An exploratory study of Information Security Auditing

A Master (minor) thesis presented by
Ritu Lakshmi K.R
727182

Supervised by

Dr. Atif Ahmad
Dr. Sean Maynard

The Department of Computing and Information Systems
in fulfilment of
50 pts Major Research Project
(ISYS90063, ISYS90065)

The University of Melbourne
Melbourne, Australia
31 October 2016
Abstract

Management of Information security in organizations is a form of risk management where threats to information assets are managed by implementing various controls. An important task in this cycle of Information Security risk management is Audit, whose function is to provide assurance to organizations that their security controls are indeed working as intended. Numerous frameworks and guidelines are available for auditing Information security. However, there is scant empirical evidence for the process followed in practice.

This research explores how security audits are conducted in practice. In order to do so, a qualitative study is conducted where 11 auditors are interviewed. The findings indicate a gap between what is expected of audit and what actually happens in practice. On exploring the Accounting roots of audit, we postulate that this gap is due to the differences in conceptualization of risk between the Accounting and Information Security discipline.
Declaration

I certify that –

(i) This thesis does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any university; and that to the best of my knowledge and belief it does not contain any material previously published or written by another person where due reference is not made in the text.

(ii) I have received clearance for this research from the University’s Ethics Committee (1647141.1) and have submitted all required data to the Department.

(iii) The thesis is fewer than 14000 words in length (excluding text in images, table, bibliographies and appendices).

Ritu Lakshmi K.R

31 October 2016
Contents

Introduction ........................................................................................................................................... 7

1.1 Research Question ............................................................................................................................ 7

Research methodology ............................................................................................................................. 9

Theoretical Background .......................................................................................................................... 11

3.1 History of Auditing ........................................................................................................................... 11

3.2 Information Systems, Computer Security and Audit ................................................................. 12

Wave 1 – Technical ............................................................................................................................... 13

Wave 2 - Managerial ............................................................................................................................. 13

Wave 3 – Institutionalization ................................................................................................................ 14

Wave 4 - Governance ............................................................................................................................ 14

Wave 5 - Cyber security ......................................................................................................................... 15

3.3 Scope and role of Information Security Auditing ........................................................................... 16

3.4 Risk based approach to Security .................................................................................................... 17

3.5 Holistic view of Information Security Auditing ............................................................................. 19

Data Collection & Results ..................................................................................................................... 20

4.1 Data Collection ............................................................................................................................... 20

4.2 Participant Demography .................................................................................................................. 23

4.3 Audit in the context of Information Security & Assurance ............................................................. 24

4.4 Purpose and scope of an audit ......................................................................................................... 25

4.5 Audit Process .................................................................................................................................. 27

4.5.1 High-Level, Business-Centric Risk Assessment .......................................................................... 28

4.5.2 Scoping ....................................................................................................................................... 28

4.5.3 Understanding risk and control environment ............................................................................. 29

4.5.4 Evaluating control effectiveness ............................................................................................... 30

Discussion .............................................................................................................................................. 33

5.1 Roles of Information Security Auditing .......................................................................................... 33

5.2 Information Security and Audit ...................................................................................................... 34

5.3 The Audit Process ............................................................................................................................ 35

5.4 Information Security perspective vs Accounting perspective of audits ........................................ 37

Conclusion .............................................................................................................................................. 39

References ............................................................................................................................................... 41

Appendices ............................................................................................................................................ 47

Appendix 1: Comparison of Computer Security, Information Security and Information Assurance (Cherdantseva & Hilton, 2014) ................................................................................................. 47

Appendix 2: Comparison of the properties of Information Security and Information Assurance (Ezingeard, McFadzean & Birchall, 2005) .......................................................................... 48
List of Tables

Table 1 Evolution of Information Security Auditing mapped onto a 2-D matrix ........................................... 19
Table 2 Themes identified from literature ......................................................................................................... 21
Table 3 Themes identified from interview data .................................................................................................. 21
Table 4 Building relationship between level 1 and level 2 themes ................................................................. 22
Table 5 Detailed Participant Demography ....................................................................................................... 23
Table 6 IT audit mapped onto the 2-D matrix .................................................................................................... 35
List of Figures

Figure 1 Three Lines of Defense Model - IIA Position Paper (2013) ......................................................... 18
Figure 2 Information Security Auditing process .......................................................................................... 27
Chapter 1

Introduction

Information Security is a form of Enterprise Risk Management where threats to information assets are managed by implementing appropriate controls (Ahmad et al., 2014; Webb et al., 2014). An important task in this cycle of Information Security Risk Management is audit, whose function is to provide assurance over security-related controls. Assurance is defined, in this context, as a state in which the “security is sound and the system provides trust and confidence in the organisation’s security and privacy practices” (Spears, Barki & Barton, 2013). Information Security can thus be viewed as “a well-informed sense of assurance that information risks and controls are in balance” (Anderson, 2003).

The origin of auditing as a discipline can be traced to the individual and societal need for reassurance about the conduct or performance of others in which they held a vested interest (Flint, 1988). Although auditing was an instrument of fraud detection, it has undergone radical changes into becoming a vital part of corporate governance (Lee & Azham, 2008). The use of computer systems to process financial information introduced issues of security and was instrumental in expanding the professional jurisdiction of the Audit Function to include Information Security. Information Security Auditing was detached from traditional auditing, necessitating changes in the kind of skills required to conduct them (Lientz & Weiss, 1977; Beatson, 1986).

Auditing is a practice-based discipline (Mautz & Sharaf, 1961). The emergence and growth of security auditing has been organic in nature, responding to the increasing scope and importance of Information Security. Therefore, a considerable amount of literature relating to security auditing is available in the form of “best-practices”, laid out as standards (E.g. COBIT, NIST, ISO27001 etc.) or frameworks for assessment of security (E.g. Wiant, 2005; Viega, & Eloff, 2010; Viega, Martins & Eloff, 2008; Eloff & von Solms, 2000). However, there is a lack of adequate exploration of the process of audit and the associated techniques from an Information Security perspective.

1.1 Research Question

The primary responsibility of the Audit function is to evaluate the effectiveness of Information Security controls (Moeller, 2010). Rahimian, Bajaj and Bradley (2016) argue that in practice, the assessment of Information Security is a simple checklist-based approach which checks only for the existence and functionality of controls. However, as Siponen and Willison (2009) contend, the mere existence of controls is not indicative of effective security. Therefore, it is crucial to understand the process of audit in order to derive conclusions about the efficacy of the audit process in providing substantial assurance. Furthermore, lapses in Information Security can have far reaching
consequences that go beyond monetary damage (Sinanaj, 2015; Acquisti, Friedman, & Telang, 2006; Goel & Shawky, 2009; Alper & Qing, 2011). The Audit Function holds a unique position of independence and objectivity within the cycle of Information Security Management. It can be thought of as being the last line of defence. Thus, it follows that understanding how auditing is done in practice can provide insights into how the Audit Function can be leveraged to strengthen Information Security. Therefore, this research poses the following question – “How do auditors conduct Information Security audits?”

This thesis, in pursuit of this question, applies both Accounting and Information Security perspectives throughout. This is done for two reasons. First, the scant exploration of audit processes within Information Security literature has necessitated the use of Accounting literature to construct a holistic picture of security auditing. Second, as audit is a practice-based discipline, exploring its historical evolution from Accounting is conducive to understanding the way it functions today.

This thesis begins with an exploration of the history of auditing and its metamorphosis into contemporary security auditing. A holistic picture of the scope and role of audit is constructed from existing Accounting and Information Security literature. A qualitative study is conducted where several auditors are interviewed in order to understand how Information Security audits occur in practice. Based on the findings, a process model of security auditing is constructed. The thesis concludes by highlighting a gap between what is expected of auditors and what happens in practice.
Chapter 2

Research methodology
Identifying the epistemological underpinnings of the research question allows the researcher to be cognizant of the approaches and methodologies available in order to pursue the answer. Based on the set of guidelines provided by Ryan (2006), this research takes on a post-positivist stance. This research attempts to document the process of auditing from a higher level of abstraction and takes on a learning role in doing so. However the researcher acknowledges that auditing takes place in the real world and codifying the process involves understanding what people are trying to communicate – thoughts, feelings and perceptions. This necessitates an interpretive view as well. The research follows Husserl’s descriptive phenomenology as described by Smith et al., (2009) which calls for a generic description of a phenomenon without a deeper investigation into the nuances of influence exerted on the phenomenon by external factors. This means that human experiences may be objectivized to a certain degree.

