Master's Thesis

Business Information Systems

2015

Gavin Doherty

ASSESSMENT AND IMPROVEMENT OF INFORMATION SYSTEM SECURITY CONTROLS FOR COMPANY X

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Systems (MBA)

May 2015 | 163 pages

Jarkko Paavola

Gavin Doherty

ASSESSMENT AND IMPROVEMENT OF INFORMATION SYSTEM SECURITY CONTROLS FOR COMPANY X

With the transfer of sensitive information through a borderless and vulnerable cyber world information security has become vitally important to businesses. Companies now depend upon information systems to conduct routine, important and critical business processes and protection of the underlying systems is crucial to their success. Information systems are subject to threats that can seriously affect business operations, organisational assets and reputation by exploiting vulnerabilities which can compromise the confidentiality, integrity and/or availability of processed and transmitted information.

Company X commissioned this research project to investigate the status of their information systems and identify, present and discuss improvements. By understanding the current company procedures in complying with international standards, binding contractual obligations and customer specific requirements it could be established how this has influenced the development of the information systems security to date and how security could be improved to meet future needs. An appropriate industry standard information security risk assessment (ISRA) framework for developing improved information system security controls was researched and selected.

The practical element of the research project used the OCTAVE Allegro ISRA to interrogate the performance of selected areas of the company's existing IT infrastructure to collect data and understand how the component parts of the system assisted daily business functions and the impact on the business should their failure occur. From the results of the ISRA a development plan was proposed to assist the company with implementing information system security control improvements and a company-wide information security awareness training programme.

The results of the research project indicate that companies of a similar size and position to Company X should regularly reassess their IT information security by implementing one of the many readily available industry standard ISRA frameworks. The study also indicates that the analysis and selection of appropriate security controls for an information system is a critical task that can have major implications on the operations and assets of a company as well as the welfare of individuals who use, are in contact with, or are responsible for these systems.

KEYWORDS:
Information systems security, security requirements, risk assessment, security risks, threats, vulnerabilities, security controls, system development, monitoring risk, risk management.

OPINNÄYTETYÖ (YAMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Business Information Systems (YAMK)

Toukokuu 2015 | 163 sivua

Jarkko Paavola

Gavin Doherty

TIETOJÄRJESTELMÄN TURVAKONTROLLIEN ARVIOINTI JA KEHITTÄMINEN – TAPAUSTUTKIMUS: YRITYS X

Arkaluonteisen tiedon siirtyminen haavoittuvaan kybermaailmaan on osaltaan aikaansaanut sen, että tietoturvallisuudesta on tullut elintärkeä osa liiketoimintaa. Yritykset ovat riippuvaisia tietojärjestelmistä liiketoiminnassaan ja näin ollen niiden suojaus on keskeistä menestyksen takaamiseksi. Tietojärjestelmät ovat alttiita uhille, jotka saattavat vakavasti vaikuttaa yrityksen liiketoimintaan, kilpailuetuun sekä maineeseen. Haavoittuvuuksien hyväksikäyttö saattaa vaarantaa tiedon luotettavuuden, eheyden ja saatavuuden.

Yritys X antoi toimeksi tämän tutkimuksen tutkiakseen tietojärjestelmiensä tilan sekä esittääkseen tilanteeseen mahdollisia parannuksia. Yrityksen nykyisten käytäntöjen mukauttamisen tarve kansainvälisiin standardeihin, sopimusvelvoitteisiin ja asiakkaiden vaatimuksiin ovat olleet perustana tietojärjestelmäkehitykselle sekä ohjaavat mihin vastaisuudessa tulisi suunnata.

Tutkimuksen käytännön osiossa hyödynnettiin OCTAVE Allegro –kehikkoa yrityksen IT-infrastruktuurin osa-alueiden toimivuuden arviointiin. Tietoa keräämällä pyrittiin ymmärtämään miten järjestelmän eri osiot edesauttoivat päivittäistä liiketoimintaa ja mitkä olisivat vaikutukset, mikäli niihin kohdistuisi häiriöitä. Riskikartoituksen tuloksena laadittiin ja esitettiin yritykselle suunnitelma tarvittavien tietoturvatoimien kehittämiseksi ja yrityksenlaajuisen tietoturvakoulutuksen järjestämiseksi.

Tutkimuksen tulokset osoittavat, että yrityksen X kokoluokan ja samalla tavalla asemoituneiden yritysten tulisi säännöllisesti arvioida tietojärjestelmänsä käyttäen saatavilla olevia riskikartoitusmenetelmiä. Tutkimus myös näyttää toteen, että tietojärjestelmän turvatoimien arviointi on kriittisen tärkeä toimenpide, jolla voi olla merkittäviä vaikutuksia yrityksen toiminnoille. Lisäksi asialla on vaikutusta myös tietojärjestelmistä vastuussa olevien ja tietojärjestelmiä käyttävien henkilöiden hyvinvoinnille.

ASIASANAT:

Tietojärjestelmien turvallisuus, turvallisuusvaatimukset, riskien arviointi, turvallisuusriskit, uhat, haavoittuvuudet, turvatoimet, järjestelmäkehitys, riskien seuranta, riskien hallinta.

Content

APPENDICES

FIGURES

TABLES

List of abbreviations (or) symbols

AS	Aerospace Standards
BMIS	Business Model for Information Security
BMS	Business Management System
COBIT	Control Objectives for Information and Related Technology
COSO	Committee of Sponsoring Organisations
CMMI	Capability Maturity Model Integration
CNC	Computer Numerical Control
CSD	Computer Security Division
DoS	Denial of Service
E2EE	End-To-End Encryption
ERP	Enterprise Resource Planning
FISMA	Federal Information Security Management Act
FMS	Factory Management System
IAQG	International Aerospace Quality Group
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IPSEC	Internet Protocol Security
IS	Information Security
ISACA	Information Systems Audit Control Association
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ISRA	Information Security Risk Assessment
ISRM	Information Security Risk Management
ISSO	Information Systems Security Officer
IT	Information Technology
ITAF	Information Technology Assurance Framework

ITGI	Information Technology Governance Institute
ITIL	Information Technology Information Library
ITL	Information Technology Laboratory
ITSM	Information Technology Service Management
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MITMA	Man In The Middle Attack
NADCAP	National Aerospace and Defense Contractors Accreditation Program
NDA	Non-Disclosure Agreement
NDT	Non-Destructive Testing
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
OS	Operating System
OTD	On-Time Delivery
PDF	Portable Delivery Format
PMBOK	Project Management Body of Knowledge
PPTP	Point-to-Point Tunneling Protocol
QMS	Quality Management System
SAE	Society of Automotive Engineers
SEI	Software Engineering Institute
SP	Special Publications
SSL	Secure Sockets Layer
TOGAF	The Open Group Architecture Framework
VPN	Virtual Private Network

1 INTRODUCTION

1.1 Information systems

Today’s information systems are a complex assembly of technology compromising hardware, software, firmware, processes, and people, working together to provide companies with the capability to process, store, and transmit information in a timely manner to support various missions and business functions. The degree to which organisations have come to depend upon these information systems to conduct routine, important and critical aspects of their business means that the protection of the underlying systems is paramount to their chances of success (NIST 2010a, 1).

For many companies, information and the technology that supports it represent their most valuable but often least understood assets (Radmanesh et al. 2013, 1). Managing the security risks associated with the growing reliance on IT is a continuing challenge. Companies, similar to the one assessed in this research project, struggle to find efficient ways to ensure that they fully understand the information security risks affecting their operations and fail to have a system to implement appropriate controls to mitigate these risks (GAO 1999, 1).

Information security is essential for the day-to-day operations in most companies. Breaches in information security can lead to a substantial impact within a company through, for example, financial or operational damage. In addition, an organisation can be exposed to external impacts such as reputational damage or legal risk, which can jeopardise customer or employee relations or even endanger the survival of the company altogether. (ISACA 2012a, 15)

The analysis and selection of appropriate security controls for an information system is a critical task that can have major implications on the operations and assets of a company as well as the welfare of the individuals who are in contact or responsible for these (NIST 2010a, 1).

1.2 Company overview

Originally founded in the 1940's, Company X (hereinafter referred to as "the company") is a business located and operated in Finland. The company's initial business activities involved the overhauling of combustion engines for commercial and governmental motor vehicles. However, during the early 1990's, the company's business strategy dramatically changed leaving behind the auto mechanics trade and turning its focus to manufacturing precision-engineered components using modern automated CNC machines.

More than twenty years later, the company has expanded its capacity and currently employs over thirty-five personnel specialised in performing precision machining, surface treatments and mechanical assembly for highly developed technologies in both foreign and domestic markets. The company has evolved dramatically to become one of Finland's leaders in the commercial, aerospace, and defence manufacturing industries.

1.3 Current business environment

The company's expansion into such a highly specialised market area has been rewarded with privileged business opportunities working with prestigious multinational aerospace and defence corporations such as Rolls-Royce Holdings PLC in the UK, Goodrich and The Boeing Company in the USA, Thales Group and Messier-Bugatti-Dowty in France and the SAAB Group in Sweden. However, with such privileges has come the progressive requirement for a far more disciplined and secure operational environment which involve the company's IT systems that store and transfer data.

Major global aerospace and defence corporations such as those mentioned above 'outsource' their business processes to carefully selected suppliers and the company is currently one of these. In order for any supplier to enter a contractually binding agreement with a corporation they must first be fully compliant with specific globally recognised standards and approved by accredited bodies.

Suppliers are ranked and categorised into different capability tiers, which are determined by these standards and bodies that they must adhere to. In addition to these onerous conditions corporations may also stipulate further obligatory requirements that must also be fulfilled. Some of these additional requirements can be information security focused and depending on the contractual conditions evidence of continual monitoring and improvement of specific processes may need to be presented on demand.

Any manufacturing and/or assembly work for aerospace and defence contracts will involve the handling and circulation of extremely sensitive data primarily in electronic format. Such data is commonly utilised in both a supplier's internal and external working environments. For example, data used by a supplier to manufacture components in-house will be circulated internally, whilst data accompanying a supplier's outsourced processes will be circulated within an external third party working environment.

Protecting this data in internal and external environments requires operational discipline and rigorous IT system security procedures and controls. The onus for ensuring that sufficient system security procedures and controls are in place falls to the supplier (the company). Failure to implement, monitor, maintain and improve a secure IT environment can breach the requirements of the accredited bodies that must be adhered to. These are obligatory contractual requirements and any other additional customer specific demands. Major penalties may be incurred for breaches such as termination of a contract, loss of accreditations or in the most extreme cases legal disciplinary action.

1.4 Future business environment

There are only a limited number of companies based within Finland that are qualified to manufacture aerospace and defence equipment. Over the next decade it is anticipated that the company would undertake one or more large-scale contracts within these market sectors. At the time of writing this report, foreign multinational corporations were in advanced discussions to supply the Finnish defence forces via several long-term contracts for the upgrade of their existing aerospace equipment and defence systems. Such corporations are obliged to commit to an ‘offset agreement’ programme with one or more suppliers. This process starts by inviting a small number of qualified potential Finnish suppliers to prepare a tender submission – the company being one of these suppliers.

‘Offset agreements’ are the means by which the award of defence contracts by foreign governments or companies are arranged. They are conditional upon commitments from the defence contractor (supplier) to provide some form of compensation to the purchaser (BIS 2013). These agreements can include mandatory activities such as co-production, licensed production, subcontracting production, technology transfer, joint ventures, training and foreign investments (ACQ 2011) (BIS 2013).

Countries such as Finland often demand ‘offset agreements’ in order to gain economic benefits when spending large sums of government budgets to buy defence equipment from foreign suppliers (FT 2013). Benefits can include easing the burden of large defence purchases on the country’s economy, increasing or preserving domestic employment, obtaining technology transfer or promoting domestic industrial sectors and moderate a country's balance of trade (ACQ 2011).

The company has over twenty years of experience in the aerospace and defence industry and a good reputation in working with globally renowned corporations. They have an extensive list of prestigious successfully completed contracts, approvals to international standards, accreditations, expert levels of knowledge and an extensive range of manufacturing capabilities to draw upon. In addition, the company still retains unique export licenses for several key-manufacturing processes, which enables them to meet most of the more demanding contractual requirements and this has helped them to retain a strong competitive advantage.

The anticipated contractual opportunities will be far more demanding than any others undertaken previously. More complex manufacturing processes, a wide range of surface treatment procedures and more extensive assembly phases are expected. These larger-scaled contracts involve the manufacture of components that are linked into an assembly line chain with the production facilities of other suppliers. The extent of internal circulation and external exchange of sensitive documentation between the company and third party sub-contractors will be substantial. The majority of this documentation will be in electronic format and can include highly confidential detailed design drawings, manufacturing procedures and supporting technical specifications. All of this data must be handled safely, securely and under a strict set of guidelines to ensure that both integrity and confidentiality of the data is preserved in accordance with contract and/or signed NDA agreement and any customer specific requirements.

Although the company's senior management have identified a general need to evaluate and improve the existing relatively primitive levels of IT security, there is clear evidence that prospective contracts will demand much more stringent, advanced and secure IT systems. The IT infrastructure must be developed to adequately support the increased volume and movement of sensitive data traffic that will be expected from the larger and more onerous aerospace and defence contracts. This data traffic will travel through internal and external working environments.

1.5 The need for improved information system security

A considerable step-change is needed to re-build the company's simple office standard IT system security. Senior management has accepted the urgent need for the company to invest in the assessment, development and improvement of the existing information and network security infrastructure for the following key reasons:

- To meet the demanding technological advances needed to maintain a business connection with the specialist aerospace and defence industries.

- To meet the demanding requirements needed to qualify for the more stringent, prestigious and higher value aerospace and defence contracts.
- To develop and maintain the company’s own information security management system (ISMS) to ensure internal confidence and safety amongst company personnel.
- To keep the company at the forefront of technology and ensure continual improvement and investment in IT related activities.

There is an urgency to strengthen security procedures to assist with the projected future growth and success of the company. Development and improvements of the IT system security will strengthen the company’s compliance with standards and accreditations. The changes will also aim to reinforce compliance with the obligatory contractual requirements and customer specific demands for information security. This will establish a benchmark standard to reassure both present and potential business partners and also benefit company personnel by creating a safer, faster and more efficient internal IT working environment.

1.6 Purpose of this research project

The purpose of this research project was to perform a thorough information security risk assessment (ISRA) on the company's existing IT infrastructure including the network and system security provisions. The evaluation involves the careful selection and use of an established risk assessment framework that has evolved through industry best practice and has been adopted by similar sized companies with similar IT security challenges. By using a tried and tested assessment methodology the intention was to clearly identify any shortcomings in the current security system and propose a detailed plan of action to mitigate any identified risks. The plan of action would provide guidance with rebuilding and improving the IT system security infrastructure and establish a safer and more secure overall operating environment.

When formulating the original scope for this research project, senior management assigned an investment budget to support and fund the ISRA evaluation processes and the implementation of key improvement changes which included:

- Human resource support, when needed, to assist the ISRA tasks and to attend regular project development meetings throughout all phases of the research project.
- Human resource support, when needed, to assist with performing any of the necessary minor hardware upgrades to improve the existing IT system security.
- The option to draw upon the support of professional IT server and storage specialists to assist with performing the more complex major hardware upgrades to improve the existing IT system security.
- The option to draw upon the support of external specialist assistance to perform, for example, customised tests on the upgraded IT systems to identify any potential security weaknesses.
- Human resource support, when needed, to assist with the creation of the necessary information security policies.
- The option to draw upon the support of professional training services to provide a suitable IT security awareness programme for all in-house personnel.
- Human resource support, when needed, to assist with the monitoring and continual improvement of the updated IT system security.

However, at the time of performing the preliminary stages of the ISRA the scope of the original project as outlined above was adjusted and significantly reduced. Due to unforeseen circumstances, senior management was advised by the board of directors to rationalise the human resources and funding available to support this research project. The amended scope required a more streamlined and analytical focus. Except for the most critical issues, the implementation of all new IT system security controls was suspended. Although the more complex IT infrastructure upgrade plans were to be temporarily placed on hold the low cost upgrading would be explored on a case-by-case basis. No major IT investments were authorised at the time of conducting this research project and writing this final report.

The research project was conducted by an employee of the company (the researcher) who had direct experience developing and working with the IT infrastructure and had previously participated in many AS and ISO annual audits. The researcher worked closely with other key personnel within the company including senior management. Regular progress development meetings were held between different internal departments in order to draw upon the best 'in-house' expertise and to openly share information. The practical research needed to complete the project objectives was completed in stages over a mutually agreed period of time. These research objectives are outlined in chapter two of this report.

Company business operations that are reliant on the IT system infrastructure were not to be disrupted during predefined working hours. It was essential that the researcher and any other parties assisting company personnel should cause the least amount of disruption to daily business operations. For these reasons, each and every phase of the project was programmed to an agreed timetable with all supporting human resources being informed well in advance. In addition, some of the practical elements of research were completed outside of the two busier daytime working shifts, which ran from 7am until 11pm. This avoided any hindrance to the employees and interruptions to the flow of the research process.

2 RESEARCH GOALS, OBJECTIVES, AND DESIGN

2.1 Research goals

The goal of this research project is to provide a practical and theoretically sound framework of requirements to assist the company in understanding the importance of matching their IT information security systems with the highly demanding stipulations for the specialist precision engineering work they are engaged with in the aerospace and defence industries. By implementing and managing improved information system security controls recommended as a result of this research the company will be able to meet the increasing onerous business challenges it will face in the future.

2.2 Research objectives

The main objectives of this research project are to:

1) Identify, present and discuss the company's information security risk status by undertaking an appropriate risk assessment procedure with regard to standards, binding contractual obligations and customer specific requirements being adhered to by the company. Show how these industry specific requirements have affected the way that the information systems security has been shaped and how it will be developed for the future.

2) Understand the relevance of the identified criteria and their interaction, and select an appropriate industry standard information security risk assessment (ISRA) framework for developing improved information system security controls.

3) Perform an ISRA on selected areas of the company's existing IT infrastructure to collect data and understand how the component parts of

the company’s IT systems assist with their daily business functions and the impact on the business should these fail due to breaches of security.

4) Propose a development plan from the results of the ISRA to assist the company with the implementation of the necessary information system security control improvements and an information security awareness training programme across the company.

2.3 Research design

From the outlined research objectives the main focus of this research project was to perform an ISRA of the company’s existing IT infrastructure. The completed assessment would provide recommendations for improving and rebuilding identified problem areas together with a proposed timeline formulated for their planned implementation. To help achieve the research objectives a research design was carefully planned and would be followed throughout the course of the project.

A research design is a systematic plan to study a scientific problem. Myers (2013, 19) explains that the main purpose of research design is to provide a *‘road map’* for a research project. Collis and Hussey (2007, 111) continue to describe how it enables project procedures to be planned in detail that are used to guide the focus of research and get the most valid findings. The creation of a research design involves deciding upon all of the various components of the research project, which include the philosophical assumptions, the research method, the data collection techniques, the methods used to analyse data, the approach used for writing up the project and how the findings are published (Myers 2013, 19-20). Table 1 on the following page summarises some of the various possibilities for designing a positivist or interpretivist research project.

Table 1. A brief summary of options for designing a research project (Myers 2013, 27) (Collis and Hussey 2009, 74).

Philosophical assumptions ⇩	Positivist	Interpretivist
Research method ⇩	Surveys Experimental studies Laboratory experiments, etc.	Action research Case studies Grounded theory, etc.
Data collection technique ⇩	Experiments Quasi-experiments Tests and Scales, etc.	Interviews Fieldwork Document analysis, etc.
Data analysis approach ⇩	Modelling Statistical analysis Simulation, etc.	Hermeneutics Semiotics Narrative analysis, etc.
Written record ⇩	Thesis Research report Journal article, etc.	Thesis Research report Journal article, etc.

A finalised research design outlines clear guidelines and procedures with regard to what is intended in the project and when this will be done. However, while the steps summarised in table 1 cover an idealised overview of the different design process options, it must be noted that in actual practice it will not always be so straightforward. Myers (2009, 19) points out that to a certain degree, a researcher should be flexible and willing to make small adjustments to the design as the research project progresses.

2.4 Identifying the research paradigm (philosophical framework)

Once the formulation of the research topic, project purpose and objectives were firmly established the next step was to investigate and identify a research paradigm that would provide the best possible guidance to the research project. In order to select a suitable research paradigm, it was first crucial to examine the core philosophical assumptions that underpin them. Finding the assumptions that best aligned with the research project objectives was the primary concern.

After this, assumptions made a clearer picture of which research paradigm to select. The assumptions that were weighted more towards a particular research paradigm influenced its selection to guide the project.

A research paradigm is an established model or philosophical framework that is accepted by a substantial number of people in a research community. Collis and Hussey (2009, 55) define it as a “constructive framework that guides how research should be conducted, based on people’s philosophies and their assumptions about the world and the nature of knowledge”. Davidson (1998, 1-3) emphasises how these philosophies and assumptions will directly affect the way in which data regarding a phenomenon should specifically be gathered, analysed and used. Through the views of Morgan (1979), Collis and Hussey (2009, 57) describe how a research paradigm can be used to provide research guidance at three different levels:

- At the ‘philosophical level’, where the term is used to reflect the basic beliefs about the world we live in.
- At the ‘social level’, where the term is used to provide guidance about how the researcher should conduct his or her endeavours.
- At the ‘technical level’, where the term is used to outline the methods and techniques, which should ideally be adopted when conducting the research task.

The two major research paradigms identified in traditional science are positivism – an objective approach (sometimes called scientific), and interpretivism – a subjective approach (also known as anti-positivist) (Galliers 1992, 144-46). The positivist approach is usually associated with natural science research whereas the interpretivist approach is linked more with social science research. Whilst natural sciences are the disciplines that study objects or processes of the physical nature by means of scientific methods, the social sciences are concerned with society and the relationships among individuals within society.

Both research paradigms contain adverse approaches and assumptions about knowledge and operate at opposite ends of the research spectrum.

Table 2. Assumptions of the main paradigms (Collis and Hussey 2009, 58-61).

Philosophical assumption	**Positivism**	**Interpretivism**
Ontological assumption *(the nature of reality)*	Social reality is objective and singular. It is concrete and separate from the researcher.	Social reality is subjective and multiple. It is a projection of human imagination.
Epistemological assumption *(what we accept as valid knowledge)*	Researcher independent of what is being researched.	Researcher interacts with that being researched.
Axiological assumption *(the role of values)*	Research is value-free and unbiased	Researcher acknowledges that research is value-laden and biases are present
Methodological assumption *(the process of research)*	Deductive process. Quantitative research. Context free research.	Inductive process. Qualitative research. Context bound research.

