepts such as applications, databases and security will enhance IS audit capabilities and knowledge.
- IS audit software and tools are more important in performing IS audit. It was clear from the survey that most companies lack IS audit software and tools for the performance of the audit.
- An IS audit plan is most important in IS audit. Most of the companies do not have an IS audit plan which definitely impedes their work in the auditing. A comprehensive IS audit plan is encouraged to be developed for all companies involved in IS audit.
- The huge number with a negative response on the use of IS audit tools signifies a wider need for the right tools and skills needed in the IS audit by companies.
- The result indicates that more people do not posses any qualification in IS audit and therefore need to be trained in IS auditing to enhance their work in the field.
- It was also found out that most of the companies do not comply with any auditing standards, guidelines or frameworks of IS audit. The main IS audit standards and

techniques need to be introduced to assist in IS audit.

- The knowledge of an IS auditor plays a role in the job title of the individual IS auditor. It was seen from the hypothesis that more IS auditors must have knowledge in both IT and Audit.
- The number of times one is involved in an IS audit has a direct relationship with the educational qualification or relevant experience of an IS auditor.

5 Conclusion

The aim of this study was introduce a set of standard techniques for auditing information systems. This will help auditors who most of the times come from non-IT profile and also the IT people who have only technological background. It is very important for an IS auditor to have both, IT and auditing knowledge to bridge the gap between IT and auditing professions.

It provided an overview of IS Auditing concept, IS Audit procedures, IS Audit techniques and standards, understanding the business needs and processes, understanding the information, the information system data flow and data structure., performing the necessary steps in an auditing ERP system and also analysing the responses from individual that has been part at least once in an IS Audit assignment.

In order to perform a successful IS audit IT and audit knowledge are required, IS audit tools and techniques are required.

To perform creditably in IS audit, a combination of IT concepts such as applications, databases and security will enhance IS audit capabilities and knowledge. An IS audit plan is most important in IS audit. Most of the companies do not have an IS audit plan which definitely impedes their work in the auditing.

A comprehensive IS audit plan is encouraged to be developed for all companies involved in IS audit.

IS audit software and tools are more important in performing IS audit. It was clear from the survey that most companies lack IS audit software and tools for the performance of the audit. The huge number with a negative response on the use of IS audit tools

signifies a wider need for the right tools and skills needed in the IS audit by companies. The result indicates that more people do not possess any qualification in IS audit and therefore need to be trained in IS auditing to enhance their work in the field. The main IS audit standards and techniques need to be introduced and observed to assist in IS audit.

As result of this study ISACA steps in performing and IS audit are reconfirmed as the only successful way to perform a successful audit assignment (Table 4).

Recommendation for further research

Traditional audit style noawdays sometimes prove to be insufficient because the lack the most essential element in business environment which is updated information.
There is an increasing demand to provide auditing over information as close to real time as possible. That is why a further step in this research would be continuous auditing.
'Continuous auditing is and audit methodology that enables auditors to provide written assurance on a subject matte using series audit reports issued simultaneously with, or a short period of time after occurrence of events underlying the subject matter' (ISACA, 2013).

The advantage continuous auditing is that voluminous data are analyzed at high speed and also aims to provide a more secure platform to avoid fraud and also real time process ensures a high level of financial control.

Bibliography

(AAS), Auditing and Assurance Standard. 2003. 2003.

Adint, L. 2002. Packaged Software Control Objective. *AuditNet.* [Online] 2002. www.auditnet.org/docs/PackagedSoftwareControlObjectives.doc.

An Information Sytem Auditor's Profile. **Carrol, Mariana. 2006.** s.l. : University of South Africa, 2006, p. 164.

Bodnar, G.H. and Hopwood, W.S. 2004. *Accounting Information Systems.* Upper Saddle River : Prentice Hall, 2004.

Brady, M., Monk, E. and Wagner, B. 2001. *Concepts in Enterprise Resource Planning.* Boston : Thomson Learning, 2001.