The use of qualitative paradigm for this research was influenced by the decision to allow the study of the phenomenon of auditing within its contextual richness (Corbin & Strauss, 2008, Galliers, 1992a). This research uses qualitative interviewing as the tool of choice to gather data. The guidelines for conducting interviews proposed by Myers and Neuman (2007) have been followed. The research question is supported by some theoretical background which makes the use of a semi-structured interview format a natural choice. Questions are drawn from theory and the participants are asked to explain what is carried out in practice. This format of interviewing allows the researcher control of the interview while countenancing for flexibility in extracting information.

Sampling for this research was judgmental (Fogelman & Comber, 2002). Participants included all those who engaged in auditing Information Security as a part of their job and possessed more than five years of experience. Although this role may be performed by people with differing titles such as internal auditor, external auditor and consultant, for the purposes of this research, the roles are indistinguishable. To ensure a well-rounded sample, participants with different titles were recruited. Based on suggestions by Denzin and Lincoln (1994) and Crabtree and Miller (1999) for phenomenological studies, a sample size of 7 - 10 participants was initially decided. The researcher was able to obtain 11 participants who were mostly from Banks and Consulting Firms. A detailed description of the participant demography can be seen in section 4.2. Approval was obtained from the ethics committee prior to conducting interviews. The associated application ID is 1647141.1.
A common criticism of qualitative interviewing is that it is inherently subjective. The researcher is cognizant of the situation and plans to utilize suggested reflexive practices such as consultation with professors and memo writing (Cutcliffe, 2003). The research does not include any form of participant observation and relies on self-reported procedures followed. The researcher intended to seek out alternate sources of information such as documentation of the process, if codified, from the participants in order to increase the reliability of the research (Yin, 1994). However the participants declined to share it with the researcher due to issues of confidentiality.
Chapter 3

Theoretical Background
Security auditing is a practice-based discipline and its development has been organic in nature. Thus, in order to build an understanding of contemporary security auditing, we must explore its evolution from a historical perspective. Information Security Auditing can be understood as the process of evaluation of security controls leading to an informed conclusion regarding its effectiveness in reducing security risks. The field of audit first began in Accounting and was intended to provide assurance over financial matters. The concept of Data Security emerged from the use of information systems within organisations and primarily dealt with the manipulation or destruction of financial information by human and non-human perpetrators.

As security audits are historically linked to Accounting audits, a brief cross section of the history of Accounting auditing is provided in section 3.1. In section 3.2, the emergence of Data Security and it’s metamorphosis into Information Security is discussed. Sections 3.3 and 3.4 review Information Security literature in order to build an understanding of the meaning, role and purpose of contemporary security auditing. A holistic view of security auditing based on its historical development is provided in section 3.5.

3.1 History of Auditing
The development of Auditing can be attributed to the individual and societal need for reassurance about the conduct or performance of others in which they held a vested interest (Flint, 1988). Lee & Azham (2008), in their analysis of the evolution of audits, concluded that before mid-1800s the main purpose of an audit was to detect financial fraud. The emergence of capital markets increased demand from investors to monitor productive employment of their investment (Edwards, Anderson & Matthews, 1997). This, in conjunction with the passage of the Registered Companies Act of 1862, expanded the role of audit as a watchdog of corporate governance thus contributing to the efficient functioning of capital markets (Lee & Azham, 2008; Watts & Zimmerman, 1983).

The growth of Corporations post 1930s in the US resulted in the separation of ownership and management. This caused a shift in audit focus from fraud detection to being a seal of credibility for the shareholders (Porter et al, 2005). This meant that although fraud detection was part of the auditor’s responsibility, the main goal of an audit was to assess the truth and fairness of an organisation’s financial statements to ensure flow of funds from the investors. The increase in the volume of business transactions during this period triggered the emergence of sampling techniques and the concept of material assessments in auditing (Lee & Azham, 2008).
The introduction of technology into organisations increased auditor reliance on internal controls and lead to the emergence of risk-based audits (Turley & Cooper, 1991). This meant that auditors would focus their assessments on areas that were more prone to errors and as a result had to build their understanding of the client’s organisation, industry and policies (Porter et al., 2005). Auditing of financial information on computer systems was referred to as an EDP (Electronic Data Processing) audit (Carlin & Gallegos, 2007). Auditors assessed computer programs for accuracy of processing and individual transactions were sampled to derive a holistic assessment. The use of commercial financial systems meant that auditors no longer had to assess the correctness of programs but rather focused on establishing the reliability of controls in producing verifiably accurate financial data.

Present-day auditing follows a Business-Risk approach (Porter et al., 2005). This implies that business-risks to an organisation are expected to incur material costs to financial statements. This paradigm of auditing is also known as Strategic Systems Auditing (SSA). It is a top-down approach as opposed to being transaction-oriented. The role of auditor’s knowledge of the auditee industry and business is emphasized as having a strong influence on audit quality and judgement (Peecher, Schwartz & Solomon, 2007).

3.2 Information Systems, Computer Security and Audit

The use of computer systems to process financial data introduced the concept of computer crime or computer abuse where users with access could manipulate data or users without access could hack their way into the systems (Chrysler, 1987; Fordyce, 1982). It is at this juncture that we see a call for Data Security to be a part of the audit repertoire. Security mainly dealt with preventing manipulation or destruction of financial data within information systems. Security consisted of aspects of physical security, access control, disaster recovery, business continuity and software security where access to software libraries was heavily controlled (Fordyce, 1982).

An understanding of the development of Information Security auditing can be built based on the progression of the field of Information Security. In order to do so, this thesis adopts the categorization of Information Security into five distinct “waves” as put forth by Von Solms (2010). Each wave possesses distinct features and builds on top of one another to provide an understanding of security that we currently possess.
Wave 1 – Technical
Security in the first wave was primarily a technical problem (Von Solms, 2000; Von Solms, 2006; Von Solms, 2010). Security was understood in terms such as Computer Crime, Computer Abuse or Data Security. Security-related controls consisted of physical security such as locks for computer terminals, user authentication, contingency planning and program security (IBM, 1970; Enger & Howerton, 1980; Fordyce, 1982). Security-related aspects of auditing involved evaluating physical security and technical evaluation of the applications, operating systems and technical environment (Beatson, 1986). Auditing was transactional in nature and was performed by financial auditors with specialized training in technology (Lientz & Weiss, 1977) or personnel proficient in technology with a tertiary degree in Accounting (Beatson, 1986). Such audits were known as EDP (Electronic Data Processing) audits and were focused on protection of financial information. The use of distributed computing brought in its own set of audit challenges in terms of network related security (Toppen, 1984).

Wave 2 - Managerial
Enhanced computer literacy, percolation of PCs and the internet created more vulnerabilities and introduced newer security threats such as viruses (Wilkes, 1990). As the effects of security breaches became more public, security entered the boardroom and had garnered management’s attention. This lead to the creation of independent security departments in organisations (Von Solms, 2000; Osborne, 1998). Security Policies began to set the direction for security. We can observe the emergence of Information Systems (IS) or Information Technology (IT) auditors with technical expertise. The IS/IT audits were still financially focused, but had a much broader scope than the typical EDP audit. Their audits ranged from general IT controls to IT security to effective utilization of IT resources (Raval & Gupta, 1998; Hermanson, Hill & Ivancevich, 2000). Technology was viewed as a tool for achieving organisational efficiency and thus IS/IT auditors were focused on cost-efficient use of IT and security was a matter of compliance with the policies. This interpretation is consistent with all the auditing frameworks & standards that came about during this time (Hermanson, Hill, & Ivancevich, 2000).

The availability of commercial certified security products meant that organisations could now purchase and plug them into their technical environment (Eloff & Von Solms, 2000). As a result, audits involved analysing the rationale behind the selection and implementation of security products. Effectiveness of the IT security was measured in the number of potential breaches identified and investigated (Osborne, 1998).
Wave 3 – Institutionalization
The growing importance and need for security resulted in the institutionalization of security in terms of standards, certifications and metrics (Von Solms, 2006). Information Security followed a “Best-Practice” approach. People were recognized as active participants in security and there was a general awareness about the security culture. Various standards for Information Security like ISO/IEC 17799, BS7799 and COBIT (Lainhart, 2000; Trcek, 2003) were developed. Security audits were geared towards compliance with these standards. Audits involved traditional aspects of security as well as an assessment of security culture (Stanton et al., 2005). Security audits were conducted for various purposes. Compliance and certification audits served to increase trust in customers or vendors, especially in the case of ecommerce (Von Solms, 2001). Audits helped “manage” Information Security by providing feedback on the effectiveness of security efforts (Von Solms, 2001). Audit in itself was considered as a deterrence tool for insider threat (Theoharidou et al., 2005).