Table 2 provides a brief summary of the primary philosophical assumptions that underpin the positivist and interpretivist paradigms, which are then discussed in further detail in the forthcoming sub-sections.

2.4.1 Positivism

Positivism was the first of the two paradigms to emerge and has been described as the natural science research model for the study of social phenomenon (Lewis and Ritchie 2003, 6). Based on the principles of realism, positivist research is underpinned by the ontological assumption that social reality is objective and singular and is not affected by the act of investigating it (Collis and Hussey 2009, 56). Collis and Hussey (2009, 59) outline that positivist research is value free and unbiased since the researcher tries to maintain an independent and distant stance from what is being researched.

Myers (2013, 38) describes how positivist researchers assume that reality is objectively given with the belief that only phenomena that are observable and measurable can be validly regarded as knowledge. Since it is assumed that social phenomenon can be measured, positivism is associated with quantitative statistical and mathematical methods of analysis (Collis and Hussey 2009, 56). Examples of quantitative analytical methods include survey methods, laboratory experiments, formal methods (e.g., econometrics) and numerical methods such as mathematical modelling (Myers 2013, 7).

Positivist research involves a deductive top-down process with a view to obtain knowledge in an attempt to try and increase the predictive understanding of social phenomena. The deductive process begins by examining scientific theories in order to produce hypotheses from them, which relate to the focus of the research (Greener 2008, 16). This proceeds to experimentation and empirical testing to prove or disprove the created hypotheses and accumulate verified facts. The results are then used to generate new theory by putting the facts and values together to establish causal ‘law-like’ generalisations that apply regardless of context (Greener 2008, 16) (Myers 2013, 40).

2.4.2 Interpretivism

Interpretivism is a paradigm that emerged in response to the perceived inadequacy of positivism to meet the demands of social scientists and sees society as being totally different from natural sciences. Whilst positivism is based on the principles of realism, interpretivism has its roots in idealism. Interpretivist research is built on the ontological assumption that social reality is multiple and subjective and that the act of investigating social reality will have an effect on it because it is shaped by our perceptions. (Collis and Hussey 2009, 56-60)

Myers (2013, 39) explains how “interpretive researchers assume that access to reality (given or socially constructed) is only through social constructions such as language, consciousness, shared meanings and instruments”. The interpretive researcher aims to see the world through the eyes of the people being studied, allowing them multiple perspectives of reality, rather than the single reality described in the positivist approach (Greener 2008, 17). Although this form of research is value-laden, biases are present since the researcher interacts with that being researched and it is impossible to separate what exists in the social world from what is in the researcher's mind (Collis and Hussey 2009, 57).

Interpretivist research involves an inductive bottom-up process. Unlike positivism, which primarily focuses on measuring of social phenomena, intepretivism focuses on exploring the complexity of social phenomena with a view to gaining interpretive understanding. The researcher looks to develop generalisations that are more context-bound and closely related to the researcher and his or her research methods (Myers 2013, 40).

Interpretivists adopt a range of methods that seek to describe, translate and come to terms with the meaning of naturally occurring phenomena in the social world. Interpretivism is associated with qualitative analysis since the research is less concerned with the frequency of phenomena and the findings are not derived from the statistical analysis of quantitative data (Collis and Hussey 2009, 56-8). Examples of qualitative data sources include observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and reactions (Myers 2013, 8).

2.4.3 The chosen research paradigm – Interpretivism

Of the two major research paradigms appraised in this report, the philosophical assumptions that form the basis of interpretivism were more in balance with the context of this research project. The ontological, epistemological and axiological assumptions from an interpretivist viewpoint better support the completion of the research objectives. With reference to table 2, Collis and Hussey (2009, 59) discuss how the first three assumptions are interrelated. This means that if one of them is accepted within a particular paradigm and the other two assumptions for that paradigm are complementary.

Ontology and its assumptions are concerned with the nature of reality. The knowledge acquired by the interpretivist approach is subjective and socially constructed, i.e., shaped by human perception. Because the interpretive researcher aims to see the world through the eyes of the people being studied this enables him or her to view multiple perspectives of reality. During the initial stages of this research project it was first necessary to observe, monitor, and attempt to understand how company personnel made use of the existing IT infrastructure and systems on a day-to-day basis. Dependent on their job requirements and level of authority the reliance and interaction with these IT systems significantly differed from person to person. Because of the broad spectrum of human interaction with the IT framework there were numerous different perspectives of reality viewed by the researcher.

Epistemological assumptions are concerned with what we accept as valid knowledge and examine the relationship between the researcher and that being researched. Unlike positivist researchers who believe that the researcher should maintain an independent stance from that being researched, interpretivists attempt to minimise the distance between the researcher and that being researched. Chapter one of this report identified that this research project was carried out by an internal employee of the company. In order for the researcher to investigate the existing IT infrastructure, complete an ISRA and implement the crucial security adjustments it is essential that the researcher shall follow and interact within all process and development changes. Due to the interactive, cooperative and participative nature of the research it was impossible to divide the interaction between the researcher and the subject in hand.

From an epistemological perspective, Myers (2013, 39) explains that the interpretivist researcher enters the field with some form of prior understanding of the research context. He or she should then attempt to look at the subject matter from an inside perspective rather than from an outside perspective looking in. Before starting this project, the researcher had already worked in the company for several years. In addition, the researcher had gained experience working with the existing IT framework, had participated in IT development discussions, had an understanding of the social and cultural behavioural patterns within the company and had a sufficient level of knowledge about the research topic in hand. All of these attributes align the researcher with the epistemological assumptions that underpin the interpretivist paradigm.

Axiological assumptions are concerned with the philosophical study of value. Interpretivists believe that since reality is mind constructed, mind dependent and knowledge subjective then social inquiry is ‘value-laden’. Interpretive researchers are influenced by their values, which inform the methods chosen to collect and analyse data by their interpretation of the findings and in the way the findings are reported. The researcher admits the ‘value-laden’ nature of the study and reports values and biases. As an employee of the company and being directly involved in the research objectives the researcher’s mind-set, personal values and experience will always influence the research results and cannot be separated. Due to these influences on the researcher the axiological assumptions that underpin the interpretivist paradigm are suited to this form of research project.

2.5 Identifying the research methodology

Based on the chosen interpretivist research paradigm the next phase of the project was to determine the research strategy. This meant selecting a suitable research methodology that broadly reflected the core philosophical assumptions of interpretivism. In addition to this the research methodology defined the best means or modes of data collection, which after analysis, were used to create an eligible plan of action to best solve the predefined research objectives.

A research methodology can be defined as the systematic, theoretical analysis of the methods applied to a field of study. It forms the general research strategy that outlines the way in which a research project is to be undertaken and identifies the methods and procedures to be used in it (Howell 2013, 58). Rajasekar (2013, 5) explains how these identified methods and procedures define how a researcher manages his or her work of describing, explaining and predicting phenomena to gain knowledge.

There is a wide range of research methodologies for collecting and analysing research data with various ways to classify and characterise their different types. However, one of the most common distinctions is between the positivist's quantative research approach and the interpretivist's qualitative research approach. Table 3 lists some of the main methodologies that are associated with the positivist and interpretivist paradigms. (Myers 2013, 7-8)

Table 3. Research methodologies associated with the two main paradigms (Collis and Hussey 2009, 74) (Myers 2013, 8).

Positivist – Quantitative research (A focus on numbers)	**Interpretivist – Qualitative research** (A focus on text)
Surveys Experimental studies Laboratory experiments Mathematical modelling Structured equation modelling Statistical analysis Simulation	Action research Case study research Ethnography Grounded theory Semiotics Discourse analysis Hermeneutics Narrative and metaphor

Although the above list is not exhaustive the methodologies mentioned are the most commonly used in social and natural science research. Since the interpretivist paradigm had already been chosen for the context of this project the methodologies listed in the interpretivist column of the table were investigated for their compatibility and suitability to provide the work plan for the research.

2.5.1 Action research

Collis and Hussey (2009, 81) describe action research as a methodology used in applied research to find an effective way of bringing about conscious change in a partly controlled environment. Unlike other research methodologies, where the researcher seeks to study organisational phenomena but not to change them, the action researcher is concerned to create organisational change and to simultaneously study the process (Baskerville and Myers 2004, 329-30). The main role of an action researcher is to assess a situation, attempt to bring about a change and then monitor the results (Collis and Hussey 2009, 81).

Action research is situation-based, context-specific and undertaken by individuals with a common purpose (Koshy and Waterman 2011, 3). The research combines theory and practice through change and reflection (Avison et al. 1999, 94). The process involves action, evaluation and critical reflection. Based on the evidence gathered changes in practice are then implemented (Koshy and Waterman 2011, 3). It is a highly participatory research methodology with a close collaboration and synergy between the researcher and subject. Theorising is shared between researchers and client participants with each bringing their distinctive sets of knowledge into the action research process (Baskerville and Myers 2004, 330). The research findings emerge as the action develops, but these are not conclusive or absolute.

The philosophical assumptions that underpin action research are that the social world is constantly changing and that both the researcher and the research undertaken are part of this change (Collis and Hussey 2009, 81). Action research is an iterative process of enquiry involving researchers and client participants acting together on a particular cycle of activities, including problem diagnosis, action intervention and reflective learning (Baskerville and Myers 2004, 330-1). As a sequence of events, the research works through a cyclical four-step process of consciously and deliberately (1) constructing, (2) planning action, (3) taking action and (4) evaluating the action. This leads to further planning (constructing) and so on (Coghlan and Brannick 2010, 8). A simplified model of this cyclical four-step process is illustrated in figure 1 on the next page, commencing with a pre-step of ‘context and purpose’.

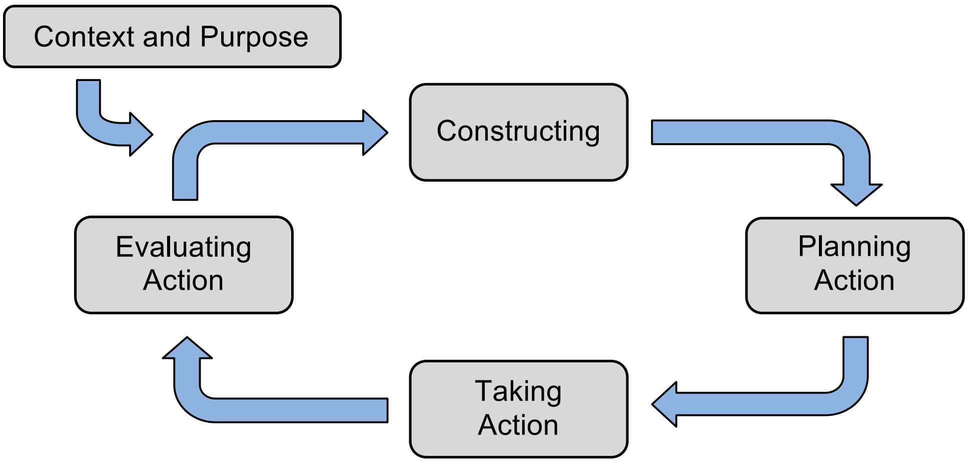

Figure 1. The action research cycle (Coghlan and Brannick 2010, 8).

The action research cycle unfolds in real time and begins with a pre-step which seeks to understand the ‘context and purpose’ of a project. From an external perspective questions are raised to assess the economic, political and social forces that drive change whilst from an internal perspective the cultural and structural forces are examined. The assessment of these forces identifies their source, potency and the nature of the demands they make on the system. The pre-step also requires consideration of the collaborative relationships between those who have ownership or need to have ownership of the above influences. (Coghlan and Brannick 2010, 8)

The first step of the cyclical four-step process is focused on *‘constructing’* what the issues are on the basis of actions to be planned and taken. The constructing process is a collaborative venture between the action researcher and other participants. The second step involves *‘planning action’* in order to prepare for the action to be implemented. It is a consistent follow-on from the exploration of the context and purpose and ‘constructing’ the issues. The third step moves onto *‘taking action’* where the plans are implemented and interventions are made collaboratively. The fourth and final step of the research cycle is concerned with *‘evaluating’*. The intended and unintended outcomes of the action taken are examined in order to identify if the original ‘constructing’ fitted its purpose, if the actions taken matched the ‘constructing’, if the action was conducted appropriately, and to determine what is fed into the next research cycle. (Coghlan and Brannick 2010, 8-10) (McNiff 2013, 57-8)

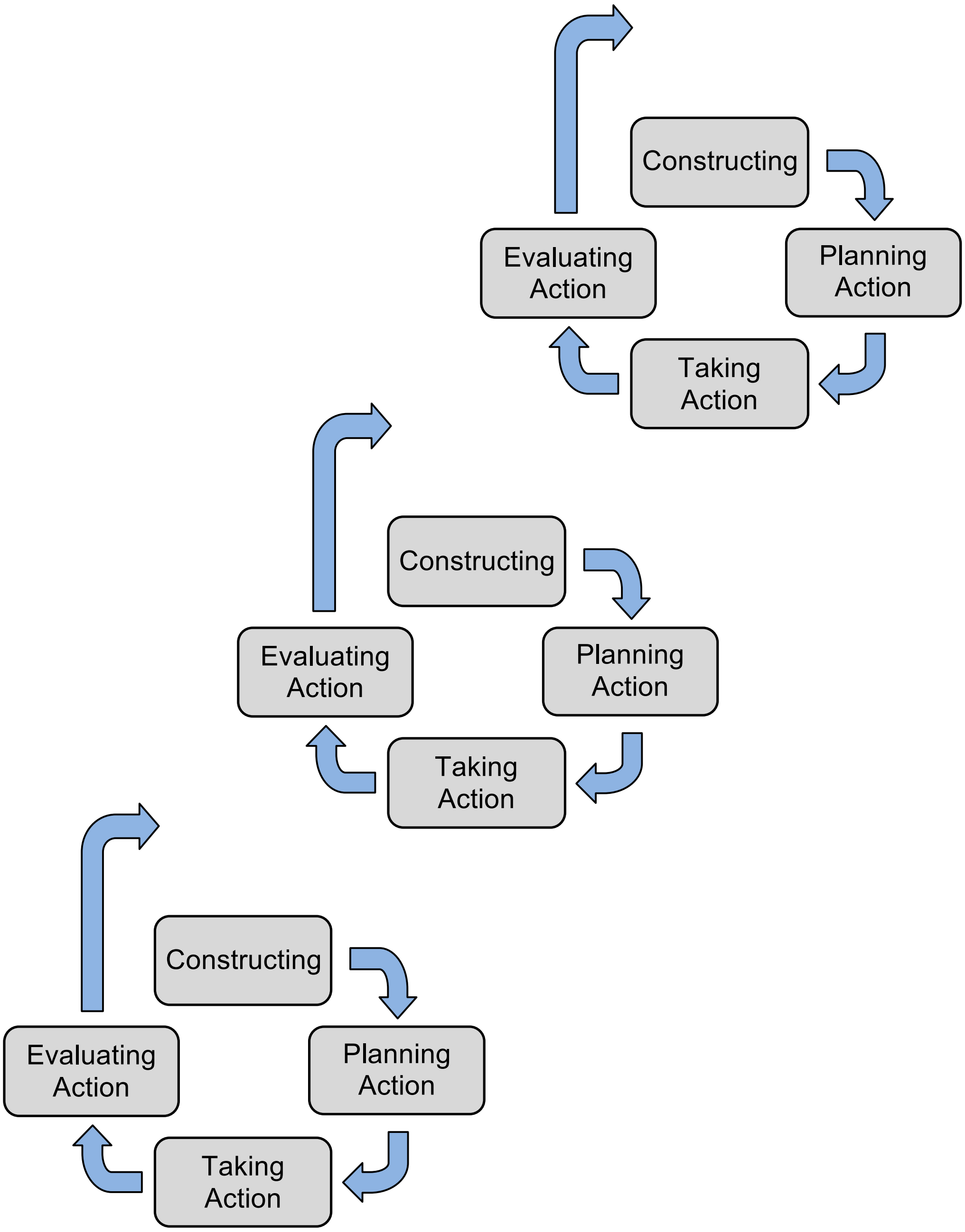

Figure 2. A spiral of action research cycles (Coghlan and Brannick 2010, 10).

Coghlan and Brannick (2010, 10) emphasise that in any action research project there are multiple action research cycles operating concurrently. The research process creates a spiral of self-contained cycles each involving further constructing, planning, acting, and evaluating (reflecting). Illustrated in figure 2 the spiral model of cycles provides a researcher with the opportunity to visit a phenomenon at a higher level each time and so to progress towards a greater more focused overall understanding of the research problem at hand.

2.5.2 Case study research

A case study is a traditional, systematic and versatile research methodology involving the exploration of events, collection of data, analysis of information and reporting of the results (Wilson 2013, 257). It is an approach that enables a researcher to obtain in-depth knowledge by examining and understanding a complex social phenomenon (the case) in its natural setting within a particular context. Case study research is context driven and can involve either single or multiple cases with numerous levels of analysis (Eisenhardt 1989, 534). Yin (2014, 4-5) describes how a variety of methods are used to allow the researcher to focus on a “case” and retain a holistic and real-world perspective. The case may be a particular business, a group of workers, an event, a process, a person, or other phenomenon (Collis and Hussey 2010, 82).

Case study research is very useful when trying to test theoretical models by using them in real world situations (Eisenhardt 1989, 534). It involves a more realistic, detailed and often intensive study of a particular situation rather than a sweeping statistical survey. It is a method used to narrow down a very broad field of research into a more easily researchable topic. Case studies allow a lot of detail to be collected that would not normally be easily obtained by other research designs. The data collected is typically of better quality than can be found using other experimental designs. Whilst a case study will not answer a question completely it will give some indications and allow further elaboration and hypothesis on a subject. (Shuttleworth 2014).

Dependent on the type of research questions and their goals there are different types of case study design to choose from and in some instances one type may be combined with another. The selection of a specific case study design is guided by the overall study purpose (Baxter and Jack 2008, 547). Collis and

Hussey (2010, 82) explore six different types of case study that are commonly used in research as summarised below.

- Exploratory case studies – where there are few theories to support the research case or there is a deficient body of knowledge.
- Descriptive case studies – where the research objective is restricted to describing an intervention or phenomenon and the real-life context in which it occurred.
- Illustrative case studies – where the research attempts to illustrate new and possible innovative practices adopted by particular companies.
- Experimental case studies – where the research examines difficulties in implementing new procedures and techniques in an organisation and evaluating the benefits it brings.
- Explanatory case studies – where existing theory is used to understand and explain what is happening.
- Opportunist case studies – where the opportunity to examine a phenomenon arises since the researcher has access to a business, person or other case. (Collis and Hussey 2010, 82) (Baxter and Jack 2008, 547-8)

The main stages in a case study involve (1) selecting the case, (2) preliminary investigations, (3) data collection, (4) data analysis and (5) writing up the conclusions from the case study material. Case studies typically combine data collection methods such as archives, interviews, questionnaires and observations with the evidence being qualitative, quantitative or a mixture of both.

2.5.3 The chosen research methodology – Case study research

After selecting the interpretivist paradigm for its suitability to guide this research project the common research methodologies associated with interpretivism were thoroughly investigated. From the corresponding methods listed in table 3, the action research and case study methodologies were shortlisted for further detailed review. Both approaches were then scrutinised to determine which would provide the best fitting and most efficient way to successfully meet the research project objectives.

The first chapter of this report described how unanticipated circumstances within the company had resulted in a number of sudden changes being made to the originally approved project scope. At the time of completing the preliminary background work for the ISRA, senior management in the company instructed that the research project objectives were scaled down and redefined to exclude the more costly practical tasks. The excluded tasks were; the investment in implementing tighter information security controls, the necessary software and hardware upgrades and an information security awareness-training programme. The previously defined research objectives listed at the start of this chapter were considerably reduced to concentrate on the IT assessment and improvement proposition stages.

Based on the original broader project scope, the action research methodology would have been selected for its suitability to guide how the research should be conducted. Collis and Hussey (2010, 81) clearly define the role of an action researcher as being to enter into a partly controlled environment, implement change and to then monitor the results. They also state that action research encourages a close collaboration and synergy between the researcher and subject, which is implicit with the demands of this research project.

In order to complete the original scope, an employee of the company (the researcher) was to perform an ISRA of the existing internal IT environment, propose an implementation plan for the recommended changes, implement the finalised changes, and then evaluate and continually monitor them to measure their improvement. All of these tasks are performed within the company’s internally controlled IT environment which is continually influenced and developed to meet the essential demands of the accredited bodies adhered to, the obligatory contractual requirements and any other additional customer specific demands.

However, a more limited and streamlined research approach was required, due to the narrowed project scope, which removed the practical upgrade implementation and the post-practical evaluation and reflecting stages. As previously illustrated in figure 1, an action research cycle involves constructing, planning action, taking action (implementing) and evaluating (reflecting) action. This leads to further similar cycles with each cycle feeding into the next. The revised project scope meant that the latter two steps of the cycle, which involved taking action and evaluating action, would no longer be completed.

With only half of the original four-step cycle in operation, the action research methodology becomes partially ineffective. Koshy and Waterman (2011, 5) explain how the concept of spiralling action research cycles are used to provide a researcher with the unique opportunity to investigate a problem at a higher level each time. This enables the researcher to progress towards a greater overall understanding of a particular research problem within a specific context and to make informed decisions through this enhanced understanding.

The reduced project scope significantly diminished the overall benefit of using action research. With no practical real-life changes to be implemented the reflective learning process driven by change was also removed. With these factors taken into consideration the ‘action research methodology’ took second preference over the ‘case study methodology’, which was adopted for its suitability to gather the relevant in-depth knowledge and still meet the objectives.

For the purposes of this project the defining beneficial feature of selecting the case study methodology is its holistic ‘company-wide’ research approach. It provides the researcher with a more robust, realistic and in-depth understanding of a research problem. It assists with capturing all of the details of a particular phenomenon relevant to the purpose of the study and within a real-life context. Eisenhardt (1989, 534) emphasised how case study research is very useful when trying to test theoretical models by using them in a real-life context. Eisenhardt’s statement supports the intended use of an industry standard ISRA theoretical framework or model to assess the company’s existing IT arrangement. The real-life context of the research lays in the risk assessment process, which examines selected areas of the internal IT environment used by company personnel on a day-to-day basis in their natural setting.