Cooke, M. 2004. Application Audits. *AuditNet.* [Online] 2004. www.auditnet.org/articles/200404%20Cooke%20Application%20Audits.htm.

Davis, Gordon Bitter and Olson, Margrethe H. 1985. *Management of Information System: Conceptual foundations, structure, and development.* New York : McGraw-Hill College, 1985. 0-07-015828-2.

Davis, Robert E. 2005. *Information Systems Auditing: The IS Audit Testing Process.* Boston : Amazon, 2005. B003L20112.

E.Davis, Robert. 2011. *IT Auditing: An adaptive process.* s.l. : Lulu.com, 2011. 9780557220519.

GLEIM. 2004. *CIA Review.* Florida : Gleim Publications, 2004.

Hahn, J. 1999. ERP Systems: Audit and Control Risks. *AuditNet.* [Online] 1999. www.auditnet.org/docs/erprisks.pdf.

Hall, James A. and Singleton, Tommie. 2005. *Information Technology Auditing And Assurance.* Mason, Ohio : Thomson, 2005. 9780324191981.

Hinson, Gary. 2006. Frequently Avoided Questions about Computer Auditing. *IsecT.* [Online] IsecT, 2006. http://isect.com/.

Champlain, Jack J. 2003. *Auditing Information Systems.* s.l. : Wiley, 2003. 978-0471281177.

IEC, ISO. 2011. *Information Security Risk Management - 27005.* 2011.

Institute of Charted Accounts. 2010. *Information System Controls and Audit.* 2010.

ISACA. 2013. *CISA Review Manual.* Rolling Meadows : ISACA, 2013. 160420303005.

IT Governance Institute. 2004. IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control Over Disclosure and Financial Reporting. *IT Governance Institute.* [Online] IT Governance Institute, 2004. http://www.itgi.org.

Jacobs, F.R. and Whybark, D.C. 2002. *Why ERP? A Primer on SAP Implementation.* New York : Irwin McGraw-Hill, 2002. 978-0072400892.

Kimpton, Clarence and Martin, Denys. 2001. Overview of Principal IT Evaluation Models. *ISACA.* [Online] ISACA, 2001. http://www.isaca.org/Journal/Past-Issues/2001/Volume-5/Pages/Overview-of-Principal-IT-Evaluation-Models.aspx.

Monk, E. and B.Wagner. 2006. *Concepts in Enterprise Resource.* USA : Thompson Course Technology, 2006.

Musaji, Yusufali F. 2002. *Integrated Auditing of ERP Systems.* New York : John Wiley & Sons, 2002. 978-0-471-23518-7.

Page, C. and Meyers, D. 2000. *Applied research design for business and management.* Sydney : McGraw-Hill, 2000. 978-8888885919.

Taylor, P. 2006. Driving Financial Process Improvement. *Strategic Finance.* 2006, Vol. 87.

Weber, Ron. 1988. *EDP Auditing - Conceptual Foundations and Practice.* New York : McGraw-Hill, 1988. 978-0070688322.

APPENDIX

Questionnaire - Interview Questions

All information provided will be used solely and exclusively for academic purposes and would be treated with the necessary confidentiality it deserves.

1. Interviewee Background

2. Job Title:

3. Number of times included in an IS Auditing Project.

4. In your opinion, what is the most relevant education or background for an IS auditor to ease the execution of a successful IS audit assignment?

5. In your opinion, what knowledge is expected from an IS auditor with regards to IT concepts (e.g. Networks, Databases, Applications, Software, Security).

6. Does your company have and IS Audit Plan?

7. Name the steps involved in performing an IS audit.

8. Does your company comply with any auditing standards, guidelines or frameworks? If yes specify please choose which one.

9. Which activities from the below list are responsibility of IS Audit?

10. What Information Technology tools and techniques (CAATs) does your company use to help meet audit objectives?

11. Do you have any qualification in IS Auditing?

12. Does your company have the right tools and skills to perform an IS Audit?