Although security audits were fixated on financial information, we can observe the expansion of its scope to include all business sensitive information. Information Security was detached from Computer Security – the former involving aspects of security culture and awareness around business-sensitive data and the latter focusing on technical security. As pointed out by Dhillion and Backhouse (2000), security in the new millennium would not be limited to protection of data but extend into the organisational context in which it was interpreted and used. Thus, security was turned into an issue of trust and ethics. However, audit was deemed unresponsive to the evolving threat landscape and lacking in measures to test the vulnerabilities inherent in the system (Jones, 1997). This lead to the development of Penetration tests, which are simulated attacks on a system designed to expose system vulnerabilities (Pfleeger, Pfleeger & Theofanos, 1989). The use of penetration tests served as an effective tool to aid security audits.

Wave 4 - Governance
The collapse of Enron and the ensuing legal and regulatory developments led to the inclusion of Information Security as an aspect of corporate governance (Von Solms, 2006). Information Security began to be handled as an Enterprise Risk Management process (Ahmad et al., 2014; Webb et al., 2014). Arena, Arnaboldi and Azzone (2010), in discussing the organisational aspects of risk management, bring attention to the increase in the professional jurisdiction of the Internal Audit Function into Enterprise Risk Management. The passage of Sarbanes-Oxley (SOX) regulations can be credited with the expansion of the scope of auditing to evaluate risk governance in addition to effectiveness of controls. An articulation of this increased scope of audit can be found in the Three Lines of Defence model put forth by the IIA (2013).
Siponen and Willison (2009) indicate in their seminal paper that following standards does not necessarily mean achieving effective security as standards are generic and not empirically validated which may lead to a false sense of security. In order to be able to obtain a realistic assessment of security, metrics began to be used for tracking risk levels. An example of this increased demand from audit can be seen in Steinbart et al., (2012) where they argue that audits must indicate the “actual level of end user compliance with policies”. Research around developing measurement instruments to assess the effectiveness of controls can also be found (E.g. Wiant, 2005; Viega, & Eloff, 2010; Viega, Martins & Eloff, 2008; Eloff & von Solms, 2000). A separation between the management of compliance from the operational aspects of Information Security can also be seen as indicated by Von Solms (2005). Compliance was focused on certification and was performed by external auditors (Von Solms, 2005). In contrast, internal auditors focused on highlighting areas of risk. Concomitant with the inclusion of security into corporate governance, it was observed that although disclosure of Information Security activities by organisations was not mandated by SOX, voluntary disclosures were found to have a positive impact on share value (Gordon et al., 2006).

Wave 5 - Cyber security
This phase of Information security, which started almost in parallel to the previous phase, is focused around the end-user as the weakest link in security (Von Solms, 2010). This meant that end-users were not only being subjected to social engineering attacks but also behaved as conduits for Information leakage. Human behaviour formed the weakest link of Information Security. In response, auditing increased scrutiny on behavioural assessments of security. Organisations such as the Information Security Forum and the Organisation for Economic Cooperation and Developments have provided guidance for auditors in assessing the Security Culture (Da Viega & Eloff, 2010). Auditors were expected to help highlight deficiencies in actual behaviour (Kruger & Kearney, 2006).

We can also observe the emergence of the concept of Information Assurance. Information Assurance can be defined as “the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users” (Cherdantseva & Hilton, 2014). Although Information Security and Information Assurance have been used interchangeably, the latter can be considered to be broader in scope than Information Security and is driven by business needs as opposed to security needs of the organisation (Ahmad & Maynard, 2014). Its scope is the protection of business as a whole and not just Information and associated systems (Ezingeard, McFadzean, & Birchall, 2005; Cherdantseva & Hilton, 2014). It is not constrained to the concepts of CIA (confidentiality, integrity and availability) but introduces authentication and non-repudiation to form the Five Pillars of Assurance. This view of security expanded the scope of audit to include all forms of information exchange (E.g. Paper, verbal etc.) (Ahmad & Ruighaver, 2004). Ezingeard, McFadzean, & Birchall (2005) argued that assurance is
more about enabling and building resilience in an organisation as opposed to a preventative approach taken by Information Security. Further differentiation between Information Security and Information Assurance can be found in Appendix 1 and Appendix 2.

3.3 Scope and role of Information Security Auditing

We can conclude from the preceding sections that Security Auditing has evolved in response to the societal demand, which is consistent with the views put forth by Brown (as cited in Lee & Azham, 2008). The scope and role of audit has expanded parallel to the growth of Information Security.

There is no standard definition of what constitutes a security audit. Dhillion (2001) believes that that the primary role of an Internal Audit is to assess weaknesses with the design of the internal controls. Activities of the Internal Audit department are prioritized based on a risk analysis. Von Solms (2005) on the other hand argues that the focus of Internal Audit is to identify areas of risk whereas that of the external audit is to report on compliance. Internal audit is responsible for ensuring that “effective Information Security is established, implemented, monitored and reviewed, maintained and updated as a continual cycle of continual improvement process” (Humphreys, 2008). This indicates a holistic approach to the evaluation of Information Security. Moeller (2010) identifies evaluating Information Security effectiveness as the primary responsibility of the Audit function. Spremić (2013) contends that Information System audits – both internal and external, help detect the level of compliance with standards, detect priority risk areas, measure efficiency of controls as well as track levels of risk. They also help organisation to improve their IT risk management practices and forensic readiness (Elyas et al., 2015; Elyas et al., 2014; Ahmad, 2002). IT audits are responsible for identifying material weaknesses in controls surrounding financial information and are thus mandated by Public Company Accounting Oversight Board (PCAOB) Audit Standard 5 (Steinbart et al., 2016). Herath & Herath (2014) argued that IT security auditing provides assurance that the systems are secure, adequately controlled and functioning as intended. Overall, security audits perform these various roles by evaluating the effectiveness of security controls within organisations.


a. Risk Management perspective – Blakley et al. (2002) argue that the application of technology to information creates risks and thus Information Security must be viewed as a Risk Management discipline. In this situation, the purpose of information Security controls is to reduce risks to acceptable levels. Effectiveness is thus defined as the ability of a control in reducing risk level.

b. Economic perspective – Using the economic approach suggested by Gordon and Loeb (2002) the motivation for organisations to implement security controls can lie in achieving a
positive return on investment (ROI) on their security investments. Thus, if a control provides positive ROI, it is deemed effective. Another perspective of measuring effectiveness is in terms of “dollar loss” as suggested by Blakley (2002). He argues that monetizing Information Security, i.e. quantifying it in terms of dollar losses is a way of solving the lack of measures around effectiveness of security controls. He views the acceptance of economic liability by a product vendor as evidence of the “effectiveness” of the product. Thus from this standpoint, effectiveness can be viewed as the ability of a control to minimize potential dollar loss.

c. Legal perspective – Security controls must also fulfil legal obligations. The implementation of these regulations in itself is expected to provide robust security (Lobree, 2002). Thus, effectiveness in this situation is the ability of a control to assist organisations in fulfilling legal requirements.

d. Cultural perspective – Multiple studies have highlighted the importance of the human element in effective Information Security. Thus, if a control is able to aid in creating good security culture, i.e. promote good security behaviours, it is said to be effective.

3.4 Risk based approach to Security
A recurring theme throughout the evolution described in section 3.2 is the risk-based approach to security. Risks initially were system-centric i.e. the subject of protection were computers. The focus then shifted towards the protection of information. This means that Information Security deals with business risks to information. Information Security can be broadly categorized as follows (NIST, 2012; Moeller, 2011; Spears & Barki, 2010; COBIT etc.)

a. Risk Assessment – This process entails a detailed analysis of threats and vulnerabilities in conjunction with the likelihood of threat occurrence and its impact on the organisation culminating in a Risk register. This register prioritizes risks and articulates the risk appetite of the organisation. Risk Assessment ensures that only the controls that are relevant to the security needs of the organisations are implemented (Shedden et al., 2010a; Shedden et al., 2016; Shedden et al., 2010b).

b. Risk Response – Based on the threat priority, impact, risk appetite and budget, organisations make decisions on how to tackle each risk. Responses include risk acceptance, risk avoidance, risk transference and risk control. (Ahmad et al., 2012; Ahmad et al., 2015 Landoll, 2006).

c. Monitor Risk – In this phase, organisations verify that the planned security controls are implemented, functional and satisfy appropriate regulatory guidelines. Effectiveness of implemented controls is evaluated in addition to identifying changes that impact the existing control environment.
This cycle of Information Security can also be understood from the perspective of the Three Lines of Defence model put forth by the Institute of Internal Auditors (IIA, 2013). The model offers a holistic approach to Risk Management by way of clear delineation of roles and responsibilities. It identifies three groups of individuals or “lines of defence”, each responsible for contributing to different stages of risk management. The first line of defence consists of the Business Owners who are involved in the operational management of risks. This implies that they are responsible for identifying risks, assessing them and implementing appropriate controls to mitigate those risks. They are also responsible for the day-to-day operation of controls. The second line of defence is comprised of Risk and Compliance Managers. They are responsible for assisting management in developing processes and controls for Risk Management. They oversee the risk assessment and implementation of controls by the operational management. The third line of defence consists of Audit. Its responsibility is to provide objective, independent assurance over risk governance, management and control operation.