Case study research enables a broad research field to be condensed into a more manageable research topic whilst retaining a high level of data collection. The research involves a more intensive study of a particular situation or specific cases rather than a sweeping statistical survey. With the company's IT environment covering such a broad research area it was necessary to limit the research but still ensure valid assessment results. Specific yet different areas (cases) of the IT environment were targeted for thorough assessment based on the influential accreditations, contractual requirements and customer demands. The case study approach supports the project by conducting a more streamlined case-specific research process to meet the defined objectives.

With case study research the researcher is able to go beyond quantitative statistical results and understand the behavioral conditions through the actor's perspective. This again supports another of the outlined research objectives of this research project to find and understand the relationships and interaction between company personnel and the IT environment. This, along with the data gathered from the ISRA will contribute to identifying the final IT system development proposals.

Collis and Hussey (2010, 82) identified six different types of case study that are commonly used in research. Since any one type can be combined with another, the exploratory and explanatory case types were selected. Exploratory case study research is used where there is a clear lack of knowledge and understanding of particular areas of the company's IT environment that need to be investigated. Explanatory case study research is used when an existing theory or framework is employed to understand and explain what is happening. In this instance, an ISRA theoretical framework will be used as a tool to confirm whether systems are or are not performing as expected or required.

3 EXISTING COMPANY IT INFRASTRUCTURE, ISRA METHODS, STANDARDS AND OBLIGATORY REQUIREMENTS

3.1 Existing IT infrastructure and its supporting role

The IT infrastructure forms the backbone of the company. Twenty-five PC workstations connect to an internal server via the corporate LAN. The server is primarily used for file sharing and stores several gigabytes of extremely sensitive data in electronic format for both active and inactive aerospace and defence contracts. This data includes manufacturing drawings, design specifications, CNC machining programs, assembly procedures, test reports, binding contractual information, NDA agreements and similarly valuable content. Dependant on the level of authority granted, personnel throughout the organisation are able to access particular parts of this data via their individual PC workstations. In addition to its basic file-sharing services, the server also stores two important databases for the company's 'Ventus' ERP and 'Fadector' FMS software systems. These two systems are crucial in supporting the company in its day-to-day business activities.

The 'Ventus' ERP system is a business management software used to manage the primary business functions within the company (Nisamest 2013). The software provides a centralised information control system to integrate all internal and external management information across the entire organisation (Krmac 2011, 591). This information includes financial accounting, management accounting, sales, human resources, project management, manufacturing, and supply chain management activities (Aptean 2013). ERP facilitates the flow of information between the company's primary business processes within the boundaries of the company and is also utilised to enable external connections for authorised outside stakeholders (Roots Infocomm 2011).

The ‘Fadector’ FMS is used for collecting shop-floor production data. The software monitors the status of the CNC machine tools and provides both graphical and numerical statistics on their operation (Fastems 2012). Key performance indicators are selected and used to measure performance against a goal (Turban et al. 2011, 298). Data such as machine utilisation, machine availability, machine cycle times, mean time between failures, overall equipment efficiency and on time delivery are collected, measured, recorded and made openly available through the software interface (InSolution 2014). Senior management and the production managers have access to the ‘Fadector’ software on their PC workstations. They use the collated data to analyse, plan and improve manufacturing activities such as delivery reliability, decrease of costs, reducing inefficiencies, increasing capacity and the overall effectiveness of the labour force.

3.2 Existing ISRA methods in place

Prior to the start of this research project, the company’s existing mechanisms for performing information security risk assessments were relatively primitive and troubled with inconsistencies. There were no rigorously documented procedures or an industry standard framework utilised to conduct on-demand risk assessments. Many important risk areas were frequently missed or insufficiently analysed. Most of the risks identified were only partially mitigated with senior management accepting short-term solutions to bypass the problem area and focus on continuing business operations as fast as possible.

In instances where risks were mitigated, no follow-up activities or monitoring programmes were used to assess if the implemented corrective actions had been successful. With no refined assessment process in place the overall IT infrastructure was susceptible to potentially critical openings that could allow the integrity of the systems security to be defeated. With such openings not being properly addressed the systems were very vulnerable. A breach in the IT systems security would not only compromise the safety of the company, but could also undermine previous and current aerospace and defence contracts.

Despite the company’s healthy portfolio of prestigious global aerospace and defence contracts, their wide range of manufacturing capabilities, and a well-established desirable array of surface treatment processes the IT infrastructure did not complement this and remained severely underdeveloped. Although no major incidents such as data loss, system compromises or critical issues had been experienced to date, senior management had failed to acknowledge and address their reliance on this critical ageing resource. There was a lack of commitment to investigate, upgrade, monitor and maintain the IT infrastructure to adequately match and support the company’s growing business demands. Management were primarily focused on the investment in more machinery to increase manufacturing capacity without realising the importance of also upgrading the company’s IT infrastructure.

3.3 Existing standards and specialist requirements adhered to

The company currently adheres to the ISO and AS globally recognised standards, which are mandatory requirements for submission of a contract tender for the manufacture of any aerospace or defence component. In addition to these standards there are other specialist regulatory requirements from other aerospace and defence bodies that may apply. Each new manufacturing contract can also stipulate any other specific requirements that must also be adhered to. Compliance with these standards and requirements is reliant directly or indirectly on the integrity of the company’s IT infrastructure. They influence how the company should keep pace and develop its ISMS.

Before any industry standard ISRA framework could be assessed for its suitability to be used within the company, a review of the existing standards and regulatory requirements was conducted. By understanding the demand and influence that each standard or requirement had on the company, a foundation of information was formed that could be built upon in subsequent stages of this research project. Sub-sections 3.3.1 to 3.3.4 list and expand on each of the existing standards and requirements currently in place.

3.3.1 ISO 9001:2008 – QMS standard

The International Organisation for Standardisation (ISO) is the world's largest developer of voluntary international standards (ISO 2013a). The ISO 9000 family of standards is related to quality management systems (QMS). They provide guidance to help companies and organisations that want to ensure that their products and services consistently meet customer and applicable statutory and regulatory requirements ensuring that the overall level of quality is continually developed and improved (ISO 2013b).

ISO 9001:2008 (version 2008) is based on a number of QMS principles that include a strong customer focus, the motivation of and implications for senior management, the process approach and continual improvement (ISO 2013b). ISO 9001:2008 is one of the most widely used management tools in the world today. It is the only standard in the ISO 9000 family that can be certified and can be used by any organisation regardless of its size and field of activity (ISO 2013c). The standard also requires that an organisation must perform regular internal audits to monitor and benchmark how its QMS is functioning and performing (ISO 2013b).

ISO 9001:2008 certification is a basic mandatory requirement for any company participating in aerospace and defence contractual activity. Although the standard has very little focus on maintaining a safe and secure IT environment, it does demand a streamlined QMS, which for the company incorporates the use of supporting software platforms that are reliant on the IT infrastructure.

3.3.2 AS9100 – Aerospace QMS standard

Aerospace standard AS9100, sometimes referred to as BS EN 9100, is a widely adopted and internationally recognised QMS that has been specifically tailored by SAE to meet the demands of the aviation, space and defence industries (Praxiom 2013). The standard covers the entire supply chain, which includes companies that design and manufacture equipment, supply accessories or replacement parts, as well as those that offer supply and maintenance, or overhaul and repair services to the above mentioned industries (SGS 2013a). The standard is a mandatory requirement for any company participating in aerospace and defence contractual activity. Compliance is seen as assurance of a continuing commitment to meeting the stringent measures demanded by these industries (SGS 2013b, 3).

SAE International is a globally active professional association and standards organisation with their principal emphasis being placed in the aerospace, automotive and commercial-vehicle industries (SAE 2014a). SAE prepare AS9100 in collaboration with the international aerospace quality group (IAQG) who is a cooperative global organisation supported by companies throughout the aviation, space and defence industries (SAE 2014b). IAQG are committed to achieving significant performance improvements realised through the development of standards, industry oversight, and guidance materials for use in all levels of the supply chain.

AS9100 incorporates the entirety of the ISO 9001:2008 standard, while adding additional requirements specifically relating to quality and safety for aviation, space and defence organisations (AS9100 2009, 7). The formula shown in figure 3 clearly explains how the AS9100 and ISO 9001:2008 standards are related to one another.

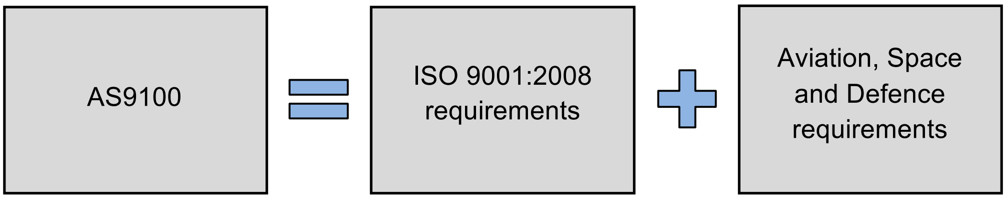
AS9100
=
ISO 9001:2008 requirements
+
Aviation, Space and Defence requirements

Figure 3. The AS9100 formula (Praxiom 2013).

Since aerospace standard AS9100 covers all of the scope contained within the ISO 9001:2008 standard it means that by auditing and receiving certification in meeting the demands of AS9100, compliance with ISO 9001:2008 is also awarded simultaneously (SAE 2014c). Similar to ISO 9001:2008, annual audits are compulsory but far more demanding within the aerospace industry. For example, any major non-conformance discovered during an audit would result in immediate suspension of the certification. This typically includes a halt in the production (work-stop) for any component manufactured under the accredited requirements and, if needed, previously delivered components must all be recalled for detailed inspection. A work-stop can potentially last many months.

3.3.3 Boeing – Special QMS requirements standard for suppliers

Boeing is the world's leading aerospace company and the largest manufacturer of commercial jetliners and military aircraft combined (Boeing 2013). They provide products and support services to customers in over 150 countries using a global network of Boeing accredited suppliers. In order to compete and win any manufacturing contract, Boeing requires that all suppliers must adhere to a preferred set of standards. They ensure compliance to the AS/EN/JISQ 9100 quality management systems standard, which covers the entire aerospace supply chain (SRI 2013).

AS/EN/JISQ 9100 is tailored for the aerospace industry and is coordinated by the international aerospace quality group (IAGQ). AS/EN/JISQ incorporates major elements of the IAQG sanctioned standards, which include AS9100, EN9100 and JISQ 9100 (Boeing 2011). The standard is primarily based on ISO 9001:2008 and AS9100, but includes over 100 other aerospace specific quality and reliability requirements (SRI 2013). The key focus areas are inspection, process-control, and information on documentation, testing and results. All of these areas typically include sensitive data that must be handled under an NDA agreement and have a strictly defined period of validity.

The company has several long-term contracts for the manufacture and assembly of Boeing aerospace components. The existing IT system infrastructure is used to store and access the associated electronic data on a daily basis.

3.3.4 Nadcap – Quality assurance standards for aerospace and defence

Nadcap (National Aerospace and Defence Contractors Accreditation Program) is a globally recognised accreditation program that focuses on achieving a tighter control over special processes within aerospace, defence and other closely related specialist sectors (Boeing 2010). Established in 1990, Nadcap is managed by technical experts and key personnel from globally renowned aerospace contractors, suppliers, and US government representatives (Keighley 2013) (PRI-Network 2013a).

The Nadcap program represents a concerted, cooperative effort to increase performance, improve safety and quality, and reduce costs throughout the global aircraft and defence supply chains. It defines a standardised approach to quality assurance and establishes requirements for accreditation. Comparable to other aerospace and defence accreditations, Nadcap requires compulsory audits that are organised by the Performance Review Institute (PRI). Expert auditors conduct technically in-depth assessments to ensure familiarity and adherence to the special processes in place. (Keighley 2013)

The company has active Nadcap accreditations for chemical processing procedures in accordance to AC7108 and NDT procedures in accordance to AC7114. Both of these comply with the global SAE aerospace standard AS7003 and are annually audited by PRI. Any non-conformity issues related to components manufactured under Nadcap approval will require more detailed investigative audits. Penalties for non-conformance to the standard are similar to those imposed within the AS9100 standard. A work-stop, product recall and temporary or permanent accreditation suspension are dependent on the severity of the non-conformance. (PRI-Network 2013b)

The company’s two Nadcap accreditations are for special surface treatment processes that are solely used for aerospace and defence components. All of the data generated from these processes is under a NDA. Documentation is usually in paper format but is scanned and stored electronically on the company server hard drives. It is a strict requirement for both of the accredited Nadcap standards that all records throughout the processing stages are recorded and safely retained for a defined time period, which means securely protecting and storing this electronic data.

3.4 Overall influence on the IT environment

Each of the preceding accredited standards and specialist requirements demand specific measures that are dependent on the company's internal IT environment to execute the tasks. The complexity of these demands and their reliance on the IT systems varies greatly. For example, an accredited standard may demand that detailed CNC calibration records are stored safely in electronic format for a defined 'shelf life', whilst a customer may stipulate that the company must install and maintain a specific software application that safely encrypts and transfers the project specific data between the two parties.

From the four main influential standards and requirements previously described, AS9100 is the most rigid, demanding and IT resource dependent of them all. The requirements of the ISO 9001:2008 standard are covered under the AS9100 scope. AS9100 is supported by document AS9101, which acts as a checklist for the customer and auditor who participate in the audit. At the time of conducting this research project, there was an increasing emphasis within the audit scope to focus on the management of information systems and data control. AS9101 section 4.2.4 – 'control of records' lists the following recent additions that must be addressed and adhered to:

- Electronic records of production origin, conformity and shipment must be maintained.
- Back-up procedures and document shelf life are defined for records stored in an electronic form.
- Electronic records shall be stored and secured safely and cannot be corrupted due to software or system changes. (SAE 2010, 27)

In addition to the IT related requirements in section 4.2.4, sections 7.5.1.2 and 7.5.1.3 – ‘control of production’ also require that the following procedures are addressed and adhered to:

- Production equipment, tools and computer software used to automate, control, or monitor manufacturing processes shall be validated, inspected, and updated periodically.
- Changes affecting equipment, tools, and computer software shall be controlled and documented. (SAE 2010, 42)

In addition to the above requirements outlined from the AS9100 and AS9101 documents, Boeing’s AS/EN/JISQ special requirement standard demands another 100 additional contract specific focus areas. Dependent on the complexity of the Boeing components to be manufactured, a contract will include the necessary corresponding focus areas that the company must adhere to in order to work on such projects. Similar to the AS9100 standard, some of these focus areas involve the reliance on the company’s IT systems to execute them.

A Boeing contractual agreement typically outlines the handling, storage and defined shelf life requirements for the project sensitive data circulated. For example, manufacturing drawings, design specifications and CNC programmes. All Boeing contracts are signed under an NDA agreement. At the time of writing this report the company was engaging in the manufacture and assembly of numerous components for several short and long-term Boeing contracts. Due to Boeing’s strict confidentiality policy, the specific focus areas outlined in the binding contractual agreements cannot be disclosed in this report.

All relevant requirements of the standards and any customer contract specific requirements dictate the basis on which the company’s information systems security will be developed and tailored from a present and future perspective. In addition to the defined research project objectives, the standard and contract specific requirements will be taken into account when selecting the appropriate ISRA methodology. The objective is to improve the information systems security for meeting accredited standards and contractual requirements for securing prospective business opportunities within the highly specialised aerospace and defence sector.

4 INDUSTRY STANDARD ISRA METHODS, GUIDES AND STANDARDS

4.1 Evaluating industry standard ISRA methods, guides and standards

With the world wide proliferation of complex and sophisticated threats to data security Information Security Risk Assessments (ISRA) have become an essential tool for organisations to employ as part of an overall comprehensive risk management program (NIST 2011, VII). Landoll (2011, 23) defines how a security risk assessment is an objective analysis of the effectiveness of the current security controls that protect an organisation's assets and a determination of the probability of losses if those threats were realised. The end result of the assessment is to ensure appropriate or strengthened levels of security for the appraised information systems.

Risk assessments are used to provide senior leaders and/or executives with the information needed to understand factors that can negatively influence operations and outcomes. It enables these decision makers to make informed judgments concerning the extent of the actions needed to reduce risk and to determine appropriate courses of action to take in response to identified risks (GAO 1999, 6). A security risk assessment is a continuous process of discovering, correcting and preventing security problems. In addition it is used to verify that the implementers and operators of information systems are meeting their stated security goals and objectives. (NIST 2010a, IX)

There are various industry standard best-practice security risk assessment models and methods available. Depending on the type of methodology employed a security risk assessment typically has numerous steps or phases each having a slightly different approach (Landoll 2011, 23). However, regardless of these differences all risk assessments generally include the following generic process phases:

- Threat identification – To identify threats that could adversely affect an organisation's critical operations and assets. Threats could include such things as disgruntled employees, intruders, criminals, terrorists, and natural disasters.

- Threat likelihood – To estimate the likelihood that such threats will materialise based on historical information and the judgment of knowledgeable individuals with relevant experience.

- Threat Identification – To identify and rank the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialise in order to determine which operations and assets are the most important to the organisation.

- Threat estimation – To estimate, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materialises including the recovery costs.

- Threat mitigation – To identify cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organisational policies and procedures as well as technical or physical controls.

- Threat documentation – To document the results and develop a plan of action to execute the changes needed. (GAO 1999, 6-7) (NIST 2011, 1)

The purpose considers standardised security risk assessment processes available. Appropriate internationally recognised security risk assessment methods, guides and standards are identified and investigated in order to understand their structure, their complexity and to assess possible challenges that may be faced when adopting any one of them. The cross-section of options was rationalised to four globally respected 'best-practice' options. These are 'COBIT' and 'OCTAVE' security risk assessment methods, the 'NIST SP 800' series of computer security guidance publications and the 'ISO/IEC 27000' family of international information security standards. The following sub-sections discuss each 'best-practice' option in further detail.

4.2 COBIT

Control OBjectives for Information and related Technology (COBIT) is a comprehensive IT governance control framework and supporting toolset developed by the IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). Since it was first published in 1996, COBIT has evolved to become the only industry standard framework that addresses the complete lifecycle of IT investment (ISACA 2013a).

The purpose of COBIT is to provide an up to date, internationally accepted set of IT governance principles, practices, analytical tools, models and controls to help increase trust in, and value provided by information systems within organisations (ITGI 2007, 9). Generic in format, the COBIT control framework can be applied across organisations of all sizes whether commercial, non-profit making or within the public sector. The framework is intended for day-to-day use in respect of:

- Executive management – to acquire value from IT investments and assist with balancing the risk and controlling investments in an often changeable IT environment
- Business management – to receive assurance on the management, security and control of IT services provided by internal or external parties
- IT management – to provide the required IT services that are needed to support the business strategy in a controlled and managed approach
- Auditors – to ratify their opinions and/or to provide better advice to management regarding the most suitable internal controls to implement. (Tarantino 2008, 181) (ITGI 2007, 25)

The logical structure of COBIT provides a mechanism to simplify the overall implementation process of an IT governance and control framework. It enables organisations to establish clear policies and good practice for IT controls in order to increase the value attained from IT-enabled resources in meeting business challenges and regulatory compliance. (ISACA 2013a, 1-6)

Released almost two decades ago, the COBIT framework has continually adapted to meet the demanding changes in the world of business and IT. Initially modelled as an IT auditing toolset for information systems COBIT has advanced through five major editions to become the leading globally-recognised framework for the governance and management of enterprise IT (Kadam 2012, 21). Figure 4 illustrates how each of the different iterations have progressively modified and extended the framework scope.

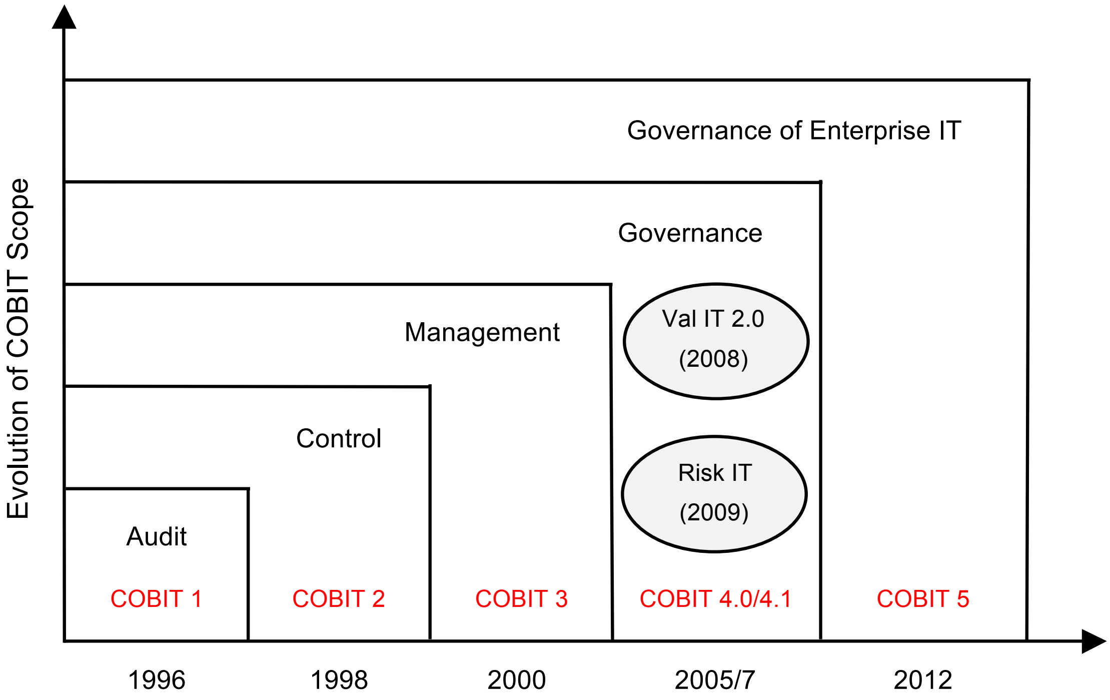

Figure 4. The evolution of COBIT frameworks (ISACA 2012a, 5).

Translated into many languages, all documentation, guidelines and support for COBIT 5 and COBIT 4.1 are openly available to download from ISACA's web pages. Published in 2007 and 2012 respectively, both editions are actively used across organisations across the world. Since initially released, COBIT's first, second, and third editions of the framework have all been developed, improved and consolidated into the fourth and then fifth edition. Due to their out-dated content and diminished online support and availability, COBIT's first three editions will not be investigated for the purposes of this research project.

4.2.1 COBIT 4.1: Control framework for IT Governance and Control

Prior to the initial release of COBIT 4.0 in 2005, the third edition of the series was active for five years (2000–2005). During the lifecycle of COBIT 3, ITGI elaborated on the existing business objective principles in greater detail and introduced the concept of IT governance into the framework. As enterprises increasingly understood the significant impact that information and IT systems had on business success the need for an industry standard IT governance control framework became apparent (ITGI 2007, 9). With growing demand COBIT 4.0 was developed to meet these IT governance requirements.

Two years after COBIT 4.0 was published a revised edition was introduced in 2007. COBIT 4.1 represented a fine-tuning of COBIT 4.0 to include enhanced performance measurement methods, improved control objectives and better alignment with business and IT goals (IIA 2013). In addition two further publications by ITGI were developed to support COBIT 4.1 in 2008 and 2009. The first was the Val IT framework for business technology management and the second was the Risk IT framework for the management of IT related business risks (Kadam 2012, 21).

The COBIT 4.1 framework is business-focused, process-orientated, controls-based and measurement-driven. The business orientation of COBIT aligns business objectives with IT goals. Demonstrated in figure 5 on the next page, COBIT achieves a sharp business focus by managing and controlling IT resources following a structured set of IT processes. This delivers the required enterprise information services needed to effectively achieve the business requirements.

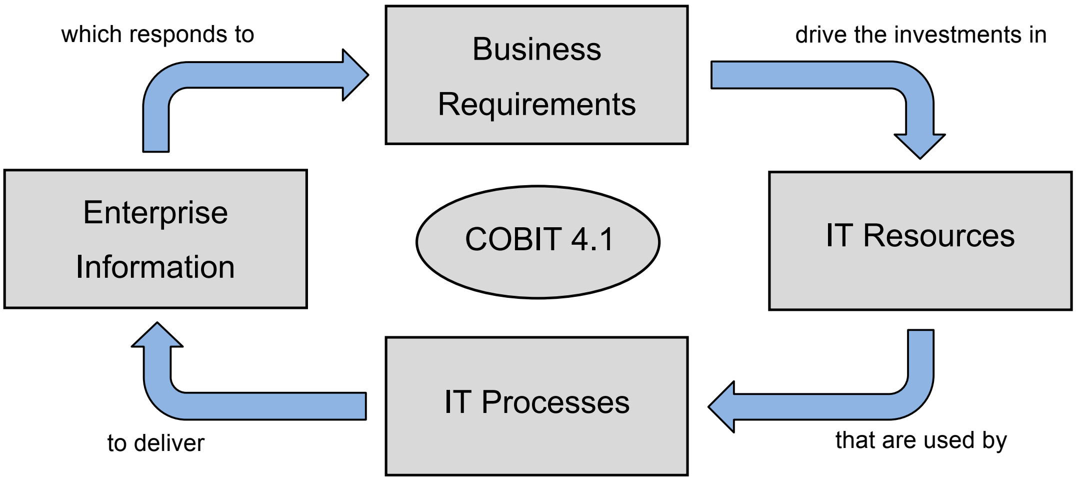

Figure 5. Business-focused: The basic COBIT 4.1 principle (ITGI 2007, 10).

The process orientation of COBIT 4.1 follows a structured and controlled model that represents all of the processes typically found in IT functions. This presents a common reference point that can be understood by both operational IT and business managers. In addition, the model also provides the capability to measure and monitor IT performance, improve communication with service providers and integrate the best management practices. By incorporating a controlled process model ownership of the process is encouraged which enables responsibilities and accountability to be more clearly defined. (Kouns and Minoli 2011, 179)

The COBIT process reference model contains 34 high-level IT processes each of which is clearly defined with information and examples to describe its inputs, outputs, key activities, responsibilities, objectives and performance measurement criteria. The processes are categorised under four interrelated domain areas of responsibility: (1) plan and organise, (2) acquire and implement, (3) deliver and support and (4) monitor and evaluate (ITGI 2007, 5). The interrelation between these four domain areas is illustrated in figure 6 on the following page and then discussed beneath this.

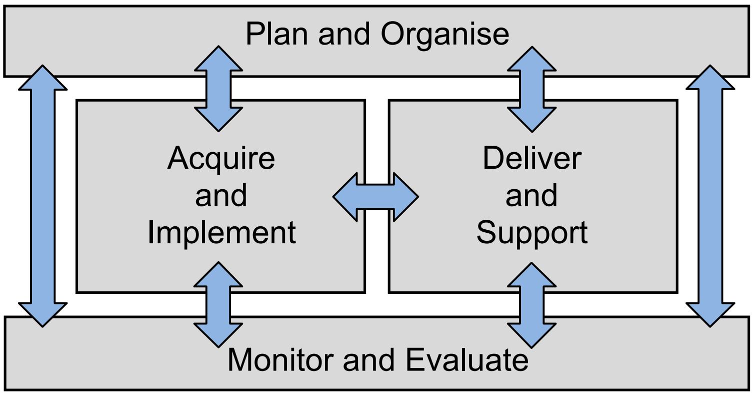

Figure 6. The four interrelated domain areas of COBIT 4.1 (ITGI 2007, 12).

- Plan and Organise (PO) – This covers the strategy, tactics, and identification of how IT resources can best contribute to achieving the goals and business objectives.

- Acquire and Implement (AI) – This concerns the identification, development or acquisition, implementation and integration of IT solutions into the current business processes.

- Deliver and Support (DS) – This focuses on the delivery aspects of the required IT services in accordance with business priorities, optimised costs, management of security and integrity, and a workforce that is able to use the IT systems productively and safely.

- Monitor and Evaluate (ME) – This involves the regular assessment of all IT services to determine their effectiveness, security, integrity, regulatory compliance, and integration to meet business goals. (Raggad 2010, 740) (ISACA 2011, 11)

The controls-based orientation of the COBIT 4.1 framework is represented by policies, procedures, practices and organisational structures that are designed to provide assurance that the business objectives can feasibly be met. This includes the prevention or detection of undesired events by appropriate corrective action. Effective controls reduce organisational risk, increase the prospect of delivering value and improving efficiency since there will be fewer errors and a more consistent management approach. (ITGI 2007, 13-14)

The framework defines 210 control objectives that are subdivided across its thirty-four high-level IT processes. Within each IT process, the linked control objectives provide action statements that outline the minimum requirements for good practice to ensure the effective management and control of the process. In addition to these action statements, each of the thirty-four IT processes has further generic requirements. When considered together, all of these elements comprise a complete view of the control-based process. However, understanding the roles and responsibilities for the control-based process requirements is key to the overall success of the IT governance framework.

The measurement-driven orientation of COBIT 4.1 builds up an objective view of an enterprise's own performance level. Both corporate and public enterprises are increasingly asked to consider how well their IT is being efficiently managed and utilised to maximum effect. Enterprises need to measure their current position, identify where improvement is required and implement a set of measurement tools to monitor this improvement. COBIT deals with all of these issues by providing the following measurement-driven tools:

- Maturity models – Developed for each of COBIT's thirty-four IT processes, the maturity models enable management to perform benchmark analyses, identify and locate issues and prioritise improvements in capability. Maturity model evaluations are made against a maturity level scale ranging from non-existent (0) to optimised (5). The scale includes zero (0) since it can be possible that no process exists at all.

- Performance goals and metrics – These are used to define and measure how well a business IT function or IT process is performing in order to meet both business expectations and IT goals. Similar goals and metrics are used for measuring internal process performance based on balanced scorecard principles.

- Activity goals and metrics – These establish what needs to happen inside a process to achieve the required effective process performance and how to accurately measure it. (ITGI 2007, 17-23)

Figure 7 provides a diagrammatic view of how the already described management; control, alignment and monitoring aspects of COBIT 4.1 are linked. COBIT connects the business requirements for information and governance to the objectives of the IT services. It enables the IT activities and the resources that support them to be properly managed and controlled based on COBIT's control objectives and are aligned and monitored using COBIT's goals and metrics.

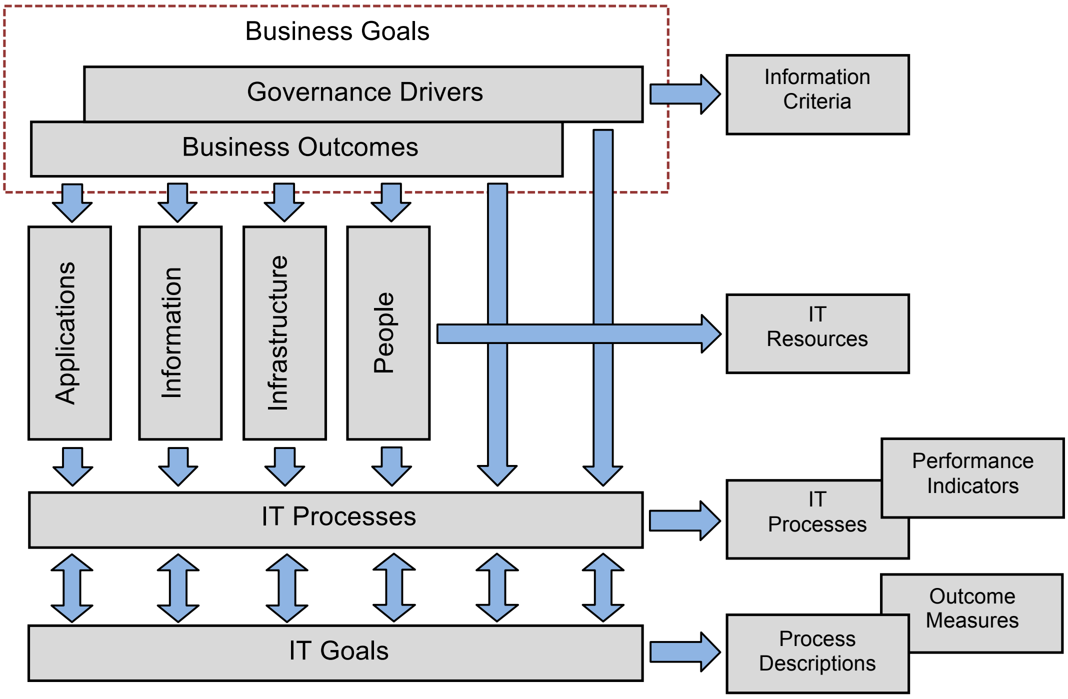

Figure 7. COBIT 4.1 framework model: Management, Control, Alignment and Monitoring (ISACA 2007, 24).

4.2.2 COBIT 5: Business Framework for IT Governance and Management

Released in 2012, COBIT 5 is the fifth and latest edition of the COBIT series to provide the next generation of guidance that assists enterprises in achieving their objectives for the governance and management of IT. The framework is based on a revised process reference model with a new governance domain and several new and modified processes that now cover enterprise activities from end-to-end, including business and IT function areas (ISACA 2013c). The generic framework is useful for organisations of all sizes and helps to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA 2012a, 13).

COBIT 5 has compiled, expanded and improved on COBIT 4.1 by consolidating, integrating and aligning with other major frameworks, standards and resources. The updated structure correlates the knowledge assets previously dispersed over ISACA's COBIT, Val IT, and Risk IT frameworks to provide a simplified and complete enterprise-wide information security assessment process (ISACA 2013c). COBIT 5 not only rationalises all of the aforementioned ISACA frameworks together but it is also aligned and harmonised with a number of other highly successful IT standards and codes of good practice adopted by the industry. The following are all covered within the scope of COBIT 5:

- COBIT 4.1 – IT governance framework and supporting toolset that assists enterprise management to relate IT control requirements, technical issues and business risks (ISACA 2013b).

- Val IT 2.0 – IT governance framework that focuses on value delivery and ensures that IT-enabled investments are managed throughout their full economic life cycle (ISACA 2009a, 1).

- Risk IT – framework for enterprises to identify, assess, govern and manage IT risk based on a set of guiding principles connecting IT with all business operations (ISACA 2009b, 2-4).

- COSO – integrated framework to enable enterprises to efficiently design, implement, evaluate and improve the effectiveness of internal control over information systems in order to meet objectives (COSO 2011, i).

- ITIL – framework of best practices for IT Service Management (ITSM) to identify, plan, deliver and support IT services and align these with the needs of the business and core business processes (ITIL 2013).

- TOGAF – de facto standard framework and supporting toolset to provide software architects with a structured approach for organising and governing their software technology design, development and maintenance (opengroup 2006).

- PMBOK – internationally recognised guidebook presenting a set of fundamental processes and guidelines needed to achieve organisational results and excellence in the practice of project management (PMI 2013).
- ISO/IEC 27000 series – a family of mutually supporting information security standards to provide best practice recommendations on security management, risks and controls within the context of an overall ISMS (IT Governance 2013).
- ISO/IEC 9000, ISO/IEC 31000, ISO/IEC 38500 – frameworks for effective quality management systems, risk management and IT governance.

In addition to the bulleted items listed above COBIT 5 also incorporates many features drawn from the Business Model for Information Security (BMIS) and the Information Technology Assurance Framework (ITAF) (Davis and Schiller 2011, 407). With all of these IT standards and good practices combined in one framework COBIT 5 provides a powerful and broad set of tools to enable organisations to execute a wide range of high-level processes across the following areas:

- Audit and assurance – to manage vulnerabilities and ensure compliance.
- Risk management – to evaluate and optimise enterprise risk.
- Information security – to oversee and manage IT security.
- Regulatory compliance – to keep pace with continually changing regulations.
- Governance of enterprise IT – to align IT goals with strategic business objectives.

COBIT 5 is based on five key principles, which enable organisations to build an effective governance and management framework that optimises information and technology investment and use for the benefit of stakeholders. These five key principles are illustrated in figure 8.

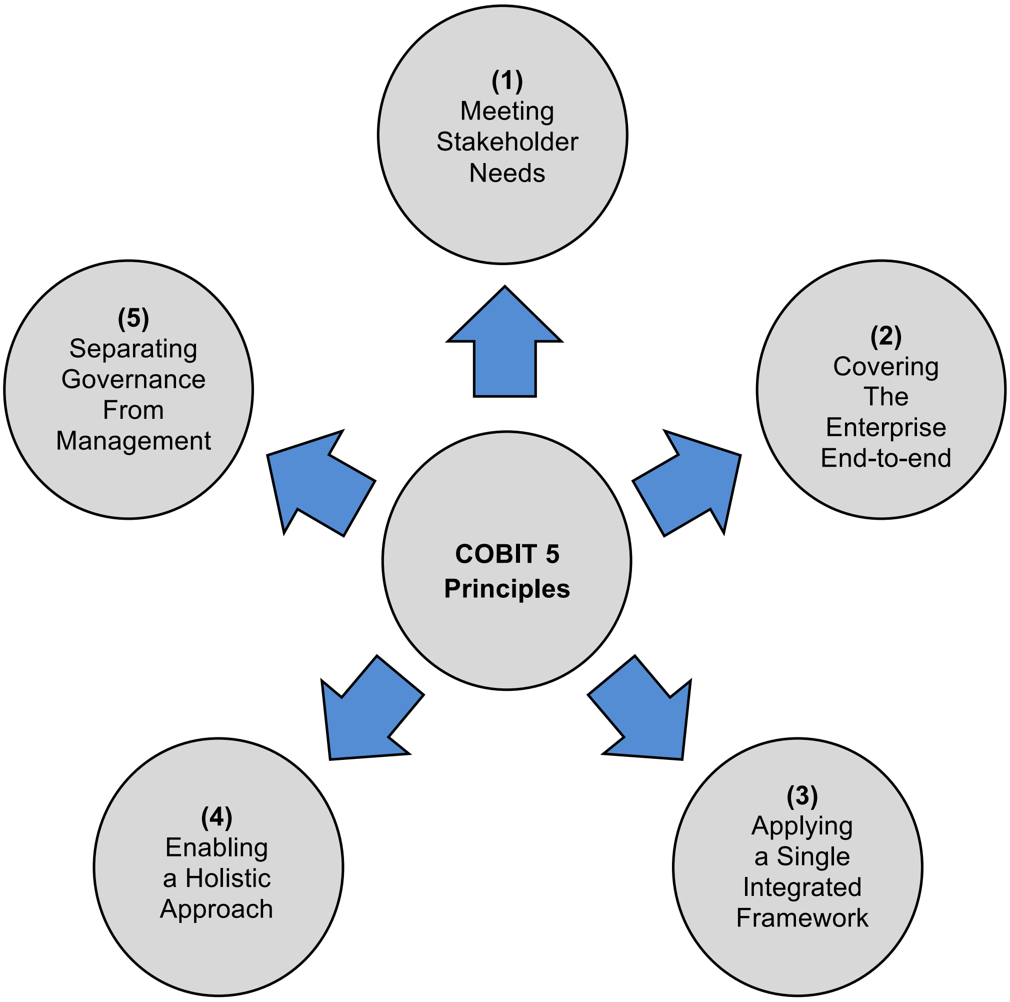
(1)
Meeting Stakeholder Needs
(2)
Covering The Enterprise End-to-end
(3)
Applying a Single Integrated Framework
(4)
Enabling a Holistic Approach
(5)
Separating Governance From Management
COBIT 5 Principles

Figure 8. COBIT 5: Key principles (ISACA 2012a, 13).

The COBIT 5 framework is not prescriptive in structure but advocates that organisations implement governance and management processes such that the key areas are covered, as shown in figure 9 on the next page.

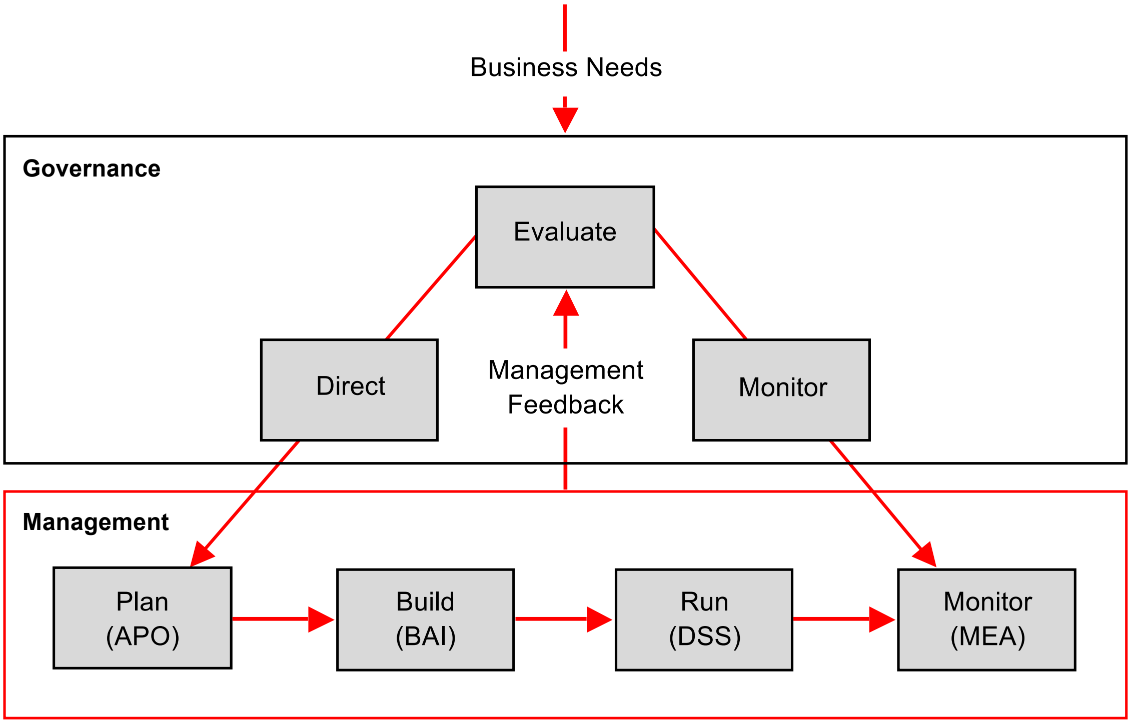

Figure 9. COBIT 5: Key areas of IT Governance and Management (ISACA 2012a, 32).

Although similar in structure to COBIT 4.1, the COBIT 5 process reference model encompasses significant improvements fully integrating with the Risk IT and Val IT process models. The COBIT 5 model represents and describes all of the processes normally found in an organisation relating to IT activities and provides a common reference point to benchmark against. The proposed process model is a complete comprehensive model but requires that each organisation must define its own processes unique to its own operational environment. (ISACA 2012a, 32-33)

Whilst the COBIT 4 model categorises thirty-four IT process tasks under four interrelated domain areas the COBIT 5 model first establishes two core disciplines ‘governance’ and ‘management’. These two disciplines contain a total of five domain areas each represented by three-letter abbreviations. There are a total of thirty-seven process tasks distributed between the five domain areas.

Table 4 gives a clearer perspective of how the disciplines, domains and process tasks are related.

Table 4. COBIT 5: Disciplines, domains and process tasks.

Disciplines	Domain area / number of associated process tasks
Governance of Enterprise IT	Evaluate, Direct and Monitor (EDM) – 5 process tasks
Management of Enterprise IT	Align, Plan and Organise (APO) – 13 process tasks
	Build, Acquire and Implement (BAI) – 10 process tasks
	Deliver, Service and Support (DSS) – 6 process tasks
	Monitor, Evaluate and Assess (MEA) – 3 process tasks

Within the process tasks outlined above COBIT 5 is supported by an implementation toolkit and other detailed stages. The framework is not intended to be a complete solution but rather a guide to avoid commonly encountered problems, adoption of good practices and to assist in the creation of successful outcomes. Optimal value outcomes are realised when the framework is properly governed and adequately managed.

4.3 OCTAVE

Originally developed by the Software Engineering Institute (SEI), the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach was created to address the security compliance challenges that were faced by the U.S. Department of Defence (DoD). Since its initial public release in 1999 there have been a number of version updates that have developed and improved the underlying framework, methods and criteria to suit different sized organisations. (SEI 2007, 1)

OCTAVE contains a framework of tools, techniques and methods that have been specifically designed for strategic risk-based information security assessments and planning (Panda 2009, 1). The OCTAVE approach is not a product, but rather a process-driven methodology to identify, prioritise and manage information security risks.