<table>
<thead>
<tr>
<th>FIRST LINE OF DEFENSE</th>
<th>SECOND LINE OF DEFENSE</th>
<th>THIRD LINE OF DEFENSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Owners/Managers</td>
<td>Risk Control and Compliance</td>
<td>Risk Assurance</td>
</tr>
<tr>
<td>• operating management</td>
<td>• limited independence</td>
<td>• internal audit</td>
</tr>
<tr>
<td></td>
<td>• reports primarily to management</td>
<td>• greater independence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• reports to governing body</td>
</tr>
</tbody>
</table>

Spears, Barki and Barton (2013) endeavour to provide a theoretical background for the role of assurance in Information Security. They apply Institutional theory and the Capability Maturity model to the process of assurance and argue that unless an organisation’s claim to assurance is backed by maturity in security practices, the assurance is based more on symbolism than effectiveness. Their research indicated that in a regulatory context organisations needed to appear to be following sound security practices. This process encouraged maturity in handling security which in turn resulted in substantive assurance. Thus, they suggest that external evaluators must begin by evaluating the basis of an organisation’s claim for assurance.
3.5 Holistic view of Information Security Auditing

From the evolution of security auditing described in section 3.2, it can be observed that each “wave” of security has added in additional tasks and expectations from audit. Initially, the audits were highly technical in nature. The next wave of Information Security saw developments in security policies which were then institutionalized within standards and regulations. The passage of Sarbanes-Oxley regulations resulted in increased engagement of audit with risk governance and the use of metrics in order to track risk levels. This was followed by a shift in the perception of security – from management of risks to building security capability and resilience. On a parallel front, the type of information to be protected within the scope of Information Security has also expanded. Initially, the focus of audits was mostly the protection of financial data. However, audits have expanded to cover any and all types of organisational communication. This nature and scope of security audits through the five waves can be articulated as a 2-D matrix as shown in Table 1. The rows indicate the evolving roles of audit and the columns indicate the expanding scope of information through the waves.

<table>
<thead>
<tr>
<th>Data/Scope</th>
<th>Financial</th>
<th>Operational Data</th>
<th>Intellectual Property</th>
<th>Organisational Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Evaluation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance to Standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Assurance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1Evolution of Information Security Auditing mapped onto a 2-D matrix
Chapter 4

Data Collection & Results

In section 4.1, data collection and the methodology for analysis of interview data are explained. Participant demography is analysed in section 4.2. Section 4.3, 4.4 and 4.5 explore some of the results of the interviews.

4.1 Data Collection

Data collection for this research was via semi structured interviews with participants. An initial set of questions was designed to obtain details about the auditor’s experience with Information Security and what their view of audit was in the scope of Information Security. This was followed by a discussion of the overall process of auditing. Content saturation was reached after 7 interviews. However it was decided to conduct further interviews in order to obtain more details about different phases within the process. The initial list of questions asked is provided in Appendix 6. However, as the interviews progressed, questions were more focused. Interviews lasted between 20 – 40 minutes participant consent was obtained to audio record them. One participant did not consent to being recorded and thus detailed notes were taken in this case.

Interviews were transcribed and subjected to thematic analysis. The themes were identified in a hybrid approach - thematic analysis was data driven as well as theory-driven as utilized by Fereday and Muir-Cochrane (2006). This form of analysis was chosen as it ensured rigor as well as allowed for themes to emerge from data. The first step of the analysis consisted of reading and re-reading of all the data that was available on the subject as suggested by Rice & Ezzy (1999, p. 258). This was to allow commonly occurring themes to emerge from literature. Search for articles was mostly conducted on google scholar with the following search terms - “information security AND audit”, “security audit”, “information assurance”, “assurance AND security”. Once relevant articles were filtered, themes with respect to auditing were identified as shown in Table 2.
The second step involved the use of deductive thematic analysis on the interview data. The themes that emerged from data are shown in table 3.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>Any type of risk assessment that was done within an audit.</td>
</tr>
<tr>
<td>Scoping</td>
<td>Decisions involving the scope of the audit.</td>
</tr>
<tr>
<td>Design effectiveness</td>
<td>The process of evaluating various aspects of a control in order to reach a judgement of its design. It includes aspects of appropriateness and adequacy.</td>
</tr>
<tr>
<td>Operating effectiveness</td>
<td>Whether the controls operated as per design?</td>
</tr>
<tr>
<td>Auditor Judgement</td>
<td>The influence of auditor’s experience, knowledge or exposure to similar work in making assessments.</td>
</tr>
</tbody>
</table>

The themes identified were corroborated with the supervisors. In the next stage these themes were used as codes and the interview data was manually coded. The following level 2 themes were identified – the codes were found to be describing either the purpose or the process of audit. The next level of analysis involved identifying any relationships between the level 2 themes. The analysis is shown in table 4.
<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Process</td>
<td>Relationship between Purpose and Process.</td>
</tr>
<tr>
<td>Appropriateness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adequacy/Completeness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost effective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functionality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design effectiveness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating effectiveness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditor Judgement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scope</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Highlight areas of Risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk reduction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Improvement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 4 Building relationship between level 1 and level 2 themes.*
4.2 Participant Demography
A total of 11 participants with more than five years of experience in auditing were interviewed from five different organisations. Participants were mostly from Banks and Consulting Firms. Participants were also from different levels of the audit hierarchy - for example, the list of participants included IT Auditors, Audit Managers as well as Directors. All the interviews conducted were from professionals working in Australia. Most participants are CISA qualified in addition to having qualifications in ISO, ITIL and COBIT. It was also observed that most participants have tertiary degrees in either Accounting or Information Technology. Seven of them listed Information Security or Cyber Security as their specialization on LinkedIn. Half the participants had experience in both external and internal auditing. A detailed breakdown of participant demography is shown in Table 5.

<table>
<thead>
<tr>
<th>No.</th>
<th>Current Role</th>
<th>Current Title</th>
<th>Current Organisation</th>
<th>Tertiary Qualification</th>
<th>Audit Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internal Audit</td>
<td>Audit manager, Technology</td>
<td>Bank</td>
<td>Commerce</td>
<td>CISA, COBIT Foundation course, ITIL Foundation certificate</td>
</tr>
<tr>
<td>2</td>
<td>External &amp; Internal Audit</td>
<td>IT Auditor</td>
<td>Consulting Firm</td>
<td>Information Systems</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Internal Audit</td>
<td>Senior Audit Manager</td>
<td>Bank</td>
<td>Accounting</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>External Audit</td>
<td>Manager, Technology Risk &amp; Assurance</td>
<td>Consulting Firm</td>
<td>Information Technology</td>
<td>CISA, CISM, MCSE, CCNA, LA ISO 27001</td>
</tr>
<tr>
<td>5</td>
<td>External Audit</td>
<td>Director</td>
<td>Consulting Firm</td>
<td>Business Administration</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>External Audit</td>
<td>Director - Technology and Controls</td>
<td>Consulting Firm</td>
<td>Accounting</td>
<td>CISA</td>
</tr>
<tr>
<td>7</td>
<td>Internal Audit</td>
<td>Senior Manager, Information and Technology Risk</td>
<td>Bank</td>
<td>Public Administration</td>
<td>CISA, CISM, CIA, ITIL, CGEIT, COBIT 5</td>
</tr>
<tr>
<td>8</td>
<td>Internal Audit</td>
<td>Senior Manager, Enterprise Technology Risk</td>
<td>Bank</td>
<td>Business Systems</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>Internal Audit</td>
<td>Audit Director Technology</td>
<td>Bank</td>
<td>Administration &amp; Management focus on International Business Law</td>
<td>CISSP, CGEIT, CISM, ITIL, CISA</td>
</tr>
<tr>
<td>10</td>
<td>Internal Audit</td>
<td>Senior Security Consultant</td>
<td>Bank</td>
<td>Technology + Business Administration</td>
<td>CISA, CISSP, ISO 27001 Lead Auditor</td>
</tr>
<tr>
<td>11</td>
<td>Internal Auditor</td>
<td>Information Security Manager</td>
<td>ICT Solutions</td>
<td>Information Systems</td>
<td>CISSP, PMP, ISO 27001 Lead Auditor, ITIL, CCSP</td>
</tr>
</tbody>
</table>

Table 5 Detailed Participant Demography
4.3 Audit in the context of Information Security & Assurance

The role of Information Security audit (internal and external) is to provide an independent and objective analysis of an organisation’s security initiatives thereby providing feedback on the effectiveness of Security (Moeller, 2010; Steinbart et al, 2012). Security audits are responsible for dealing with aspects of Risk Management, Control implementation and effectiveness as well as providing assurance over the security within an organisation. Therefore, interviews with the participants began with a discussion of what the role of audit was from an Information Security perspective.