The principal role of OCTAVE is to enable organisations to understand, assess and address their information security risks from their own perspective. By following the OCTAVE approach organisations can utilise the framework to make effective decisions regarding protection of information based on risks to the confidentiality, integrity and availability of critical information assets. OCTAVE is intended to help an organisation to:

- Develop qualitative risk evaluation criteria that describe the organisation's operational risk tolerances.
- Identify assets that are of most importance to the organisation.
- Identify threats and vulnerabilities to the identified assets.
- Determine and evaluate the consequences to the organisation if the threats were to be realised.
- Initiate corrective actions to mitigate risks and create a practice-based protection strategy. (SEI 2007, 1)

There are three distinctive methodologies within the family of OCTAVE information security assessments available for public use:

- The original OCTAVE method – for larger organisations.
- The OCTAVE-S method – for smaller organisations.
- The OCTAVE-Allegro method – a streamlined approach for small to large organisations.

The OCTAVE-S and OCTAVE Allegro methods are based on and developed from original OCTAVE criteria providing the foundation of the whole concept.

These criteria establish the fundamental principles of risk management used within all OCTAVE methodologies. Published in 2007, OCTAVE Allegro is the most recently developed method whilst the two older methods, OCTAVE and OCTAVE-S are still available and widely used. Sections 4.3.1 to 4.3.3 below briefly expand on the three active OCTAVE methodologies.

4.3.1 OCTAVE method

Launched in 1999, the OCTAVE method was the original release of the OCTAVE methodologies developed for larger organisations with 300 or more employees (CERT 2013a). Although the method focuses on the requirements of larger organisations it is not the only consideration of the methodology. More specifically it was designed for organisations that:

- Have a multi-layered hierarchical structure
- Are responsible for maintaining their own computing infrastructure
- Are familiar with and capable of operating vulnerability evaluation tools
- Are familiar with and are capable of interpreting the results from vulnerability evaluations (SEI 2007, 2)

The OCTAVE Method uses a three-phased approach to examine organisational and technological issues in order to assemble a comprehensive picture of the organisation's information security needs (Alberts and Dorofee 2004, 44). The purpose of each phase is as follows:

- Phase 1: Perform an organisational evaluation to determine the critical assets and the existing methods protecting them. Identify the security requirements for each critical asset and build asset-based threat profiles.
- Phase 2: Perform a technological evaluation to identify the infrastructure vulnerabilities that are related to and expose each critical asset.

- Phase 3: Perform a risk analysis to develop a security protection strategy and mitigation plans to address the identified risks. (Panda 2009, 4)

Figure 10 illustrates how each phase of the OCTAVE method is broken down into eight sub-processes: four in phase 1, two in phase 2, and two in phase 3. These processes utilise knowledge from the various levels in the structure of the organisation to complete a systematic information security risk evaluation.

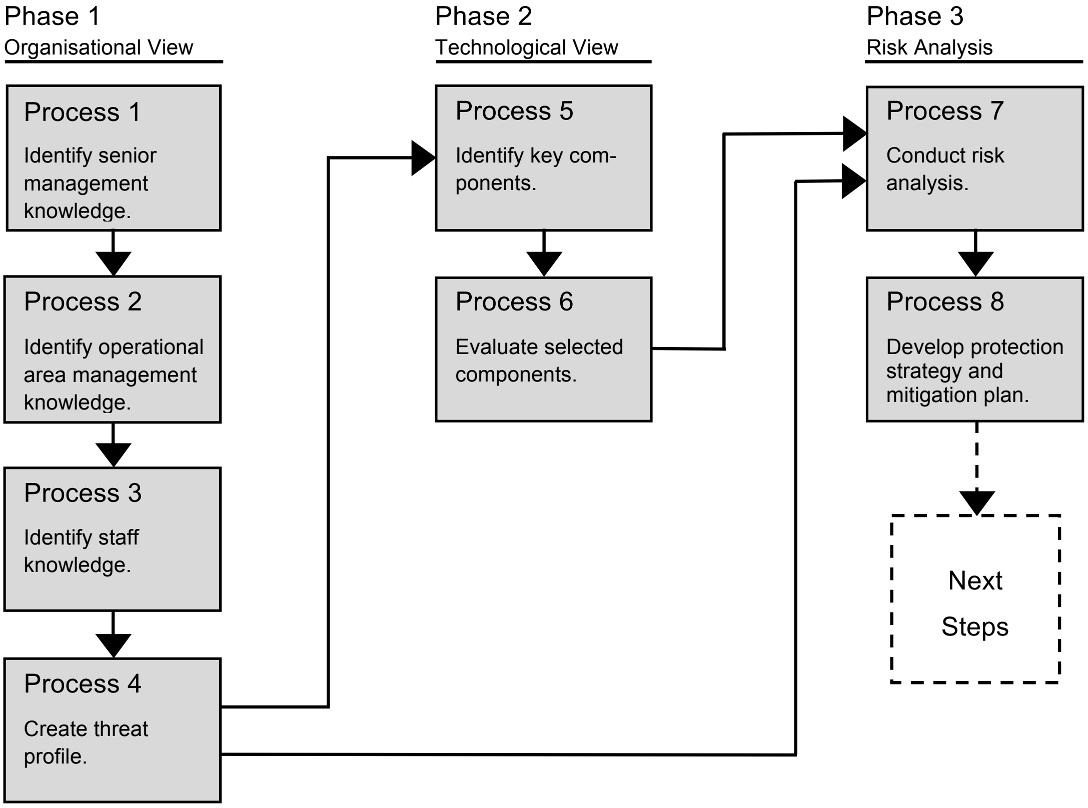
Phase 1
Organisational View
Phase 2
Technological View
Phase 3
Risk Analysis
Process 1
Identify senior management knowledge.
Process 2
Identify operational area management knowledge.
Process 3
Identify staff knowledge.
Process 4
Create threat profile.
Process 5
Identify key com-ponents.
Process 6
Evaluate selected components.
Process 7
Conduct risk analysis.
Process 8
Develop protection strategy and mitigation plan.
Next
Steps

Figure 10. The OCTAVE method three-phased approach (Panda 2009, 3).

The three phases and associated sub-processes are supported by a series of data gathering workshops that involve the completion of surveys and risk measurement worksheets. These activities are essential to the whole risk assessment in order to elicit and capture information during focused discussions and problem-solving sessions (CERT 2013a).

4.3.2 OCTAVE-S method

The OCTAVE-S method is a variation of the original OCTAVE approach that was developed to meet the needs of smaller sized organisations of about 100 or less employees (CERT 2013b). OCTAVE-S was adapted to use a more streamlined process that is customised to the more limited means and particular constraints typically found in smaller organisations. This method focuses on organisations that:

- Have a flat or simple hierarchical structure with people from different organisational levels being accustomed to working with each other
- Outsource most or all of their IT functions
- Have a simple IT infrastructure that is well understood internally
- Have limited familiarity with vulnerability evaluation tools
- Have limited knowledge to sufficiently interpret the results from vulnerability evaluations or obtain external professional assistance (Alberts et al. 2004, 8).

Although the appearance and structure of OCTAVE-S differs from the OCTAVE method, the technique meets the same underlying criteria and achieves similar results in providing a protection strategy suited to the organisation (Alberts et al. 2004, 3). OCTAVE-S is similarly based on the three-phased approach described in the OCTAVE method. However, the number and sequencing of the sub-processes have been condensed into just four (Figure 11):

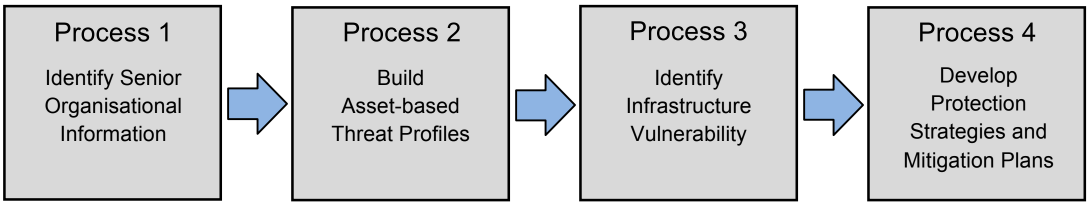
Process 1
Identify Senior Organisational Information
Process 2
Build Asset-based Threat Profiles
Process 3
Identify Infrastructure Vulnerability
Process 4
Develop Protection Strategies and Mitigation Plans

Figure 11. The OCTAVE-S method processes (Panda 2009, 4).

In order to perform the OCTAVE-S risk assessment a small interdisciplinary analysis team of three to five people is required. The team must have a broad understanding of the organisation's business and security processes sufficient to execute all of the OCTAVE-S activities. The extent of the analysis team's knowledge means that, unlike the OCTAVE method, OCTAVE-S discards the data gathering workshops held in the initial stages of the evaluation process in order to obtain information about crucial assets, security requirements, threats, and existing security practices (CERT 2013b).

OCTAVE-S conducts a limited exploration of an organisation's computing infrastructure since small sized companies predominantly outsource their IT services and functions (CERT 2013b). In addition, small companies typically do not have the developed organisational capabilities to run or interpret the results of vulnerability evaluation tools. Instead of using vulnerability data to assess current security practices OCTAVE-S examines the existing processes employed to securely configure and maintain an organisation's IT infrastructure (Alberts et al. 2004, 5).

4.3.3 OCTAVE Allegro method

Published in 2007, the OCTAVE Allegro method is the SEI's third and latest addition to their portfolio of risk assessments available for public use. Similar to the OCTAVE and OCTAVE-S methods, OCTAVE Allegro has been designed to perform a broad assessment of an organisation's operational risk environment, but offers an alternative approach. The risk assessment is refined and improved to produce more robust results in a more efficient and effective manner and requires less resources to achieve the result (SEI 2007, 4).

One of the key drivers that led the SEI to formulate the OCTAVE Allegro methodology was the need to refine the definition of the assessment scope and streamline the data collection and threat identification processes (SEI 2007, 4). Unlike previous OCTAVE versions, Allegro focuses primarily on information assets and introduces the 'container' concept. Containers are used to describe the places where information assets are stored, transported, and processed, and how each of these affects exposure to threats, vulnerabilities and disruptions (SEI 2007, 18).

OCTAVE Allegro streamlines the risk assessment process by eliminating and/or simplifying many of the existing processes of the two earlier methodologies. The less involved approach is suitable for use by individuals who want to perform a more cost effective risk assessment without the need for engaging extensive organisational involvement, expertise or input. Similar to previous iterations the risk assessment can be performed in a 'workshop-style' collaborative setting supported with clear guidance, structured worksheet templates, and questionnaires. (SEI 2007, 4)

The OCTAVE Allegro method comprises eight 'process steps' organised into four 'phases' (areas) of activity. The four phases are described in more detail below whilst the relationship between these and the eight process steps are illustrated in figure 12:

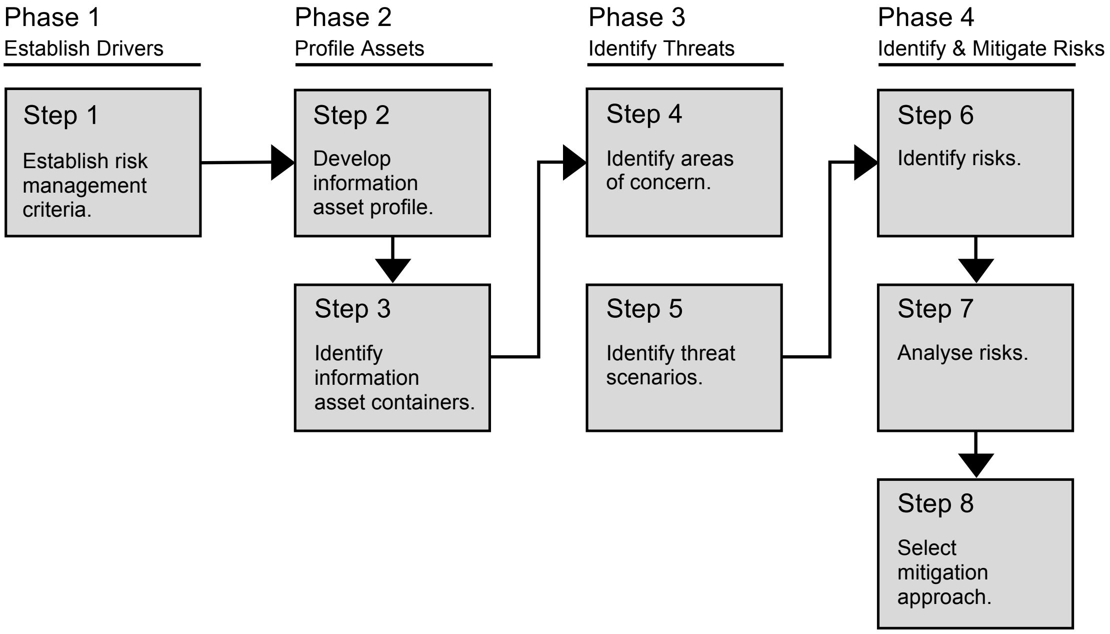
Phase 1
Establish Drivers
Phase 2
Profile Assets
Phase 3
Identify Threats
Phase 4
Identify & Mitigate Risks
Step 1
Establish risk management criteria.
Step 2
Develop information asset profile.
Step 3
Identify information asset containers.
Step 4
Identify areas of concern.
Step 5
Identify threat scenarios.
Step 6
Identify risks.
Step 7
Analyse risks.
Step 8
Select mitigation approach.

Figure 12. The OCTAVE Allegro roadmap (Panda 2009, 5).

- Phase 1: Establish drivers – Participants develop risk measurement criteria consistent with organisational drivers. I.e., the organisation's mission statement, goal objectives and critical success factors.
- Phase 2: Profile assets – Participants create a profile of each critical information asset. The process establishes clear boundaries for the asset, identifies its security requirements, and identifies all the locations where the asset is stored, transported, or processed.
- Phase 3: Identify threats – Participants identify threats to each information asset in the context of the locations where the asset is stored, transported, or processed.
- Phase 4: Identify and mitigate risks – Participants identify and analyse risks to information assets and the development of mitigating actions. (Shostack 2014, 399) (Panda 2009, 4-5)

4.4 NIST Special Publications 800 series (Computer Security)

Established in the late 1980's, the National Institute of Standards and Technology (NIST) is the U.S. federal technology agency that worked with industry to develop, apply and maintain technology, measurements, and standards. NIST organises its core activities across six laboratory units with their Information Technology Laboratory (ITL) managing the Computer Security Division (CSD). ITL are responsible for the development of NISTs special series of information security publications with the CSD providing tests, metrics, approval programs and standards to measure, validate and promote the security in information systems and services. (NIST 2013a)

NISTs expanding '800 series' of Special Publications (SP) have been specifically developed to outline the minimum information security requirements to improve the efficiency and operation of federal information systems and offer guidance against threats to the confidentiality, integrity, and availability of the information and supporting services. This series of publications have evolved from ITLs extensive on-going proactive research in creating workable and cost-effective methods to optimise the security of IT systems and networks.

The concepts and principles contained in the SP 800 series are intended for federal agencies but are also suitable for use by small, medium or large public and private sector organisations (Landoll 2011, 83). NISTs SPs complement other international standards and guidelines used in the protection of information security systems. NIST have established and mapped specific risk assessment processes, approaches and guidelines that are similar to those described in the ISO/IEC standards (NIST 2011, VII). These NIST mappings can assist organisations by providing evidence to efficiently ascertain if existing ISO/IEC security controls are implemented correctly, operating as intended and satisfactorily meeting security requirements (Chabrow 2014).

4.4.1 NIST Special Publication 800-30 – Conducting Risk Assessments

NIST Special Publication 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, provides comprehensive risk management guidance on the practice of conducting information security risk assessments within organisations. The publication describes risk assessments as a tool to “identify, prioritise, and estimate risk to organisational operations (including mission, functions, image, and reputation), organisational assets, individuals, other organisations, and the nation(s), resulting from the operation and use of information systems” (NIST 2011, 1).

Risk assessment is an intrinsic component of a holistic, organisation-wide risk management process. SP 800-30 focuses exclusively on the risk assessment component of risk management, which is one of four fundamental processes. This includes: (i) establishing the context for risk management activities that need to be executed – i.e. risk framing; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk (NIST 2011, 4-5).

Figure 13 illustrates the steps in the risk management process including the risk assessment step. The information and communications flows are necessary to make the process work effectively.

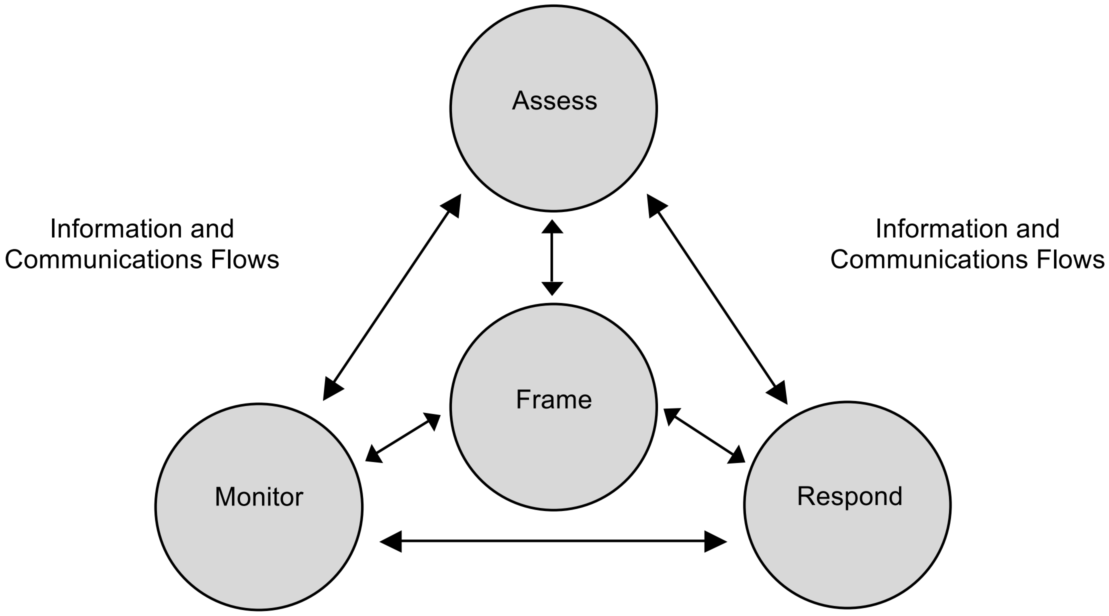
Assess
Information and Communications Flows
Information and Communications Flows
Frame
Monitor
Respond

Figure 13. The four steps in the risk management process including the risk assessment step (NIST 2011, 4).

SP 800-30 provides practitioners with a feasible step-by-step process on the activities necessary to prepare for risk assessments, the activities necessary to conduct effective risk assessments and the activities necessary to ensure that risk assessments remain current over time (NIST 2011, 23). Each of the risk assessment process steps comprise a set of tasks that organisations must execute in order to successfully complete each process step. Figure 14 on the next page provides a pictorial overview of the basic steps required in the risk assessment process and the tasks associated with the steps.

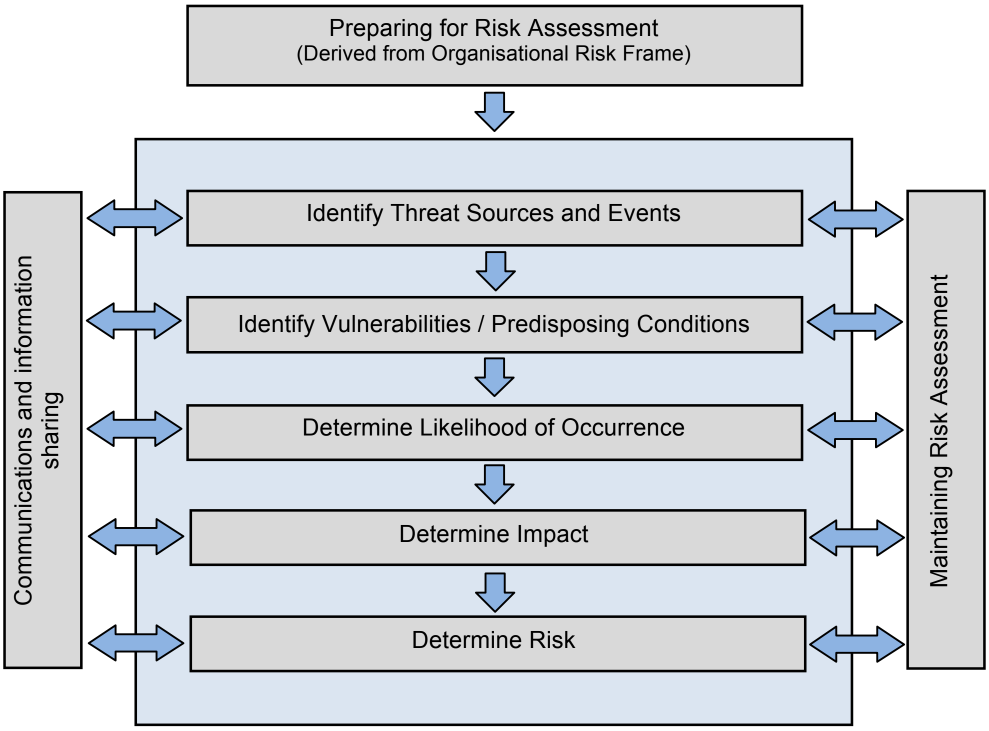
Preparing for Risk Assessment
(Derived from Organisational Risk Frame)
Identify Threat Sources and Events
Identify Vulnerabilities / Predisposing Conditions
Determine Likelihood of Occurrence
Determine Impact
Determine Risk
Communications and information sharing
Maintaining Risk Assessment

Figure 14. Risk assessment process (NIST 2011, 23).

In addition to providing a comprehensive process for assessing information security risk the NIST publication describes how to apply the risk assessment process across all three tiers in the risk management hierarchy. Tier 1 (the organisation level), Tier 2 (the mission and business process level) and Tier 3 (the information system level) (NIST 2011, 1). More traditional risk assessment frameworks generally focus on Tier 3 (tactical level) whereas SP 800-30 broadens the scope by taking into account other significant risk factors usually assessed at the Tier 1 or Tier 2 strategic levels of the risk management hierarchy (NIST 2011, 17).

To facilitate ease of use for individuals or groups conducting risk assessments this publication supports each stage of the assessment process with supplementary guidance and information. Templates, tables and assessment scales for common risk factors are cross-referenced to more detailed information in the supporting appendices to provide maximum flexibility in designing risk assessments. These are based on the purpose, scope, assumptions and constraints established by the federal agency or organisations (NIST 2011, 23).

The risk assessment approach described in SP 800-30 is supported by a series of related security standards and guidelines necessary for managing the information security risk process (NIST 2011, 3). Table 5 lists the special publications that were developed to produce a unified information security framework suitable for federal agencies as well as public and private organisations:

Table 5. NIST Special Publications security related standards (NIST 2011, 3).