Overall, most participants agreed that audit in a security context involved evaluating effectiveness of security. This process must be done in an independent capacity and in an objective manner. Most participants from the Internal Audit Function highlighted the existence of audit within the Three Lines of Defence. This view can be ascribed to the structuring of audit within their organisation which was based on the Three Lines of Defence model. Participants belonging to the internal audit function seemed to have greater involvement in risk management as they indicated that they not only provided opinions on control effectiveness but also on risk governance. Three participants articulated concepts of Confidentiality, Integrity and Availability of information. There was a general emphasis on the importance of audit to the board and executive levels by both internal and external auditors, especially by those at higher levels in the audit hierarchy. This can be attributed to their frequent interaction with the board to whom the audit reports are generally presented.

In addition to ensuring mitigation of risks, few participants, especially those with more experience, emphasized the importance of evaluating the resilience of the organisation with respect to security. This meant that auditors not only had to make judgements about whether specific risks were mitigated but whether the organisation had the capability to detect and correct security issues. As participant 8 stated, “Looking at the controls which we have implemented within the businesses and pulling it all together. [Do] we have the ability to protect information, detect if it changes and [do] we have the ability to correct [?]. Those are the components that roll up to whether we are secure or whether it’s effective.”

Participant 3 viewed audit as a process detached from compliance. Audit is a feedback mechanism which provides input on the current state of affairs and how it could be improved. This implies that audit provides a “report card” which articulates current problem areas of the organisation. This is indicative of a role of audit that has expanded into the advisory domain. As she articulated – “I think it’s about providing an independent opinion. Not even an opinion, I think an assurance conclusion. It’s about being independent, providing a conclusion whether or not, things are operating as they should be? Are they effective? Are they ways that things can be improved? So it’s not only from a
compliance point of view. It’s about efficiency - how can we do things better? What can we cut out? Cost savings etc. I think it’s from both angles.” However, in contrast to this, participant 4 believed that these evaluations can be called audit only when the process has the authority to mandate changes in the organisation – “You look at the controls and review it but you don’t have the mandated authority to go and say guys, correct it. So the company decides what to do with it. While in internal audit or external audit the client has to fix it, right? So you have that authority.” According to him, other forms of control evaluations fall under advisory work. The Accounting background of the participant may provide an explanation for this view of audit.

Participant 11 on the other hand viewed audit as an organisational process driven primarily by adherence to some requirement - An organisational policy or a standard. This implies that the security risks had already been analysed and articulated in a policy document. An auditor’s role is to ensure that that the policy is being implemented as intended. As he stated, “So you have a documented set of [security] requirements, then you are checking whether what you do in real life actually adheres to what is written down”. Participant 10, who is involved in vendor risk management, believes that the objective of security audits is to highlight areas of risk. When asked what is the output expected of his audit, he answered “Of course, risk. If at all any risk is identified. Our intention is to understand the security posture of the company. If they are secure enough, we are happy, there is nothing to be concerned about.”

4.4 Purpose and scope of an audit
The next set of questions to the participants revolved around the purpose and scope of an audit. From an internal audit perspective, the participants interviewed provided instances of a wide range of audits. For example, participant 11 indicated that internal audit can help prepare organisations for an external audit – “So for you to get the certification you need to have an external auditor, an independent auditor to come and conduct the audit. But before that happens, as an organisation you need to prepare yourself. So that’s where the role of the internal auditor comes in. Making sure all the requirements are being met. So [that] when [the] external auditor comes, it won’t be like ‘Oh, We didn’t know’.” Participant 10, who is involved in vendor risk management, was responsible for identifying risks around the transmission, storage and use of proprietary data within vendor systems.

Participants involved in Internal Audits indicated that audits were usually driven by the prioritized list of risks that the organisation wanted to tackle within the time and budget they had. For example, if there were ten risks identified, based on the priority, budget and time, the organisation could decide that the audit must focus only on the top three risks. Once this was completed and the auditors felt that the risks were being handled well, then those risks were not included as part of the next audit cycle. Thus, internal audits were based mainly on priority and the result of the audits
determined the risks that were to be included in the next audit. For example, as participant 4 said—“If there are five high risks obviously you have to include those in the first year. Then once you audit those areas then you figure out, saying there are controls in place. The residual risk maybe medium or low. So next year you might say, Okay we’ll pick up those two because they are still medium but the low ones we don’t want to worry about. Let’s go to the other medium ones and then you do those. So there is an audit planning process, yearly audit planning process which takes a lot of time.”

Internal audits were conducted all through the year. In contrast, some audits like IT audits are usually mandated and conducted on an annual basis. These audits are more attuned to protecting financial information. When asked about the types of audit, participant 4 said “So that’s external auditing. That’s for financial statements only. While internal auditing is different. So in internal audit, you look at all the internal controls not just financial statements. I think all the operational risks. Including IT, including Information Security, all those sort of things.”

Sometimes the organisation may use audit as a fact-finding exercise. This was the opinion of Participant 3 who was working in internal audit under operational risk. Her team was usually provided with a topic, an area or a business unit and it was up to the team to gather all relevant information like financials, organisational structure, previous history, major events etc. in order to derive a comprehensive set of risks that affected the chosen area. When asked if the internal audit was provided with the scope at the beginning of an audit, she said – “No they don’t. How it works here is we are given a topic, a subject, area or a BU [Business Unit]. And then essentially our processes are we go there and actually build up scope. We start doing interviews, walkthroughs, ascertaining any and all background information we can about that topic or business we are given. For example, if we are auditing home loans. There is a background on it, qualitative and quantitative. Not only the financials, org-structure, previous history, major events or incidents and things like that. You start to do walkthroughs of key processes. From there you identify your risks and controls. And that forms your scope. It’s a fact-finding exercise for the first few weeks, which then forms your scope. It gives you direction that this is exactly what I’m going to be providing assurance over”.

Participant 5 on the other hand, clearly delineated two purposes for audit in an Information Security context – Compliance and Risk Management. When asked what audit means from an Information Security perspective, she answered - “Audit is a way to help manage risks by determining the level of controls. So risk mitigation, risk control is one. The second part of audit, where the focus is on, is actually compliance with specific regulatory requirements.” Risk-based audit is driven by risks to the organisation, whereas a compliance audit follows a simple yes or no approach. The objective of a Risk-Based audit is to evaluate controls in the areas self-assessed by the organisation as high-risk. In contrast, compliance audits are geared towards ensuring that organisations adhere to regulations.
4.5 Audit Process
Next, the participants were asked to describe how audits were conducted. The process of audit described by the participants was found to be fairly similar across all of them. The first step involves understanding the purpose and requirements of an audit. This is followed by a high-level, business-centric risk assessment. This helps determine the scope of the audit. Scoping involves making decisions about the areas, processes, systems or personnel that will be covered by the audit. The auditor then tries to understand the risk and control environment within the organisation. Once the auditor gains an understanding of all the controls within the scope, the control design is assessed. If the design is deemed effective, the operating effectiveness of the controls is determined. This is an assessment of how well the operationalized process adheres to design. The process concludes with the generation of an audit report. This process is described in figure 2.