Published Standards	**Description of Standard**
NIST SP 800-39	Managing Information Security Risk: Organisation, Mission, and Information System View
NIST SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organisations
NIST SP 800-53A	Guide for Assessing Security Controls in Federal Information Systems & Organisations: Building Effective Security Assessment Plans

Special Publication 800-53 in particular supports the core risk assessment processes by assisting with selection of baseline security controls or control enhancements. These controls are used to generally improve the existing security of an organisation's information systems and to mitigate any risks identified in the SP 800-30 risk assessment. The objective is to adequately address and meet an organisation's security risk management needs.

4.4.2 NIST Special Publication 800-53 – Security and Privacy Controls

Since its inception in 2005, NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organisations* has provided federal agencies and organisations with a comprehensive catalogue of baseline security and privacy controls necessary to support and strengthen their information systems and the environments in which those systems operate. The publication contains clear guidelines for selecting and specifying the appropriate controls to prevent breaches of IT security and potentially serious implications for the operations and assets of organisations as well as the welfare of individuals, other organisations and nation(s). The guidelines are applicable to all components of an information system that process, store or transmit data (NIST 2013b, 2).

The baseline security controls and control enhancements in SP 800-53 address areas such as: mobile and cloud computing, applications security, trustworthiness, assurance and resilience of information systems, insider threat, supply chain security and advanced persistent threat (NIST 2013b, XV). The extent of these safeguards and countermeasures provide federal agencies and organisations with the means to resist a range of IT security threats. For example, hostile cyber attacks, natural disasters, accidents, structural failures, and human errors, both intentional and unintentional (NIST 2013b, 25).

Although these baseline controls are well positioned to support most information security and privacy organisational processes some may require an element of customisation. SP 800-53 provides organisations with the flexibility to develop and tailor their particular applicable baseline security controls using a concept of overlays. These overlays provide a structured approach to help those organisations that need to tailor their security control baselines and develop specialised security plans. These can be aligned and applied to specific missions and business functions with specific environments of operation and particular technologies (NIST 2013b, XV). The resulting set of customised security controls establishes a bespoke level of security suited to the organisation.

4.5 ISO/IEC 27000 series – ISMS ‘family’ of international standards

The ISO/IEC 27000-series of international standards are jointly developed, promoted and maintained by ISO and IEC for worldwide standardisation. This is also known as the ‘ISMS family of standards’ or abbreviated to ‘ISO27K’ and is specifically dedicated to international management systems standards for information security. These standards are deliberately wide in scope so that they are applicable to organisations of all types and sizes and provide world-renowned best practice with recommendations on information security management, risk assessments and controls within the context of the overall ISMS. (ISO 2014a)

The ISO27K series allows organisations to develop and implement a framework for managing the security of their information assets. These assets may include financial information, intellectual property and employee details or information entrusted to them by customers or third parties (ISO 2014a). The ISO27K series can also be used as a tool to assist organisations with preparing and performing an ISRA of their own ISMS.

The ISO27K series is formed from several major ISO/IEC operational international standards under the general title *‘Information Technology – Security Techniques’*. The common purpose of the series is to address the following four core areas that:

a) Define requirements for an ISMS and for those certifying such systems;

b) Provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain and improve an ISMS;

c) Address sector-specific guidelines for an ISMS; and

d) Address conformity assessment for an ISMS. (ISO 2014a)

There are currently fifteen different international standards that form the complete ISO27K series which, when used together, specify the complete implementation of an ISMS. Table 6 on the following page lists all fifteen standards in numerical order. However, it is worth noting that at the time of writing this research report not all standards were in circulation since some were still under final development.

Table 6. The ISO27K series of International Standards (ISO 2014a).

Standard Code	**Brief description of Standard**
ISO/IEC 27000	ISMS – Overview & vocabulary
ISO/IEC 27001	ISMS – Requirements
ISO/IEC 27002	Code of practice for information security controls
ISO/IEC 27003	ISMS – Implementation guidance
ISO/IEC 27004	Information security management – Measurement
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC 27008	Guidelines for auditors on information security controls
ISO/IEC 27010	Information security management for inter-sector and inter-organisational communications
ISO/IEC 27011	Information security management guidelines for telecommunications organisations
ISO/IEC 27013	Guidance on the integrated implementation of ISO/IEC 27001
ISO/IEC 27014	Governance and information security
ISO/IEC 27015	Information security management guidelines for financial services
ISO/IEC 27016	Information security management – Organisational economics

From the complete list of standards outlined in table 6 the focus of ISO/IEC 27000 is to provide a general overview of the series together with a glossary of information security terms and of the standards concerned. The two core standards are (1) ISO/IEC 27001, which specifies the requirements for an ISMS and (2) ISO/IEC 27002, which establishes guidelines and principles to plan the implementation of the ISMS.

ISO/IEC standards 27003 to 27008 cover areas of the ISMS such as its final design, guidance for management approval, security metrics (measurement) and guidance for accredited certification bodies (auditors). It also describes the method of flow of the technical auditing process. The remaining standards in the series focus on the guidelines for sector specific implementation of information security management systems.

Since the ISO/IEC 27001 and 27002 standards form the core of the ISO27K series and the ISO/IEC 27005 standard focuses on the practical phases of information security implementation these are relevant to this research project. Each of these is discussed in further detail in the following sub-sections.

4.5.1 ISO/IEC 27001 – ISMS requirements

First published in 2005, the ISO/IEC 27001 International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented information security management system in the context of the organisation’s overall business risks. In addition, the scope of the standard also includes over 130 generic controls for the assessment and treatment of information security risks tailored to the needs of an organisation. (ISO 2013d)

The controls cover a range of detailed areas where information security could be compromised. These include: security policy, staffing issues, equipment issues, access controls to both computing equipment and data, compliance with legal requirements and standards, acquisition, development and maintenance of the system and management of business continuity. (Higgins 2013)

ISO/IEC 27001 adopts a process approach for establishing, implementing, monitoring, and maintaining an information security management system. These processes are achieved through the use of a "Plan-Do-Check-Act" (PDCA) model. The PDCA model encourages its users to follow a four-step process:

a) PLAN – ‘Establish’ the ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organisation’s policies and objectives.

b) DO – ‘Implement’ and operate the ISMS policy, controls, processes and procedures;

c) CHECK – ‘Monitor’ and assess the effectiveness and process performance against the ISMS policy, objectives and practical experience.

d) ACT – ‘Maintain’ and continually improve the ISMS by taking corrective and preventative actions, based on the results of the internal ISMS audit. (ISO 2013d)

The design and implementation of an ISMS is influenced by, and scaled in accordance with an organisation’s needs, objectives, security requirements, the processes employed and the size and structure of the organisation. Based on these influences, the standard is used by internal and external parties to assess the organisation’s ability to meet predefined information security requirements. In order to support consistent and integrated implementation and operation with other related international management standards ISO/IEC 27001 has been aligned with ISO 9001 and ISO 14001. (ISO 2013d)

4.5.2 ISO/IEC 27002 – Code of practice for information security controls

The ISO/IEC 27002 International Standard is designed for organisations to use as a reference for selecting information security controls within the process of implementing an ISMS based on ISO/IEC 27001. It is also used as a guidance document for organisations implementing commonly accepted information security controls including those essential for legislative compliance as well as those required for best practice (ISO 2013e) (Higgins 2013).

The latest revision of ISO/IEC 27002 was published in 2013 and contains 114 controls as opposed to the 133 documented in the previous 2005 version. For clarity these controls are presented in fourteen sections, rather than the original eleven. These controls and control objectives are intended to address specific requirements identified via a formal risk assessment. In addition the standard is intended to provide a guide for the development of organisational security standards and effective security management practices and help build confidence in inter-organisational activities (ISO 2013e).

ISO/IEC 27002 is regarded as a starting point for developing specific information security guidelines for an organisation. Not all of the controls and guidance in this standard may be applicable and so additional controls and guidelines may need to be carefully selected and adopted. ISO/IEC 27002 is frequently cross-referenced within ISO/IEC 27001 as this is indispensible for its application. Therefore, both standards are complementary and intended for use together.

4.5.3 ISO/IEC 27005 – Information security risk management

ISO/IEC 27007 provides guidelines for information security risk management (ISRM) in an organisation. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach (ISO 2011). The standard does not provide or recommend a specific methodology for an ISRM since it is the responsibility of each organisation to define their own individual approach to risk management. For example, this might be dependent on the scope of the ISMS, the context of risk management or the industry sector.

ISO/IEC 27005 is applicable to any type and size of organisation which intends to manage risks that could compromise its information security. The standard is relevant to “managers and staff concerned with information security risk management within an organisation and where appropriate external parties supporting such activities” (ISO 2011).

In order to ensure a complete understanding of the ISO/IEC 27005 standard it is essential that knowledge of the core concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is first attained.

4.6 Selecting a suitable ISRA framework for this research project

At the start of this report it was clarified that the scope of the project had been reduced over the original project brief to rationalise resources and costs. These changes directly influenced the selection of the evaluated security risk assessment methods and standards. It was important to select an information security risk assessment methodology that was relatively easy and quick to use, required minimum training and knowledge and involved the least amount of human resources. It would also need to produce reliable and consistent results, encourage development of the company’s ISMS and support both the current and future business environments.

4.6.1 The chosen framework – OCTAVE Allegro method

From the four best-practice options appraised in this chapter the OCTAVE series of security risk assessment frameworks was shortlisted for its overall suitability to scale and type of the company being appraised in this research project. From the three different methods in the OCTAVE series the OCTAVE Allegro methodology was chosen to perform the company ISRA and to best assist with the completion of the research project objectives.

OCTAVE Allegro simplifies many of the existing processes from the earlier OCTAVE and OCTAVE-S methodologies. The Allegro method has been designed to perform a broad assessment of an organisation's operational risk environment requiring less extensive examination of the information infrastructure yet will still produce reliable results in a more efficient and effective manner (SEI 2007, 4). Selecting OCTAVE Allegro meets the key objective in obtaining the outputs required by the company with limited investment in time and resources. This particular method streamlines and optimises the process of assessing information security risks (SEI 2007, IX). These factors are also key to the success of the research project with its restricted time frame for completion using the least possible investment resources.

SEI (2007, 3) states that "OCTAVE Allegro is specifically designed for organisations of about 100 people or less" which is appropriate for the company's thirty-five strong workforce. Allegro is suitable for use by individuals wishing to perform a security risk assessment without extensive organisational involvement, expertise, or input (SEI 2007, 4). Allegro's capabilities and methods also meet the requirements of this research project since the core areas of research were conducted by an individual employee of the company (the researcher) working with very limited support from a small internal group providing assistance with some of the preparatory phases only. It should also be noted that all personnel involved in the risk assessment process had relatively little expertise in the field of information security.

With no rigorously documented company IT procedures in place, no industry standard ISRA framework in place, limited resources and lack of internal experience in performing an ISRA adopting OCTAVE Allegro's lean assessment methodology would be beneficial to the company. The method provides:

- Ease of use – The size and complexity of processes that must be understood and applied to a risk assessment. The amount of data that must be collected and managed throughout the process is to be minimised. Guidance, worksheets and examples provide a structured path when performing the risk assessment.

- Refined scope – Accurately defining the scope of a risk assessment improves the results and requires less overall effort. OCTAVE Allegro focuses exclusively on the most important information assets to enable the organisation to define a manageable scope from the outset.

- Reduced knowledge and training – By minimising the amount of risk management and IT knowledge required to perform an effective Allegro risk assessment the number of internal personnel needed to participate in the process is reduced. Consequently the cost associated with the training and mentoring is also reduced.

- Reduced resource commitments – To optimise the use of resources the Allegro assessment reduces the required process activities to only those that are necessary. This ensures that those conducted are more meaningful, require less data manipulation and are streamlined for identifying and mitigating risks. Documentation and the organisation of data are also improved through the efficient and effective design of Allegro worksheets that reduce the amount of data carried forward.

- Consistent and comparable results – The Allegro methodology supports and enables a larger enterprise risk management effort by allowing the organisation to achieve not only consistent results over time but results that are generically comparable across all operating units and lines of business.

- Facilitates a risk-aware culture – This is promoted by Allegro's accessible risk assessment methodology with low barriers of use and no specialised training being needed. It encourages the production of meaningful results that can be understood throughout the organisation helping to cultivate risk management appreciation. This assists employees to better perform their job responsibilities in safeguarding the company security interests.

- Supports compliance activities – The Allegro risk assessment methodology supports other organisations allied to the company with their information security risk management activities enabling them to act quickly and achieve compliance with various laws and regulations efficiently. (SEI 2007, 8-10)

4.7 Reasons for discarding other ISRA options

The COBIT security risk assessment method, NIST SP 800 series of computer security guidance publications and the ISO/IEC 27000 family of international information security standards were not adopted for the purposes of completing this research project for the following reasons.

The process orientation of COBIT involves a number of systematic procedures that require planning, implementation, execution and monitoring activities. However, the benefits of using COBIT rely heavily upon these activities, but due to the reduced project scope could not be carried out. COBIT does not always provide detailed explanations of specific procedures since the control objectives are more aligned with achieving outcomes (Mataracioglu and Ozkan 2011, 3).

The NIST SP 800-30 guide for conducting risk assessments explores more tactical and organisational issues. Is very detailed and rigid in structure and is more suited to third party execution by a professional body. This is quite the opposite of the OCTAVE method where there is much more flexibility to operate a self-directed internal team that makes use of existing knowledge within the organisation. NIST also tends to focus heavily on promoting information gathering such as questionnaires, interviews and document reviews rather than a more practical workshop-based approach involving key personnel to gather information and make decisions. (Tewari 2013)

The ISO/IEC 27001 standard requires several complex and resource intensive phases to define the scope of an organisation’s ISMS. With this level of complexity demanded by ISO/IEC 27001 and supplementary standards from the ISO27k family, seeking professional guidance and support from external consultants would need to be sought (Raywood 2010). A considerable amount of time and resources would be needed to produce the relevant company specific information, security policies and procedures under the supervision of a consultant, which would be a considerable expense for a smaller sized company. These overheads and the preparatory work required are not suited to this research project.

5 PREPARATIONS AND PROCESSES FOR THE ISRA

5.1 Preparation for the OCTAVE Allegro risk assessment

Prior to the commencement of the OCTAVE Allegro risk assessment two supporting documents from the SEI were thoroughly reviewed by the company's senior management, IT personnel and the researcher. The first document named *'Introducing OCTAVE Allegro'* is a technical report highlighting the design considerations, requirements and preparatory work needed for an OCTAVE Allegro risk assessment. The second document named the *'OCTAVE Allegro Guidebook'* provides guidance, worksheets and examples used to support the completion of the practical steps of the risk assessment.

For the purposes of this research project the information and guidance from the two SEI documents provided a reference point throughout the OCTAVE Allegro risk assessment process. The documents also outlined the necessity to complete a certain level of preparatory work before beginning the company specific risk assessment. Some of the preparatory activities included obtaining management support, allocating appropriate organisational resources to the processes and scoping the numerous risk assessment steps (SEI 2007, 23). The activities were addressed during several internal initiation meetings involving senior management, IT personnel and the researcher. The topics and outcomes from the meetings are discussed below.

5.1.1 Organisational resource commitment

Obtaining full sponsorship from the company's senior management was a critical factor in successfully performing the OCTAVE Allegro risk assessment. From the initial preparatory stages of this research project it was ensured that senior management were fully committed and available when necessary to provide active support to the risk assessment process. Although the OCTAVE Allegro methodology promotes a streamlined assessment that can minimise the participation of busy senior management, their input was still essential in the development of the organisation-wide risk measurement criteria.

During the inaugural meetings with senior management discussions were focused on the rationalisation of human resources that were to be made available for the completion of this research project. In an effort to free up specific resources it was agreed that sufficient and suitably skilled company personnel would be allocated to the different in-house assessment processes. This support enabled the members of the assessment team to devote the necessary time required to perform a more complete and thorough process. This promoted a greater chance of developing useful results towards improving the company's overall level of information systems security.

5.1.2 Allocation of organisational resources

Two important aspects of the OCTAVE Allegro method are the size and composition of the assessment team. Guidance from the supporting documentation specifically states that the level of a company's expertise and the perceived involvement of different departments in the assessment process determine the size and capability of the assessment team. This can be from as little as one person to as many as seven. (SEI 2007, 23)

Taking the SEI's guidance into consideration those company personnel having the relevant skillsets to assist with the risk assessment process were shortlisted. An importance was placed on candidates who had the knowledge and experience working within operational areas of the business where the risk assessment would be focused. Based on the diversity and capacity of the company's resource pool it was concluded that four personnel from across four different departments were to be selected to form the OCTAVE Allegro risk assessment team. Information about the chosen candidates and the departments they work in are briefly outlined in table 7 on the next page.

Table 7. A list of the company personnel involved in the OCTAVE Allegro risk assessment process including their working roles.

Position / Department	Role of the Department
Technical Director (Project Management)	Responsible for incoming and outgoing quotations involving the handling of sensitive project related data entered into the company's internal database system.
Administration Manager (Administration Department)	Responsible for sending and receiving invoices and paying employees' salaries, which includes access to employee and project related sensitive electronic data stored on the company's internal server.
Production Manager (Production Department)	Responsible for managing the manufacturing phases of all active projects, which includes the handling of sensitive data printed from electronic files stored on the company's internal server.
IT Administrator and personnel (IT Department)	Responsible for installing and maintaining all IT related systems and ensuring the security and integrity of all electronic data stored on the company's internal server.

Access to the company IT department and knowledge from the IT personnel and the researcher were priority resources during the assessment steps. These steps involved the mapping of information assets, the development of threat scenarios and risk mitigation plans. The IT personnel were needed to provide the technical in-depth knowledge that other members of the assessment team lacked.

5.1.3 Training and timescale requirements

Although the OCTAVE Allegro methodology has been designed for ease of application previous working knowledge and experience in any of the different OCTAVE risk assessments would be beneficial. This would enable an organisation to quickly become familiar with the guidance, worksheets and questionnaires associated with the OCTAVE Allegro method. Organisations totally new to the OCTAVE process are generally advised to set aside ample time to review the steps involved and perform basic ‘starter workshops’ to support the assessment team members. The SEI claim that by spending just one or two days following the guidance and self-explanatory worksheets included in the supporting documentation, an assessment team can become fully functional and ready to deploy the components of the Allegro method without significant delay or challenge (SEI 2007, 24).

Prior to starting the OCTAVE Allegro assessment the company decided to perform six separate three-hour starter workshop sessions spread across a one-month time period. The sessions were used to introduce the OCTAVE Allegro process to all team members to achieve a common base knowledge level before formally commencing the assessment programme.

When performing the practical element of the OCTAVE assessment the time commitment required from the organisational resources proved difficult to predict. This was not only dependent on the availability, experience and make-up of the assessment team, but also on other influential factors such as the complexity of a company information asset, the complexity of the environment in which the asset was stored, transported or processed, and the number of information assets that were reviewed. Due to the limited time and resources assigned to this research project it was decided that the number of information assets reviewed in the risk assessment would be minimised.

5.2 Performing the practical steps of the OCTAVE Allegro assessment

The practical steps of the OCTAVE Allegro risk assessment process were completed in different activity phases over a five-week period using the allocated organisational resources outlined in table 7. Eight practical steps split into four phases were performed in a workshop-style collaborative setting in accordance with the SEI’s guidance and worksheets. The relationship between the activity phases and steps of the methodology were previously illustrated in the OC-

TAVE Allegro roadmap in figure 12. A breakdown of how each of the phases and steps were completed over the five-week time period is defined in table 8.

Table 8. A breakdown of the OCTAVE Allegro phases and steps completed over the five-week time period.

Week number / Phase	**Step number / Purpose**
WEEK 1: ESTABLISH DRIVERS	STEP 1 – Establish risk measurement criteria
WEEK 2: PROFILE ASSETS	STEP 2 – Develop information asset profile STEP 3 – Identify information asset containers
WEEK 3: IDENTIFY THREATS	STEP 4 – Identify areas of concern STEP 5 – Identify threat scenarios.
WEEK 4+5: IDENTIFY AND MITIGATE RISKS	STEP 6 – Identify risks STEP 7 – Analyse risks STEP 8 – Select mitigation approach

The outputs from each step in the process were captured in a series of worksheets with the output of one step being used as the input into the next step of the process. The individual steps of the methodology are described in more detail below with the completed worksheets listed in the appendices.

5.2.1 Step 1 – Establishing risk measurement criteria

During the first step of the assessment process the team established the organisational drivers that were used to evaluate the effects of a risk to the company's mission and business objectives. Risk measurement criteria are essentially a set of qualitative measures against which the effects of a realised risk can be evaluated and form the foundation of an information asset risk assessment (SEI 2007, 17). It was important to use consistent risk measurement criteria that accurately reflected the company's view since it ensured that decisions about how to mitigate any identified risks would be consistent across the many and various information assets involving different departments.

To facilitate this first step the standardised set of blank OCTAVE Allegro worksheet templates were completed to create the relevant risk measurement criteria in several impact areas and then to prioritise them. During the process the assessment team identified high, medium, and low risk impacts within each of the following impact area categories:

- Worksheet 1 – Reputation and customer confidence
- Worksheet 2 – Financial
- Worksheet 3 – Productivity
- Worksheet 4 – Health and safety
- Worksheet 5 – Fines and legal penalties
- Worksheet 6 – ‘User-defined’

The five standardised impact area categories and the impact areas listed within each were common to most of the company’s mission and business objectives. However, there were still company specific impact areas of importance that were missing. To enable customisation of the worksheets each worksheet contained an option entitled ‘other’ to supplement the standard impact areas with additional categories that were more meaningful to a company. A sixth worksheet was also provided which focused on a ‘user-defined’ impact area category along with standard impact areas. Due to the necessity for the company to outsource smaller project-related manufacturing and processing tasks to third parties it was concluded that the sixth worksheet would be used and customised to focus on the impact area category involving ‘customer responsibility’.

Once the assessment team had populated the relevant company information into the predefined and user-defined impact areas across the six worksheets a seventh worksheet entitled ‘impact area prioritisation’ was used in calculating the relative risk scores. The process resulted in the prioritisation of the impact area categories with the most important category receiving the highest score of (6) and the least important category receiving the lowest score of (1). All six of the completed impact area category worksheets and the seventh impact area prioritisation rankings are available in appendices one to seven of this report.