![Figure 2 Information Security Auditing process](image-url)
4.5.1 High-Level, Business-Centric Risk Assessment
Based on the purpose of an audit, an initial level risk assessment is conducted. The Industry in which the auditee organisation operates offers some input about the inherent risks. In order to refine her/his understanding of the risks, the auditor may select key stakeholders involved in a process in order to conduct further interviews. Auditee organisations may also request auditors to pay attention to certain specific risks. All these contribute to refining the auditor’s understanding of the organization’s risk profile. As participant 5 articulates – “So when we speak to clients, for example their risk is Information Security but the risk statement is around inappropriate access then the audit scope will be very much focused on access controls, segregation of duties and how access is managed.”

In the case of audits focused on compliance, this phase may not be conducted. As indicated earlier, compliance audits follow a yes or a no approach and are not driven by specific risks. As participant 5 articulates - “The compliance is very broad and it is highly aligned with whatever legislative or regulatory requirement they are trying to comply with.” High-level risk assessment may not be conducted in case of IT audit as well. As indicated by participant 6, IT audit is focused on financial information and thus is concerned with the systemic risks that arise out of the use of IT in processing financial information - “IT is IT. It has common risks around access controls, business continuity etc. For example, access [control] is a risk that is standard across the use of IT.” Thus, it can be seen that the purpose of the audit decides whether this phase is conducted.

4.5.2 Scoping
Scoping process is where decisions regarding the business areas, processes, systems and personnel to be covered by the audit are finalized. Determining the scope was deemed as an important process as determining the correct scope ensured that specific risks that applied to that scope could be determined. As participant 1 articulated - “Once we’ve determined the specific scope of that audit then we’ll determine the specific risks as it applies to that scope.”

This stage may also be used by auditors to highlight some of the emerging risks in the industry that they feel ought to be addressed by the auditee. Participant 5 talks about how auditors use internally generated reports regarding emerging security threats in scoping meetings. She goes on to say – “That’s why the scoping is really important. You don’t just want to use some sort of generic industry risks and feel it’s quite not relevant. Because scoping meeting is where we talk about what are some of those risks, threats that are current to that organisation. And then as we progress through the audit we actually have that as a point that we raise in the interview to see how they are managing those types of new threats applicable to their business”.

28
4.5.3 Understanding risk and control environment

This level consists of the auditor building an understanding of the risk and control environment within the scope of the audit. Auditors may be provided with the risk register of the organisation. In case the organisation does not have a risk register, interviews and walkthroughs are conducted with key stakeholders. Participant 5 articulates – “The risk register has the defined risk and it has the associated control. So the risk register gives us an idea of what controls currently exist. If they are a mid-tier or a smaller organisation, visibility over controls only comes only when we interview the client as a part of the scoping exercise. We do have a list of standard controls that we would expect to see. In case they don’t have a formal risk register we will then go through the interview process and ask questions around what actually exists in an organisation.” As indicated in the previous section, Scoping decisions drive the specific risks that apply to the scope of the audit. Conversely, identifying the risk and control environment within the auditee organisation may also influence scoping decisions. Thus, these phases feed information to one another.

Another approach to articulating the risks, particularly in the case of IT audits and IT general control audits is the use of a template of pre-defined risks. This template or a standardized list of risks was the result of an aggregation of the firm’s expertise in auditing and the guidelines provided by various standards. It contained the risks have been observed in the course of the firm’s audit experience over the years. These risks are quite broad in nature to ensure wide applicability and deal with aspects of access control, business continuity, incident management etc. This template could be customized to include certain factors that were unique to the organisation. Participants 2 and 7 indicated the use of this template. Participant 2 stated – “IT general controls audits are carefully performed, standardised and leave little room for going off script as they are very tightly bound and a lot of effort goes into a small(ish) set of controls – we need to be very confident and comfortable that a control is designed and operating up to expectations in order for us to sign off on it as effective.” When asked in detail about how customization occurs, Participant 6 provided an example - In the case of an IT audit, the standardized list of risks may consist of interface risks i.e. risks that arise out of the interfacing between multiple systems. However this risk is not applicable if the auditee organisation is utilizing only one system. The use of this template was found only among external auditors.

Participant 5 and participant 1 spoke about a standard list of controls that they expected to see during an audit. Once an understanding of the risk profile was obtained, there were certain kinds of controls auditors could “expect to see” within that environment. This expectation is determined by auditor’s experience and exposure to similar environments. As participant 1 indicated - “So I guess as auditors you have an idea what controls should be there. In a typical process there should be this kind of check or there should probably be this level of review or this IT control in place. Because you
know this is how it should operate in a sound environment.” Participant 5 indicated that this “master list” of controls was codified whereas according to participant 1, it was more of an auditor expectation and not formally maintained. By the end of this phase, the auditor has a clear idea of the risks and controls that are present in the environment of the auditee organisation within the given scope. The risks identified within this stage are more granular and specific in nature.

4.5.4 Evaluating control effectiveness
On obtaining a comprehensive understanding of the risk and control environment, auditors now evaluate the effectiveness of controls. This is done in two stages - The first stage is assessment of design effectiveness which is followed by an evaluation of the operating effectiveness. Design effectiveness comprises of an assessment of the design of the control in order to ensure that it is able to handle the risks it has been designed for. This also includes a determination of appropriateness of the control for the risk. As participant 1 indicated – “So that’s when you do design assessment to understand in detail how the controls [work]… well understanding the process, understanding what control is in place and then to see whether the control is designed in such a way that meets that risk. If we then decide that actually, you know, the control inherently misses out on aspects of the risk, then it’s designed ineffectively.”

Auditors examine documentation pertaining to the design of the control such as process document, a network or system configuration document in order to make evaluations. As participant 4 said, when asked to explain what design effectiveness entails – “It means you need to explain to us - Is there a documented procedure? Is there a policy that drives this procedure? We review it and then say yep, its meets all industry standards, it has everything done. And then we say ok, go to test of effectiveness.”

Participant 8 indicated that design evaluations are guided by control criteria. This can be obtained from the standards or the audit methodology. Criteria for evaluation of design may consist of qualities such as reliability, repeatability, accountability, traceability and transparency. This implies that the control must be reliable, its associated activities must produce the same results over time, it must have appropriate governance structures around it, any violations must be traceable and all its activities transparent. On asked whether anyone would be able to produce an assessment of the design provided the audit methodology, all participants admitted that although in theory all evaluations must lead to similar outputs, in reality the quality of audit was highly dependent on the experience, exposure and the knowledge of the auditor. Participant 8 contends - “Theoretically, everyone should come out with the same answer. Now that doesn’t necessarily always happen in reality, because it depends on the person’s experience.”
Analysis of the rationale behind the design is also a component of evaluating design. Thus, auditors may also pose questions relating to why a particular design choice was made. Design evaluation was a subjective assessment of the process document – whether the process inherently missed aspects of risk. In the case of technical controls, design evaluations could consist checking the configuration – for example, were the right attributes logged? Participant 9 highlighted the existence of what he called “adopted controls”. These were technical tools, usually purchased from a vendor which were configured without knowledge about its capabilities and limitations. This implied that the rationale behind the use of the tool was fallible and thus constituted a failure in design. This issue was also exacerbated by control design personnel leaving the organisation. In order to ensure that the controls were adequately addressing the risks, both key and non-key (compensation) controls were checked for existence and functionality.

Once the design is deemed to be effective, auditors now measure the operating effectiveness. The assessment of operating effectiveness is heavily driven by sampling methodology. Participant 1 and 9 indicated that the audit methodology was used to determine sampling sizes and approaches. Sampling is a way of deriving statistically relevant samples from a population in order to be able to draw conclusions with a certain degree of certainty. Sampling may be judgemental or random. Once a sample of instances of a process transaction was chosen, evidence pertaining to that is collected. This may be in the form of system logs, screenshots or process walkthroughs. This allows the auditors to compare the operationalized process to its design in order to produce conclusions about operating effectiveness. This implies that auditors checked if the process was working as designed. As participant 5 indicates – “Effectiveness is how well that control has been implemented in practice. Effectiveness can only be determined by sample testing what actually happens on the ground within an organisation.”

Participants 2 and 11, however, indicated the existence of three steps in evaluating effectiveness of controls.

a. What they [auditee] are meant to be doing – This is derived from policy/standard.
b. What they [auditee] say they are doing – This is derived from interviews with key personnel.
c. What they [auditee] actually do – This is derived from sampling and audit logs.

If there was no history of control violation within the samples selected for an appropriate timeframe, then the control was deemed effective. However before making this judgement, auditors had to consider if these controls were sufficient to handle emerging threats that were identified as relevant during scoping. This evaluation was based on the auditor’s experience and how other auditees in the industry have handled that. Thus, most participants stressed the importance of auditor knowledge about the latest threats and industry trends. In case of internal audit, data of
such nature could be circulated amongst similar organisations. Auditors were also expected to network and talk to other professionals to keep abreast of the latest developments. In the case of external auditing, the audit firm was responsible for collecting and maintaining such knowledge base. Auditors questioned personnel regarding the sufficiency of the controls to handle emergent threats. Based on the answers provided, the auditor would reach a conclusion regarding the capability of the control.

Aberrations in the samples (i.e. control violations) usually indicated a failure of operationalization of the process. For example, in a control designed to prevent unauthorized access, deviation may be in the form of a bypass of the processes - someone who is responsible for revoking access privileges has not done so. This is a clear violation of the operationalization of process not its design. Participant 9 believed that, control infractions rarely indicated flaws in design. Operating effectiveness was a method to ensure that auditees were doing “what they say they are doing”.

On completion of the evaluation process, an audit report was presented to the auditee. The report, based on the type of the audit, could contain ratings for each control. Some participants reported conducting an informal discussion on the residual risk. As participant 3 indicated when asked whether residual risk was measured - “You are meant to. It’s an internal thing. We don’t really share that with the stakeholders. We will come together at the end and say, well what do you think the residual risk is?” In contrast, Participant 6 contended that residual risk is included in the report in the form of observations - “It is presented to the client in terms of what we observe and how it impacts the financial information.” Thus, risk levels may or may not be explicitly tracked based on the type and purpose of audit.

Many participants, especially the more experienced, indicated that the maturity of the process of Information Security Management was also symptomatic of effective security within the organisation. They argued that rather than testing controls, audits must begin with an understanding of how Information Security is managed in the organisation – Is a robust framework used for risk assessment? Are there proper governance procedures around security? Is the lifecycle of a control managed effectively? As participant 7 aptly stated, “If the foundations of the building are gone, game over. Why would you go to the 20th floor and look for the plumbing?”
Chapter 5

Discussion

The purpose of this thesis was to investigate how auditors perform Information Security audits. An exploratory study was conducted involving interviews with 11 auditors from Banks and Accounting firms. In addition to gaining a grounded view of the process of audit, some interesting themes emerged during the discussions.

5.1 Roles of Information Security Auditing

Interviews indicated that overall, audit was viewed as a process of evaluating if an organisation demonstrated effective security. Consistent with the various roles of a security audit described in section 3.3, participants stated that an audit could serve the following purposes.

   b. Advise for and evaluate risk governance.
   c. Provide inputs for process improvement.
   d. Highlight areas of Risk.
   e. Provide assurance over security within organisations.
   f. Ensure cost effective use of IT.

However, the extent to which each role was played by audit depended on the purpose and audience of audit. For example, internal auditors included risk governance within their role whereas IT auditors held an assurance view around financial information. The participant involved in vendor risk management contended that the role of an audit lay in highlighting risks whereas the participant within operational risk quoted aspects of operational risk management, process improvement as well as cost effective use of IT.

The Internal Audit Function was found to be more involved in risk management consistent with the literature as outlined in section 3.3. They behaved as feedback mechanisms for security initiatives within the organisation in terms of highlighting issues relating to risk management, process improvement as well as cost efficient use of IT. In alignment with the view put forth by Dhillion (2001), internal audits dealt with a prioritized list of risks. In addition to the above roles, internal auditors also provided support for external auditors by acting a point of contact from within the organisation as well as helped organisations prepare for external audits. Internal audits could also be used as a fact-finding exercise. Thus, internal auditors have more diverse roles and a greater span of operations.
From an external audit perspective, we can clearly delineate two roles of Security Auditing - Compliance and Risk Management. Contrary to Von Solms’ (2005) view that external audits focused on compliance, interview data indicated that external audits can focus on risk if requested by the client. The involvement of external auditing in Risk management may indicate increased demand from the shareholders for higher accountability in terms of Information Security. Escalating security breaches may have necessitated a mandate not just to understand if the organisation is doing the right things but if they are doing things the right way. Additionally, external audits may also be used by the organisations as a starting point of Security Risk Management. This implies that the auditee organisation intends to leverage the experience of the external auditing firm in order to set itself a security baseline. This can also be viewed as a fusion of audit and advisory roles among external auditing firms.

5.2 Information Security and Audit
As seen in section 3.2, IT audits are quite broad in scope ranging from general controls to security (Raval & Gupta, 1998; Hermanson, Hill & Ivancevich, 2000). This was reflected in the tendency of the participants to begin answers with “It depends on the kind of audit”. Although the questions asked pertained solely to Information Security, it was observed that the participants discussed aspects of security from their range of their experience within IT audit. Based on this, it can be argued that although there are different kinds of audits, all of them address some aspects of security. Each kind of audit is responsible for contributing information on different but interrelated facets of Information Security within the organisation. For example, IT Audits reviewed controls around financial information in order to assess integrity and reliability of financial statements. Vendor risk management involved assessing the vendor’s risk posture around proprietary information. Operational Risk audits assessed the reliability of business data against operational risks. Thus, it can be concluded that although security may not be the primary focus, all audits provided input on different aspects of security.

This understanding can be envisioned from the perspective of the 2-D Matrix of audit evolution described in section 3.5. As seen previously, this matrix covers the span of areas pertaining to Information Security within the organisation. Taking the IT security audit conducted by Lo and Marchand (2004) as an example, it can be seen that the following aspects were covered in the security audit – Technical evaluation of ports and networks, system policies and password audit. Although there is no information provided in the case study regarding type of information that was covered, we can assume that financial and operational data were the subject of protection. This can be mapped onto the matrix as shown in table 6.
Although this format is simplistic, it can provide a bird’s eye view of the current audit situation within the organisation. This allows an articulation of the areas and focus of all the audits conducted and can be utilized as a dashboard to drive more focused use of audit resources. Additionally, organisations can also leverage data from audits that have already been conducted.

5.3 The Audit Process
From the process of audit described in section 4.5, it can be concluded each audit is unique and warrants some variations in the process dependent on the purpose and scope of the audit. For example, some audits involved a high-level, business-centric risk assessment whereas other audits such as compliance audits or IT audits did not. Risks may also be derived from a pre-defined template as indicated in Section 4.5.3. The rationale behind the use of this template, as explained by participants, is that most of the risks that arise out of introduction of technology into a business are standard. In other words, these are the systemic risks that can be expected due to the introduction of IT into the business place and are hence standardized. The focus here, as it can be observed, is not on Information Security Risks but rather on IT Risks. This also explains the limited use of these templates – i.e. in the case of IT audits and IT general controls audits which tend to be financially focused.

The use of this template can be thought of as being symptomatic of four issues –

a. It can be argued that there is sufficient knowledge about systemic IT risks in order to be able to standardize them and audit with confidence. This indicates a maturity (or a perception of it) in the understanding of IT risks.

b. It is a movement towards an assurance view of Information Security which does not indulge in a detailed risk assessment but rather views the capability of the organisation to deal with generally identified risks.
c. As indicated in section 4.5.3, IT audits are subject to legal repercussions and are thus heavily standardized in order to allow them to make confident judgements within the bounds of time and budget allocated.

d. It imposes a structure to the risk assessment which could be the result of a functional interpretation of the organization as argued by Dhillon and Backhouse (1996).

Consistent with the theory of substantive assurance put forward by Spears, Barki and Barton (2013), many participants, especially those more experienced, believed that effective security begins with mature security practices. Thus, auditors began evaluation by understanding the maturity of the risk management practices in the organisation. Although auditors did not explicitly track risk levels, at the end of an audit, depending on the type and scope, an informal discussion was conducted on the residual risk. Risk levels are not explicitly tracked unless requested by the client. Many participants also expressed an assurance view of security wherein emphasis was placed not only on mitigating specific security risks but also on ensuring resilience within the organisation concurrent with the observations made by Ezingeard, McFadzean, & Birchall (2005).

The process of control evaluation is guided by control criteria available within the audit methodology and standards. However, despite this, this process was found to be highly subjective. The audit outcome was dependent on the auditor’s experience, expertise and exposure to similar work. Additionally, auditors with experience in advisory roles were expected to generate better insights than “career auditors”. This was also noticed among one of the participants who had years of experience in an advisory capacity, and drew attention to the issue of adopted controls. This raises questions around the extent to which the educational background and experience of the auditor can have implications for audit quality. Most auditors who perform security audits have background in Accounting or Information Technology. This background requirement has been constant throughout the evolution of security auditing as indicated in section 3.2 (Lientz & Weiss, 1977; Beatson, 1986). Security-related knowledge is obtained from experience and additional qualifications such as Certified Information Systems Auditor (CISA), ISO27001 etc.