5.2.2 Step 2 – Developing an information asset profile

The primary focus of an OCTAVE Allegro assessment is on the information assets of a company. In the second step the team began the process of identifying the company's information assets on which the assessment was later performed. Using the SEI's guidance the following questions were considered when identifying the company's critical information assets:

- What information assets are the most valuable to the company?
- What information assets are used in the day-to-day work processes and operations within the company?
- What information assets, if lost, would significantly disrupt the company's ability to accomplish its goals and contribute to achieving its mission?
- What other assets are closely related to these assets? (SEI 2007, 35)

Once the critical information assets were identified a 'profile' was created for each, which formed the basis for the identification of threats and risks in the subsequent steps. The profile is a representation of an information asset describing its unique features, qualities, characteristics and value. The profiling process ensured that the boundaries of an identified asset were clearly described and that the security requirements for the asset were also adequately defined (SEI 2007, 18-35). The profile for each company asset was captured on a single worksheet. The completed worksheets are available in appendix eight.

5.2.3 Step 3 – Identifying information asset containers

Step three of the process involved the identification of the company's information asset containers. An information asset container describes the places where information assets are stored, transported, or processed and is a place where an information asset 'resides'. Containers are most typically identified as some form of information asset such as hardware, software, application systems, servers and networks. However, a container can also include items such as files and folders where information is stored in written form as well as any person authorised to carry around intellectual property or information that is sensitive or confidential. The person who possesses such key organisational information is essentially classed as a 'container' and must be considered when profiling risks to that particular information asset.

During the risk assessment the identification of information asset containers was essential to identifying the risks to the information asset itself. By mapping an information asset to all of the containers in which it 'resides' the process defines the boundaries of the technical environment and infrastructure that were then examined for risk. Any risk to the containers in which an information asset resides are inherited by that particular information asset. During the container identification process it was recognised that some of the information assets not only reside within containers in the company's boundaries but also reside in containers that were not under the direct control of the company.

Worksheet 9a was used to identify and record the containers that were under direct internal control of the company and those that were managed outside of the company. Worksheet 9b was used to identify the physical locations where the information assets existed either inside or outside of the company. Worksheet 9c was used to identify people that were internal or external to the company with detailed knowledge of the information asset. The assessment team and other influential personnel were used to develop an accurate map of all the places where the company's information assets were stored, transported or processed. Appendix nine lists the results of these activities.

5.2.4 Step 4 – Identifying areas of concern

Step four involved the development of information asset risk profiles for the company's information assets. Here the assessment team began to address the threat component of the risk identification process by brainstorming the possible conditions or situations that could threaten a company information asset. These scenarios are referred to as 'areas of concern' and may represent threats and corresponding undesirable outcomes. By identifying areas of concern any threat that is unique to the company and its operating conditions could be quickly established.

The purpose of this step was not to focus on capturing a complete list of all possible threat scenarios related to an information asset, but to quickly capture and record obvious situations or conditions. This step was performed by the assessment team who considered the various actors, motives and outcomes inherent in the area of concern whilst keeping in mind the security requirements for the particular information assets. This included agreeing how these assets might be compromised due to a threat in a 'real-world' scenario. The areas of concern were then captured and recorded on the information asset risk Worksheet *ten* with the details used to feed into the development of risk profiles in step five. The completed Worksheets can be viewed in the appendices.

5.2.5 Step 5 – Identifying threat scenarios

In the fifth step of the process the documented areas of concern captured in the preceding step were expanded into threat scenarios that further detailed the properties of the identified threats. In order to expand the areas of concern more accurately, four different categories of threat 'tree' models were used from the SEI's supporting documentation (SEI 2007, 49-50). Each threat tree structure visually represents a range of threat scenarios to help the assessment team consider a range of potential threats to the company's information assets when determining risk. A description of the four different threat tree categories is described in table 9.

Table 9. Description of the four OCTAVE Allegro threat tree categories (SEI 2007, 19).

Threat Tree category	**Definition of category**
Human actors using technical means	The threats in this category represent threats to an information asset via a company's technical infrastructure or by direct access to a container (technical asset) that hosts the asset. They require direct action by a person and can be deliberate or accidental in nature.
Human actors using physical means	The threats in this category represent threats to an information asset that result from physical access to the asset or container that hosts the information asset. They require direct action by a person and can be deliberate or accidental in nature.
Technical problems	The threats in this category represent problems with a company's IT and systems such as software and hardware defects, malicious code (e.g., viruses), and other system-related problems.
Other problems	The threats in this category are problems or situations that are outside the control of the company. Examples include natural disasters (e.g., floods, earthquakes) and interdependency, which include critical infrastructures not being available (e.g., power supply).

The threat scenarios derived from the areas of concern correspond to a branch of a threat tree. To ensure a more robust consideration of the threats, each branch of the threat tree was considered for each information asset. The information asset environment maps (Worksheets 9a, 9b and 9c) created in step four were used to assist with the process.

5.2.6 Step 6 – Identifying risks

With the threat scenarios identified in step five, the sixth step focused on the consequences for the company should a threat be realised. The assessment team analysed each of the threat scenarios recorded on the information asset risk worksheets to determine how the company would be impacted. A minimum of one consequence was documented with others added as necessary. It was important for the team to understand that a threat can potentially have multiple impacts on the company. For example, it might affect both the reputation and the financial position of the company. By identifying how the company would be impacted the risk equation was completed, which can be illustrated as follows:

Threat (condition) + Impact (consequence) = Risk
[Steps 4 and 5] + [Step 6] = Risk

A risk is the probability of the company suffering harm or loss from a person doing something undesirable or a natural occurrence causing an undesirable outcome resulting in a negative impact or occurrence. A risk is composed of three elements: an event, a consequence and uncertainty. (SEI 2007, 53)

5.2.7 Step 7 – Analysing risks

For the seventh step of the Allegro process the assessment team qualitatively measured the extent to which the company would be impacted by a threat. This was achieved by calculating a risk score for each risk to each information asset. The scoring information was then used to assist the team with determining which tasks needed to be mitigated immediately and for prioritising mitigation actions for the remaining risks that were tackled in final eighth step.

Through the guidelines and examples provided in the SEI's documentation the team followed a set of calculation methods to generate a relative risk score for each information asset. The relative risk scores were obtained by considering the extent to which the different consequences of risks recorded in Worksheets *ten* affected the company compared with the relative importance of the high, medium and low impact areas in Worksheets *8*. For example, if reputation was of particular importance to the company and the consequence of a risk would cause significant damage to the company's reputation then action must be taken to ensure the risk is mitigated. By using these criteria the assessment team ensured that the risks were scored in the context of the organisational drivers.

This step in particular required the team to combine their own company knowledge with common sense. The SEI guidance states that the different risk scores generated are only to be used as a prioritisation tool and that differences between risk scores are not considered to be of significance. For example, a risk score of 40 would mean that the risk is relatively more important to the company than a score of 25, but there is no importance placed on the difference in the 15 points. The different risk score outcomes can be viewed between appendices ten to fourteen.

5.2.8 Step 8 – Selecting a mitigation approach

In the eighth and final step of the OCTAVE Allegro assessment process the team determined which of the identified risks from step seven would be mitigated and how. This was achieved by first prioritising the risks based on their relative risk score from step seven and then deciding on an approach to mitigate the most important risks based on a number of organisational factors.

The company's decision to accept a risk, mitigate it or defer it was based on a number of important and influential factors. Although the impact value of a risk was a primary driver so was the probability of its occurrence. For example, a risk that could seriously or significantly impact the company but was highly unlikely to occur was ranked highly for priority mitigation. Since the impact and risk of a threat is specific to the company the assessment guidelines alone do not provide a decisive path regarding which risks to mitigate. This was a decision that had to be driven by the individual team members involved in the risk assessment together with their knowledge of the company.

SEI's guidance documentation assisted in sensibly categorising the risks. Once the risks had been prioritised and a decision made to mitigate one or more of them, a mitigation strategy was developed by the team. This considered the value of the assets, the places where they reside and the company’s unique operating environment. The decision to mitigate a risk was a complex endeavour that required discussion with the necessary relevant skilled personnel within the company. Throughout the process it was important to have the support of the senior management and to collaborate with the IT department and other stakeholders to develop balanced and cost-effective mitigation strategies that provided the best overall long-term protection for the company.

6 PERFORMANCE AND ANALYSIS OF THE ISRA

The content featured in this chapter will not be published since it discusses information which is confidential and under a Non-Disclosure Agreement (NDA).

7 IMPLEMENTATION PLAN FOR MITIGATING RISKS

The content featured in this chapter will not be published since it discusses information which is confidential and under a Non-Disclosure Agreement (NDA).

8 RECOMMENDATIONS FOR FUTURE DEVELOPMENT

8.1 Strategy and timeline for implementing the risk mitigation proposals

The previous chapter outlined the proposed risk mitigation policies and practical procedures that will need to be implemented throughout the five identified areas of concern also known as ‘threat areas’. The principal of each risk mitigation proposal was researched and then discussed during several action-plan meetings held between senior management, IT personnel and the researcher. Further iterations were then made between the board of directors and senior management, which concluded with approval to proceed with more detailed research and development for each risk mitigation approach. The completion of more detailed research will promote the development of the best possible mitigation methods to ensure that financial and human resources are carefully considered for the optimum solution.

Table 10 featured in chapter seven lists the five threat areas that could potentially lead to the greatest risk and impact on company operations. The probability of these risks occurring and the severity of the associated impact have been calculated in each case. Under normal circumstances a complete company-wide OCTAVE Allegro risk assessment could take considerably more time (months) and resources to implement fully. This would likely identify many more areas of concern of the order of maybe ten times than has been the case for this limited risk assessment. Because of the restricted scope of this research project the number of risks to be scored, prioritised and mitigated were far fewer. Based on the relative risk scores assigned to the five threat areas the order of prioritisation to mitigate each of them would be as follows:

1) VPN connections – Risk score 57

2) Off-site backups stored to USB hard disk – Risk score 52

   Email Encryption – Risk score 52

3) Unlocked PC workstations – Risk score 45
4) Control of printed technical documentation – Risk score 43

Although the relative risk scores created from an OCTAVE Allegro assessment should primarily be used to define the order of risk mitigation, there are other factors, which can effect prioritisation. For example, the immediate availability of appropriately skilled personnel within the company assigned to research and test more secure software systems. The availability of finance to immediately purchase and implement the necessary company-wide training for these system upgrades would also influence prioritisation.

Further iterations between senior management, IT personnel and the researcher concluded that the less complex and less resource intensive risks that pose the least amount of disruption to the company's workflow would be mitigated first. In order to differentiate the complexity of tasks each of the five threat areas were broken down into smaller 'sub-tasks'. An estimate of the human resources and costs required to complete each sub-task was made taking account of the disruption to the company's daily operations and of any training required to support the mitigation activity. At the time of writing this report a completed 'action plan' was still being adjusted to finalise a comprehensive mitigation strategy. This strategy was not available for inclusion in this report and the timeline for the tasks and sub-tasks will not be discussed in any further detail.

8.2 Recommendation 1 – Further OCTAVE Allegro risk assessments

Only one critical company information asset was reviewed in the OCTAVE Allegro risk assessment due to the limited time and resources assigned to this research project. The investigation of other critical information assets will require a similar assessment process to be conducted. However, these future assessments would be subject to senior management's approval and the availability of resources. The operational environment of the company is continually evolving and because the OCTAVE Allegro assessment is essentially a 'snapshot' of the ‘health’ of the IT security it can quickly become out-dated. An OCTAVE Allegro assessment will therefore need to be repeated every time there is a significant change in an information asset’s risk environment.

One option is for the company’s IT personnel to schedule all smaller assessments to ensure that changes in the risk environment are tracked at regular intervals ensuring that they receive the proper attention required. However, there is concern that if significant changes to the company’s operational environment are implemented between these regular scheduled assessments then new risks might be introduced without being mitigated. Another approach would be for the company to perform a new assessment whenever there is a significant change to an information asset or its environment. This approach is more suited to regularly changing environments. The company needs to determine criteria for repeating the OCTAVE Allegro assessment and implementing and adopting this as company practice and policy. (SEI 2007, 25)

8.3 Recommendation 2 – IT security penetration testing

Ensuring the long-term security of the company’s IT systems and critical information assets will involve more than just the completion of a single OCTAVE Allegro risk assessment. Further ongoing action will be required to supplement the improved *‘patch’* management, firewall protection, anti-virus software and other protective measures discussed in chapter seven. The long-term information security improvement process will require frequent ‘real-world’ validation to confirm which software and systems are reliably effective and those that are prone to failure. One of the most effective ways to identify weaknesses and deficiencies in any of the company’s programs and systems is to perform IT security penetration testing.

A penetration test, also known as ‘ethical hacking’ and ‘white-hat hacking’, is an authorised attempt to defeat the security protection of an IT system by safely attempting to exploit system vulnerabilities, including any OS, service and application flaws, improper configurations and/or end-user behaviour (Landoll 2010, 15). A penetration test enables a company to assess its own ability to protect its IT network(s), applications, endpoints and users from external or internal attempts to breach its security controls and gain unauthorised or privileged access to protected critical information assets. (Coresecurity 2015)

With the completion of the company's first ever ISRA in line with the OCTAVE Allegro industry standard framework the risks identified during the process will be mitigated by implementing the necessary software, hardware and information security policy improvements described at the start of this chapter. Once these necessary changes are implemented it is recommended that a penetration test is performed to provide senior management with further evidence to reassure that the risk mitigation measures introduced are fully effective and that the financial and human resource investments were justified.

The penetration test process will enable the company's authorised IT personnel to rigorously simulate the methods that a potential attacker might use to circumvent security controls, bypass security mechanisms and gain access to the company's critical information systems. Software such as 'Metasploit' by Rapid7 can be freely downloaded and used to perform reliable penetration tests to identify security issues and verify that any risk mitigation measures taken have been effective. The Metasploit framework is the world's most used open source platform, which encompasses contemporary hacking tools and techniques to confirm that existing information security controls provide effective protection. The framework also provides a consistent, reliable library of constantly updated actions for automating every aspect of a penetration test (Engebretson 2011, XIV). Part of the process includes probing for vulnerabilities as well as providing 'proof of concept' attacks to demonstrate that these vulnerabilities are real. (Kennedy et al. 2011, 1-6)

Once complete the results of a penetration test will identify possible ways in which an attacker might be able to compromise the company's security controls to exploit the critical information systems and potentially damage the company. In many cases the data obtained from a successful penetration test will often uncover issues that an architecture review or vulnerability assessment would not have been able to identify. A properly executed penetration test will result in specific recommendations for addressing and fixing issues identified during the test. These can then be used to help further develop, improve and secure the necessary hardware and software systems against future attack. (Kennedy et al. 2011, 1-6)

By embracing frequent and comprehensive penetration testing the company will be more effective in countering any emerging security risks and preventing unauthorised access to critical systems and valuable information. Penetration testing will enable the company to meet its objectives by intelligently managing security vulnerabilities, avoiding the cost of network and system down time when recovering from a security breach, meeting regulatory requirements, avoiding fines and preserving their corporate reputation and customer loyalty.

8.4 Recommendation 3 – Information security awareness and training

It is a common misjudgement by companies, similar to the one in this research project, not to invest financial and human resources in securing their information technology software and hardware assets. Equally, little if any investment is made in ensuring that their employees are educated in the importance of these security measures. As a result, it is often the people and not the technology that are responsible for compromising the information security chain. It is essential that the company complement the reinforced technical information security controls with an ongoing programme of information security awareness, training and educational activities for their employees to avoid human vulnerabilities undermining these technical advances.

Similar to health and safety or any form of legal compliance, it is unrealistic for senior management to simply expect employees to comply with company information security policies, adopt security standards and follow security procedures if they are not fully informed of their personal responsibilities as part of an organisation. Information security awareness is therefore an essential element of an effective information security management system supporting and enhancing the technical and procedural information security controls and contributing to a company’s overall IT governance framework. (Hinson 2009, 1-7)

Information security awareness can be loosely defined as the extent to which personnel within a company fully understand the importance of information security, the level of security required by that organisation and their individual security responsibilities (ISF 2007, 92). In order to establish a genuine security culture throughout any company, awareness will need to go well beyond simply informing the employees of their security obligations. To overcome the inevitable resistance to change employees will have to be both informed and motivated to modify their behaviour in order to think security and act more securely. (Herold 2013)

The most effective way to secure the ‘human element’ in the security chain will be to implement a company-wide high-impact information security awareness training program that goes beyond just compliance of changing the long-term outlook of the company on this critical subject matter. Although the company’s IT personnel are competent in information security awareness the security training programme would best be delivered by a skilled professional training organisation. However, the training programme will need to incorporate knowledge specific to the members of the IT department who will be able to assist with this.

Company personnel will be taught the key elements of information security, why it is needed, their personal mandatory responsibilities and why a vigilant attitude will provide a safer more efficient working environment. The training will also ensure that role-based, security-related training is undertaken before personnel will be granted renewed authorisation to access the information systems after the security updates and improvements have been implemented. Regular security-related refresher training will need to be planned in accordance with the company-defined frequency. A carefully monitored information security awareness training programme will help ensure that company employees have a solid understanding of the company security policy, procedures and best practices in place.

8.5 Recommendation 4 – Improved IT management roles and responsibilities

The completion of the ISRA not only uncovered several critical risk areas to be mitigated, but also highlighted the necessity for a more knowledgeable and re-structured IT department. The previous sub-section 8.4 outlined the proposals for the implementation of a company-wide information security awareness-training programme to address the identified knowledge shortfall. Training would increase in-depth understanding of the company policies, procedures and introduce other industry standard best practices.

However, the structure of the company's IT department lacks a designated person who would take on the role and responsibility of establishing and enforcing information security policies that protect the company's IT infrastructure, networks and data (Linton 2015). This responsibility would usually fall to an information system security officer (ISSO).

An information system security officer is given the responsibility for ensuring that a company's operational security is appropriately maintained for an information system. The officer works in close collaboration with the information system owner such as the IT Administrator and serves as a principal advisor on all matters technical and otherwise involving the security of an information system. The officer must have the relevant detailed knowledge and expertise required to manage all security aspects of an information system. He/she is assigned responsibility for security operations of a system ensuring that the security of company personnel, handling of security incidents and organising information security awareness training are carried out. (Linton 2015) (NIST 2010b, 70)

It is recommended that the company appoint a suitable candidate to undertake the role of an information security officer. Due to the relatively small size of the company and the limited resources it will be more cost effective to train an existing capable employee to a reasonable level of competency. The person who will be working within the boundaries of the company would be called upon to assist in the development of and compliance with security policies and procedures. The appointee would actively participate in the monitoring of the company's IT systems and their environment of operation to assist in developing and updating the security plan, managing and controlling changes to the system and assessing the impact on security of those changes (NIST 2010b, 70).

9 PROJECT EVALUATION SUMMARY

9.1 Achieving the research objectives

Chapter two of this report outlined four main research objectives forming the scope for this research project. The chosen project objectives were specific, measurable (ISRA assessment), achievable, realistic and timely to ensure that the research problem was explored effectively. The clearly defined project objectives enabled the research team to focus on the research problem, avoid the collection of unnecessary data, provide a clear direction to the research study and contribute a practical and theoretically sound framework of proposals to improve the company's IT systems security.

Achieving the four objectives proved to be a demanding task given the limited time constraints and reduced human and financial resources decided by senior management. The research, selection and then execution of the company specific ISRA required considerable effort in coordinating the personnel involved. Careful planning and professional guidance in the supporting ISRA documentation meant that this research project was able to fulfil the requirements of all four objectives. A brief summary of how each objective was achieved is discussed in the following sub-sections below.

9.2 Objective 1 – Identifying the company's information security risk status

Prior to the start of this project, the first of the four research objectives involved an extensive company-wide preliminary investigation by the research team to identify, present and then discuss the status of the existing information security. The information gathered during these initial investigations concluded that the company's existing mechanisms for maintaining a secure IT system environment were relatively primitive and troubled with inconsistencies. There were no rigorous policies, procedures or industry standard framework for conducting on-demand information security risk assessments in place.

Further investigations were carried out to understand the international standards, binding contractual obligations and customer specific requirements adhered to by the company. The results identified that ISO 9001:2008, AS9100, Nadcap and Boeing QMS international standards and special requirements demand that to some extent these are all dependent on the company's internal IT environment to execute the defined tasks. Although some developments had been made to the company's IT systems security in order to meet standards and requirements, it became clear that the overall level of the systems security did not align with the highly onerous stipulations for the specialist precision engineering work in the aerospace and defence industries.

9.3 Objective 2 – Selecting an appropriate industry standard ISRA framework

Taking into consideration the influential criteria and interaction within the company's IT environment the second objective was to select an appropriate industry standard information security risk assessment (ISRA) framework for developing improved information system security controls. A cross-section of viable ISRA frameworks was investigated and rationalised to shortlist four globally respected 'best-practice' options. These were the 'COBIT' and 'OCTAVE' security risk assessment methods, the 'NIST SP 800' series of computer security guidance publications and the 'ISO/IEC 27000' family of international information security standards.

With no rigorously documented policies and/or procedures in place, limited resources and lack of internal experience in performing an ISRA the OCTAVE Allegro lean assessment methodology was deemed to be the most beneficial of the four options. The OCTAVE Allegro method is user-friendly and contains a refined risk assessment scope. It only requires a limited level of knowledge and training to understand the processes involved and therefore fewer resource commitments were needed. In addition the output of consistent and comparable results facilitated a risk-aware culture and supported the company's business compliance activities.

The OCTAVE Allegro method is particularly suited for use for performing a security risk assessment without extensive organisational involvement, expertise, or input. Therefore, this particular lean method of performing a usually complex ISRA fitted the requirements of this research project since the core areas of research were conducted by an individual employee of the company (the researcher) working with very limited support from a relatively small and unskilled internal group of company personnel.

9.4 Objective 3 – Performing an ISRA on the company's IT infrastructure

The fulfilment of the third objective required extensive preparation for the processes involved in conducting the OCTAVE Allegro ISRA on selected areas of the company's existing IT infrastructure. From the outset it was ensured that senior management were fully informed, committed and available when necessary to provide active support to the risk assessment process. Company personnel with relevant skill sets were recruited to assist the project team with the risk assessment process. They were trained how to perform the OCTAVE Allegro ISRA during several in-house workshop sessions. Importance was placed on those who had knowledge and experience in working within the operational areas of the business that the risk assessment was to be focused on.

The data collected from the assessment helped both the research team and senior management to understand how the component parts of the company's IT systems assisted with their daily business functions and clearly identified the impact on the business should these systems fail due to breaches of security. The company's internal ERP system was identified as the most critical information asset of greatest concern that could be directly or indirectly threatened. Guidance, worksheets and examples from the supporting Allegro documentation provided the assessment team with a structured path when performing the risk assessment. The simplicity of the OCTAVE Allegro methodology helped considerably in reducing company human resources and minimising the time spent on the ISRA.

9.5 Objective 4 – Proposing a development plan from the results of the ISRA

The fourth and final research objective involved the proposal of a development plan from the results of the ISRA. This was to assist the company with the implementation of the necessary information system security control improvements and an information security awareness-training programme across the company. The OCTAVE Allegro's risk mitigation prioritisation process for the identified risks provided senior management with a clear view of what needed to be achieved to immediately improve the company's weakest links in their IT systems security. This information together with further detailed research enabled the assessment team to propose five risk mitigation proposals – one for each of the five areas of concern (threat areas).

The majority of this objective was achieved with the detailed mitigation proposals, which are outlined in chapter seven of this report. Recommendations for future development of IT system security, building on the first company specific Allegro risk assessment, provided a solid foundation for further similar assessments to be conducted at regular intervals in the future. Although the company managed to successfully complete this ISRA the implementation of a company-wide information security awareness training programme and more advanced testing such a 'penetration testing' techniques would be required. These elements are recommended but were unable to be implemented within the limited scope of this research project.

9.6 Comment – Limitations of the research project

The scope of this report was significantly reduced after it had commenced. The Company Board of Directors advised senior management that, due to unforeseen circumstances, the human resources and funding previously envisaged should be scaled back and rationalised. This meant that it would not be possible to conduct in-depth analysis on industry standard information controls.

This report also highlighted that due to the continually evolving operational environment of the company a single OCTAVE Allegro risk assessment only provided a snapshot indication of the health of specified areas of the existing IT systems security. It was also identified that in order to obtain long-term benefit from the conducted OCTAVE Allegro assessment the company would need to perform further assessments at regular intervals over the forthcoming years. The future success of the recommended IT systems security improvements is interdependent with continued company-wide support of senior management and in promoting and enforcing security awareness. Due to the limitations of this research project the period following the completion of this report will be critical to the success or failure of the company’s information security protection strategy and mitigation plans.

OCTAVE Allegro is a lean risk assessment method and does not provide guidance in selecting security controls. A comprehensive list of controls and control objectives intended to address specific requirements identified via a formal risk assessment are provided in ISO/IEC 270002, from the ISMS family of international standards. ISO/IEC 270002 would have been utilised extensively to assist with the creation of fully customised company-specific information security controls. However, this was not possible with the reduced project scope, resources and funding allocated by the company to this research project.

References

ACQ, 2011. *'DPAP Defence Procurement and Acquisition Policy – Offsets of Foreign Military Sales'*. Consulted: 17.2.2013.
http://www.acq.osd.mil/dpap/cpic/ic/offsets_of_foreign_military_sales.html

Alberts, C., and Dorofee, A., 2004. *'Managing Information Security Risks – The OCTAVE Approach'.* 2nd edition. USA: Pearson Eduction, Inc.

Aptean, 2013. *'What is an ERP System?'.* Consulted: 22.7.2013.
http://www.aptean.com/solutions/application/erp-solutions

Avison, D., Lau, F., Myers, M., and Nielsen, P. A., 1999. *'Action Research'* Communications of the ACM Vol. 42. No 1/1999. p94 – 97. Consulted: 16.3.2013.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.4732&rep=rep1&type=pdf

Baskerville, R., and Myers, M. D., 2004. *'MIS Quarterly Special Issue – Special issue on Action Research in Information Systems: Making IS Research Relevant to Practice – Foreword'.* MIS Quarterly Vol. 28, No. 3, p329-335, September 2004. Consulted: 20.4.2013.

Baxter, P. and Jack, S., 2008. '*Case Study Methodology: Study Design and Implementation for Novice Researchers*'. McMaster University, Canada. The Qualitative Report, Vol. 13, No. 4, p544-559. Consulted: 22.5.2013. http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf

BIS, 2013. *'Bureau of Industry and Security – Reporting offset agreements – Background'*. Consulted: 17.2.2013.
http://www.bis.doc.gov/index.php/other-areas/strategic-industries-and-economic-security-sies/contact-the-office-of-strategic-industries-a-economic-security/guidance-for-reporting-on-offset-agreements

Boeing, 2010. *'Nadcap Accreditation – Frequently Asked Questions'.* Consulted: 15.3.2014.
http://www.boeingsuppliers.com/nadcap/nadcap_faq.htm

Boeing, 2011. *'Boeing Quality Management System Requirements for Suppliers'*. Supplier Quality Integration Team (SQIT). Document Number: D6-82479. Consulted: 12.3.2014.
http://www.boeingsuppliers.com/supplier/D6-82479.pdf

Boeing, 2013. *'Boeing – About Us'*. Consulted: 17.3.2014.
http://www.boeing.com/company/

CERT, 2013a. *'CERT – Home – Cyber Risk and Resilience Management – Products & Services – Octave – Octave Method'.* Consulted: 22.12.2014
http://www.cert.org/resilience/products-services/octave/

CERT, 2013b. *'CERT – Home – Cyber Risk and Resilience Management – Products & Services – Octave – Octave-S Method'.* Consulted: 22.12.2014
http://www.cert.org/resilience/products-services/octave/ocatve-s-method/

CERT, 2013c. *'CERT – Home – Cyber Risk and Resilience Management – Products & Services – Octave – Octave Allegro Method'.* Consulted: 27.9.2013
http://www.cert.org/resilience/products-services/octave/ocatve-allegro-method/

Chabrow, E., 2014. *'Mapping NIST Controls to ISO/IEC Standards'.* Consulted: 6.6.2014.
http://www.bankinfosecurity.com/mapping-nist-controls-to-iso-standards-a-7251

Cisco, 2015a. *'VPNs and VPN Technology'*. Consulted: 3.3.2015.
http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=3

Cisco, 2015b. *'Cisco AnyConnect Secure Mobility Client and Cisco ASA 5500 Series SSL / IPsec VPN Edition'*. Consulted: 4.3.2015.
http://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/product_data_sheet0900aecd80402e3f.html

Coghlan, D., and Brannick, T. 2010. *'Doing action research in your own organisation'.* 3rd edition. London, UK: SAGE Publications Ltd.

Collis, J., and Hussey, R. 2009. *'Business Research – A practical guide for undergraduate and post graduate students'.* 3rd edition. Basingstoke, UK: Palgrave Macmillan.

Company X, 2013. *'Company X – Front Page'.* Consulted: 10.1.2013.
http://www.companyx.com/index.php/en/

Coresecurity, 2015. 'Penetration Testing Overview'. Consulted: 4.3.2015.
http://www.coresecurity.com/penetration-testing-overview

COSO, 2011. *'COSO: Internal Control – Integrated Framework'*. Consulted. 6.11.2014.
http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

Davison, R. M., 1998. *'An Action Research Perspective of Group Support Systems'*.
City University of Hong Kong, Doctor of Philosophy Ph.D dissertation. Chapter 3: Research Methodology. p3-1. Consulted: 18.3.2013. http://www.is.cityu.edu.hk/staff/isrobert/phd/phd.htm

Davis, C., and Schiller, M. 2011. *'IT Auditing – Using Controls to Protect Information Assets'.* 2nd edition. USA: McGraw-Hill.

Eisenhardt, K. M., 1989. *'Building Theories from Case Study Research'*. The Academy of Management Review. Vol. 14, No. 4, p 532-550. Consulted: 19.5.2013.
http://www.jstor.org/stable/258557?seq=3#page_scan_tab_contents

Engebretson, P., 2011. *'The Basics of Hacking and Penetration Testing – Ethical Hacking and Penetration Testing Made Easy'*. 1st edition. USA: Syngress (Elsevier Inc.)

Fastems, 2012. *'Fastems Factory Automation – Products – Automation software – Fadector'*.
Consulted: 6.1.2014.
http://www.fastems.com/en/products/automation_control_systems/fadector/

FQS, 2009. *'Ontological and Epistemological Foundations of Qualitative Research – The Path of Epistemological Reflection'.* Consulted: 3.01.2014.
http://www.qualitative-research.net/index.php/fqs/article/view/1299/3163

FT, 2013. *'Aerospace & Defence – Q&A: what are offsets?'.* Consulted: 19.2.2013.
http://www.ft.com/intl/cms/s/0/87728d1e-197a-11e3-afc2-00144feab7de.html#axzz3bqhhZzGw

Geier, E., 2013. *'How (and why) to set up a VPN today – Picking a secure Protocol'*. Consulted: 6.3.2015. http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

Galliers, R. D., 1992. *'Choosing Information Systems Research Approaches in Information Systems Research: Issues, methods and practical guidelines*'. 1st edition. UK: Blackwell Scientific.

GAO, 1999. *'Information Security Risk Assessment – Practices of Leading Organisations'.* Consulted: 5.6.2014. http://www.gao.gov/special.pubs/ai00033.pdf

Greener, S., 2008. *'Business Research Methods*'. 1st edition. UK: Ventus Publishing ApS https://kosalmath.files.wordpress.com/2010/08/introduction-to-research-methods.pdf

Herold, R., 2013. *'Why Information Security Training and Awareness are Important'*. Consulted: 15.4.2015. http://www.infosectoday.com/Articles/Security_Awareness_Training.htm

Higgins, S., 2013. '*Information Security Management: The ISO 27000 (ISO27K) Series"* Consulted. 18.6.2013. http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/information-security-management-iso-27000-iso-27k-s

Hinson, G., 2009. *'Handbook of Research on Social and Organisational Liabilities in Information Security'*. 1st edition. New Zealand: IsecT Ltd.

Howell, K. E., 2013. *'An Introduction to the Philosophy of Methodology'*. 1st edition. London, UK: SAGE Publications Ltd.

ISF, 2007. *'Information Security Forum – The Standard of Good Practice for Information Security'.* Consulted: 16.4.2015. https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf

Infosec Institute, 2013. *'VPN Pivoting – What is VPN Pivoting?'*. Consulted: 12.3.2015 http://resources.infosecinstitute.com/vpn-pivoting/

InSolution, 2014. *'Fadector – Product Info - Fadector, data collection and reporting system for production machinery'.* Consulted: 8.2.2014. http://fadector.insolution.fi/product_info.php?tab=5

IIA, 2013. *'The IIA Research Foundation – Topics – Cobit 4.1'*. Consulted: 17.10.2014 http://www.theiia.org/bookstore/product/cobit-41-1200.cfm

ISACA, 2009a. *'Val IT Brochure'.* Consulted: 1.11.2014. http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Documents/Val-IT-Brochure.pdf

ISACA, 2009b. *'Risk IT Brochure'*. Consulted: 3.11.2014. http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Documents/Risk-IT-Brochure.pdf

ISACA, 2011. *'Cobit Process Assessment Model – Using Cobit 4.1'*. Consulted: 29.9.2013. http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cobit-assessment-program.aspx

ISACA, 2012a.*'Cobit – A Business Framework for the Governance and Management of Enterprise IT'.* Consulted: 8.9.2014. http://www.isaca.org/COBIT/Documents/COBIT5-Ver2-FrameWork.pdf

ISACA, 2012b.*'A Cobit 5 Overview'.* Consulted: 15.9.2014. http://www.isaca.org/COBIT/Documents/A-COBIT-5-Overview.pdf

ISACA, 2013a. *'Cobit 4.1 Brochure'.* Consulted: 16.9.2014. http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-4.1-Brochure.pdf

ISACA, 2013b. *'Cobit 4.1: Framework for IT Governance and Control – Overview'.* Consulted: 16.9.2014. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

ISACA, 2013c. *'About Cobit 5: The Enterprise IT governance and management framework – What is COBIT 5?'*. Consulted: 18.9.2014. https://cobitonline.isaca.org/about

ISO, 2011. *‘ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management’*. Consulted: 19.6.2013.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

ISO, 2013a. *‘About ISO – What is ISO?’*. Consulted: 11.11.2013.
http://www.iso.org/iso/home/about.htm

ISO, 2013b. *‘ISO 9000 – Quality Management”.* Consulted: 12.11.2013.
http://www.iso.org/iso/iso_9000

ISO, 2013c. *‘Standards – Management System Standards’.* Consulted: 14.11.2013.
http://www.iso.org/iso/home/standards/management-standards.htm

ISO, 2013d. *‘ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements’*. Consulted: 19.6.2013.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO, 2013e. *‘ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls’*. Consulted: 19.11.2013.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

ISO, 2014a. *‘ISO/IEC 27000:2014 – Information technology – Security techniques – Information security management systems – Overview and vocabulary’*. Consulted: 27.2.2014.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

ITGI, 2007. *‘Cobit 4.1 – Framework, Control Objectives, Management Guidelines, Maturity Model’.* Consulted: 16.9.2013.
http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

IT Governance, 2013. *‘The ISO/IEC 27000 Family of Information Security Standards’.* Consulted: 18.11.2014.
http://www.itgovernance.co.uk/iso27000-family.aspx#.VDlr6CmSxUM

ITIL, 2013. *‘What is ITIL? ITIL: Overview and Benefits’.* Consulted: 8.11.2014.
http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

Kadam, A. W., 2012. *‘CSI Communications – The Evolution of Cobit’.* Consulted: 15.9.2014.
http://www.csi-india.org/c/document_library/get_file?uuid=03800361-1386-4416-bfb6-6bfe474e8ef9&groupId=10157

Keighley, 2013. *‘Nadcap Merit Accreditation’.* Consulted: 13.4.2014.
http://www.keighleylabs.co.uk/keighley-laboratories-achieves-nadcap-merit-accreditation/

Kennedy, D., O’Gorman, J., Kearns, D., and Aharoni, M., 2011. *'Metasploit – The Penetration Tester’s Guide'.* 1st edition. San Francisco, USA: No Starch Press.

Koshy, E., Koshy, V., and Waterman, H., 2011. *'Action Research for Improving Educational Practice – What is Action Research?'.* 2nd edition. London, UK: SAGE Publications Ltd.

Kouns, J., and Minoli, D. 2011. *‘Information Technology Risk Management in Enterprise Environments’*. 1st edition. New Jersey, USA: John Wiley & Sons, Inc.

Krmac, E. V., 2011. ‘*Intelligent Value Chain Networks: Business Intelligence and Other ICT Tools and Technologies in Supply / Demand Chains’.* p591. Consulted: 12.7.2013.
http://www.intechopen.com/download/get/type/pdfs/id/18527

Landoll, D. J. 2011. *‘The Security Risk Assessment Handbook’*. 2nd edition. Boca Raton, USA: CRC Press.

Lewis, J., and Ritchie, J. 2003. *'Qualitative Research Practice – A guide for social science students and researchers'.* 1st edition. London, UK: SAGE Publications

Linton, I., 2015. *'Responsibilities of an Information System Security Officer'*. Consulted: 01.01.2015.
http://work.chron.com/responsibilities-information-system-security-officer-15533.html

Mataracioglu, T., and Ozkan, S. 2011. *'Governing Information Security in Conjunction with COBIT and ISO 27001'.* White paper. Ankara, Turkey. Consulted: 9.6.2013.
http://arxiv.org/pdf/1108.2150.pdf

McNiff, J. 2013. *'Action Research: Principles and practice'.* 3rd edition. New York, USA: Routledge Publications.

Microsoft, 2015. *'Tips for creating a strong password'*. Consulted: 29.3.2015:
http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password

Morgan, G., 1979. *'Response to Mintzberg'*. Administrative Science Quarterly, Vol. 24, No. 1. p137-9. Consulted: 19.3.2013. http://www.jstor.org/stable/i353064

Myers, M. D., 2013. *'Qualitative Research in Business and Management'*. 2nd edition. London, UK: SAGE Publications Ltd.

Nisamest, 2013. *'Tuotteet – Ventus Software'.* Consulted: 09.07.2013:
http://www.nisamest.fi/tuotteet/

NIST, 2010a. *'Guide for Assessing the Security Controls in Federal Information Systems and Organisations'*. NIST Special Publication 800-53A, Revision 3. Consulted: 3.2.2013.
http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

NIST, 2010b. *'Guide for Applying the Risk Management Framework to Federal Information Systems'*. NIST Special Publication 800-37, Revision 1. Consulted: 23.03.2015
http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

NIST, 2011. *'Guide for Conducting Risk Assessments'.* NIST Special Publication 800-30, Revision 1. Consulted: 17.2.2014
http://www.nist.gov/customcf/get_pdf.cfm?pub_id=912091

NIST, 2013a. 'NIST - *Information Technology Laboratory – Computer Security Division'.* Consulted: 4.10.2013. http://www.nist.gov/itl/csd/

NIST, 2013b. *'Security and Privacy Controls for Federal Information Systems and Organisations'*. NIST Special Publication 800-53, Revision 4. Consulted: 24.2.2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Opengroup, 2006. *'Welcome to TOGAF – The Open Group Architecture Framework – Introduction'*. Consulted: 18.9.2014
http://pubs.opengroup.org/architecture/togaf8-doc/arch/

Panda, P. 2009 *'ISACA Journal, Volume 4 – The OCTAVE Approach to Information Security Risk Assessment'*. Consulted: 24.9.2014.
http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Documents/jpdf094-the-OCTAVE.pdf

PMI, 2013. *'PMBOK Guide – Fifth Edition'*. Consulted: 18.9.2014.
http://www.pmi.org/PMBOK-Guide-and-Standards/pmbok-guide.aspx

Praxion, 2013. *'AS9100C 2009 – A Plain English Introduction'*. Consulted: 15.11.2013.
http://www.praxiom.com/as9100-intro.htm

PRI-Network, 2013a. *'PRI Performance Review Institute – Nadcap – About Nadcap'*. Consulted: 7.5.2014. http://www.pri-network.org/nadcap/about-nadcap/

PRI-Network, 2013b. *'PRI Performance Review Institute – Nadcap – Accreditaion – Scope of Accreditation'*. Consulted: 9.5.2014. http://www.pri-network.org/nadcap/accreditation/

Radmanesh, S., Tavakoli, A., Nakhaei, Sh. 2013. *'A comparative and assessment study of the role of Information Technology in SPGC'*, Proceedings of 23rd International Business Conference. p1. Consulted 3.2.2013. http://www.wbiworldconpro.com/uploads/melbourne-conference-2013-november/management/1384595541_407-Sima.pdf

Raggad, Bel G., 2010. *'Information Security Management: Concepts and Practice'*. 1st edition. Boca Raton, USA: CRC Press.

Rajasekar, S., 2013. *'Research Methodology'*. Consulted: 23.4.2013. http://arxiv.org/pdf/physics/0601009.pdf

Raywood, D., 2010. 'Implementing ISO27001 in the real world'. Consulted: 06.06.2013 http://www.scmagazineuk.com/implementing-iso27001-in-the-real-world/article/167815/

Roots Infocomm, 2011. *'ERP Solutions – Enterprise Resource Planning (ERP)'*. Consulted: 28.7.2013. http://www.rootsitservices.com/CustomPages/erpsolutions.aspx

SAE, 2009. *'Quality Management Systems – Requirements for Aviation, Space, and Defence Organisations'.* SAE Aerospace Standard, Revision C. SAE International Group, USA

SAE, 2010. *'Quality Management Systems – Audit Requirements for Aviation, Space, and Defence Organisations'.* SAE Aerospace Standard, Revision D. SAE International Group, USA

SAE, 2014a. *'About SAE International'*. Consulted: 14.2.2014. http://www.sae.org/about/

SAE, 2014b. *'IAQG – Organisation'*. Consulted: 15.2.2014. http://www.sae.org/iaqg/

SAE, 2014c. *'Quality Management Systems - Requirements for Aviation, Space and Defense Organisations'.* Consulted 18.2.2014. http://standards.sae.org/as9100c/

SEI, 2007. *'Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process'*. Software Engineering Institute Technical Report. Consulted: 22.3.2014. http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

SGS, 2013a. *'Industrial Manufacturing - JISQ 9100, AS 9100, EN 9100 - Quality Management Systems For The Aerospace Industry'.* Consulted: 12.2.2014. http://www.sgs.com/en/Industrial-Manufacturing/Services-Related-to-Suppliers/JISQ-9100-AS-9100-EN-9100-Quality-Management-Systems-for-Aerospace-Industry.aspx

SGS, 2013b. *'SGS: Aerospace Quality Management Systems – Audit, Certification & Training Services'.* Consulted: 13.2.2014. http://www.sgs.com/~/media/Global/Documents/Brochures/SGS_SSC_NG2_AEROSPACE_web_LR.pdf

Shostack, A., 2014. *'Threat Modeling – Designing for Security'.* 1st edition. Indiana, USA: John Wiley & Sons, Inc.

Shuttleworth, M., 2014. *'Case Study Research Design'* Consulted: 16.5.2013. https://explorable.com/case-study-research-design

SRI Quality System Registrar, 2013. *'Standards – AS/EN/JISQ 9100/9120 Aerospace Quality Management Standard'*. Consulted: 12.3.2014. http://www.sriregistrar.com/A55AEB/sricorporateweb.nsf/layoutC/6518B3E456F624CD8525703B0051D029?Opendocument&key=Standards

Stake, R. E., 1995. *'The Art of Case Study Research'* 1st edition. Washington DC, USA: SAGE Publications, Inc.

Tarantino, A., 2008. *'The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices'*. 1st edition. New Jersey, USA: John Wiley & Sons, Inc.

Tewari, A., 2013. *' A Comparison between ISO 27005, OCTAVE and NIST SP 800-30'.* Consulted: 4.2.2014. http://blog.sisainfosec.com/2014/07/comparison-between-iso-27005-octave.html

Turban, E., Sharda, R., Delen, D., and King, D., 2011. *'Business Intelligence, A Managerial Approach'.* 2nd edition. New Jersey, USA: Prentice Hall.

Wilson, E., 2013. *' School-based Research – A guide for education students'.* 2nd edition. London, UK: SAGE Publications Ltd.

Windows Security, 2015. *'Secure Socket Tunneling Protocol'*. Consulted: 30.3.2015: http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/Secure-Socket-Tunneling-Protocol.html

Yin, R. K., 2014 *'Case Study Research Design and Methods*'. 5th edition. Washington DC, USA: SAGE Publications, Inc.

APPENDICES

The content featured in the appendices will not be published since it discusses information which is confidential and under a Non-Disclosure Agreement (NDA).