It must be noted that this method of control evaluation process is not unique to the field of Security audits but is rather borrowed from the Accounting field as a participants indicated. The process of security audit is concomitant with the Strategic Systems Approach followed in Accounting audits as showed by Peecher, Schwartz and Solomon (2007). A major implication of borrowing the evaluation techniques from Accounting is that security audits are susceptible to all its limitations. Some examples include the Halo effect (E.g. Ed & Schultz, 2005) and Auditor Expectation gap (E.g. Fisher & Naylor, 2016). A deeper discussion pursuing this line of inquiry is out of scope of this thesis but forms an interesting avenue for further research.
5.4 Information Security perspective vs Accounting perspective of audits

The main function of a security audit lies in evaluating effectiveness of security-related controls. From an Information Security risk management perspective, a control is deemed effective if it causes a reduction in risk levels by having a positive effect within its operating environment (Hagen, Albrechtsen & Hovden, 2008; Spremić, 2013). For example, Steinbart et al., (2012), argues that auditors must be able to determine the “actual level of user compliance” to security policies. This indicates that auditors are expected to provide an idea of whether the security efforts are working as intended and have thus resulted in a discernible reduction in risk. However, from the interview data, effectiveness is interpreted to mean adherence to design. Auditors pass judgements on the “effectiveness” of controls during the design phase where they evaluate if the control inherently misses aspects of risk. This can be thought of as judgements relating to adequacy – whether the control is adequate to handle the risk. Design effectiveness is about how well the control is designed and how it is expected to work “in theory”. Operating effectiveness, on the other hand, is about how well the control operates as per the design. A control is deemed to be operating effectively if it adheres well to its design. Thus, auditors do not evaluate the effect of that control within its operating environment. The meaning of effectiveness from an Information Security perspective is different from that of the Accounting perspective. This is indicative of a missing link between what the auditors do and what is expected of them from the Information Security literature.

As indicated in section 3.1 traditional auditing involves an assessment of the truth and fairness of an organisation’s financial statements (Lee & Azham, 2008; Porter et al, 2005). The underlying motivation for Accounting audits is to ensure reliability and verifiability of financial information produced by an organisation. The use of sampling, test of details and analytical procedures performed in Accounting audits are geared towards ensuring that the controls can be relied upon and that any transactions that occur can be verified. For example, by sampling transactions, auditors can ensure that the control can be relied upon to produce the same output over time. Thus, effectiveness of controls from a traditional Accounting perspective refers to the ability of a control to produce reliable and verifiable financial accounts. Risk management within Accounting refers to operational risks that have a material impact on financial statements. Thus risks can be viewed as areas that are “prone to errors” in financial reporting. Additionally, effectiveness of internal controls is also tied to the achievement of business objectives (Spira & Page, 2003).
In contrast to this approach, control effectiveness from an Information Security perspective refers to the ability of a control in causing a discernible reduction in security risks. As a result, security auditors must evaluate,

a. How are the Information Security risks being assessed?
b. Are they being assessed correctly?
c. What controls have been selected and why?
d. Do the controls, when in operation, cause reduction in risk levels?

Thus, the expectation of audit from Information Security literature is geared around risk reduction. Additionally, it can be seen that the conceptualization of risk within Accounting is very different from that of risk within Information Security. These two different approaches to auditing impose different meanings of effectiveness.

The findings of the study indicate that security auditing exhibits a mixed approach – it utilizes techniques from both Accounting and Information Security. The use of sampling methodologies and evaluation of design and operating effectiveness are techniques borrowed from Accounting. However, they are more suited to establishing the reliability of Information Security controls rather than establishing that the controls have resulted in a reduction of risk. However, techniques such as evaluation of risk governance and management, understanding the rationale behind implementation of security products, penetration tests etc. follow an Information Security approach to audit as they explicitly track risks. However, Information Security risks are viewed as business risks and treated as such by the Audit Function.
Chapter 6

Conclusion

In order to understand how security auditing is conducted in practice, this research poses the following question – “How do auditors conduct Information Security audits?” In pursuit of this question, a qualitative study was conducted where 11 auditors were interviewed. The findings indicate that auditors conduct security audits in a five-stage process as follows.

a. High-level, Business-centric risk assessment – An initial, high-level risk assessment provides an overview of the risks faced by the auditee organisation.

b. Scoping – Based on the identified risks, the processes, systems and personnel to be audited are decided.

c. Understanding the risk and control environment – Auditors build an understanding of all the risks and controls within the identified scope.

d. Evaluation of design effectiveness – Auditors evaluate the design of the control – Does the control address the risk? Is the design adequate?

e. Evaluation of operating effectiveness – Auditors evaluate the operationalized process against the design. If the controls operate as dictated by the design then they are said to be operating effectively.

The process of audit was found to be subjective in nature, heavily reliant on the auditor’s experience, knowledge and exposure. The findings also indicate that although security may not be the focus of an audit, all audits provide information regarding different aspects of Information Security.

The main contribution of this research is to draw attention to the gap that exists between what is expected of security auditing and what is carried out in practice. In evaluating the effectiveness of security, audits apply an Accounting view of effectiveness which is different to the Information Security view of effectiveness. Exploring the Accounting roots of security auditing has allowed us to postulate that this gap is due to the different conceptualization of risk between the Accounting and Information Security disciplines. Further research is required to determine how this gap can be reduced.
In addition to establishing a need for future research, this thesis also makes the following contributions. From a theoretical perspective, this research

b. Applies a dual perspective – Accounting and Information Security to explore the role of security auditing within practice.
c. Explores Information Security Auditing from a historical perspective to build a holistic understanding of contemporary security auditing.

From a practice-based perspective,

b. Provides an instrument for articulation of the current state of security within organisations.

It must be noted, however, that the outcome of this research is contingent on self-reported procedures followed by the participants. No other sources of data could be obtained due to issues of confidentiality. Additionally, the research is limited to the experiences of 11 participants within Banks and Accounting firms. Both were large organisations and thus the procedures may differ in smaller organisations. The study is also limited to participants based out of Australia and may not necessarily reflect the practices of other countries.

The area of Information Security auditing research is still in its infancy and this study establishes the need for future research in the area. Potential areas of future research include

a. A comprehensive analysis of audit approaches towards security
b. Implications of security auditing following an Accounting approach to audit.
c. Impact of auditing results on Information Security strategy and Investment.
d. Differences between the roles of Internal and external auditors.
e. Application of various theories of Accounting to security auditing.

Auditing aims to provide well-informed assurance over Information Security efforts. Understanding the underlying approach for audit thus provides insights into how the unique position of independence and objectivity occupied by audit can be leveraged to strengthen Information Security.
References


IBM. (1970). CONSIDERATIONS OF DATA SECURITY IN A COMPUTER ENVIRONMENT. *Considerations Of Data Security In A Computer Environment*


Appendices


<table>
<thead>
<tr>
<th>Discipline Characteristics</th>
<th>Computer Security</th>
<th>Information Security</th>
<th>Information Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dates (approx.)</td>
<td>Since the early 1960s</td>
<td>Since the 1980s</td>
<td>Since 1998</td>
</tr>
<tr>
<td>Subject of protection</td>
<td>Computers</td>
<td>Information and information systems</td>
<td>Business as a whole</td>
</tr>
<tr>
<td>Goals</td>
<td>Reliability</td>
<td>Confidentiality, Integrity, Availability, and in addition Authenticity &amp; Trustworthiness, Auditability, Accountability, Non-repudiation and Privacy</td>
<td>Overall business protection</td>
</tr>
<tr>
<td>Type of information</td>
<td>Electronic</td>
<td>Primarily electronic</td>
<td>All types (electronic, paper and verbal)</td>
</tr>
<tr>
<td>Approach</td>
<td>Strictly technical</td>
<td>Domination of the technical approach, initial attempts to consider soft aspects (e.g. human factor, administration)</td>
<td>All-encompassing multidisciplinary systematic approach</td>
</tr>
<tr>
<td>Security Mechanisms</td>
<td>Technical</td>
<td>Primary focus is on technical security mechanisms; initial consideration of organisational and human-oriented mechanisms</td>
<td>All available (technical, organisational, human-oriented, legal)</td>
</tr>
<tr>
<td>Role within a business</td>
<td>Supporting system</td>
<td>Supporting system, often inducing some restrictions on business</td>
<td>An integral aspect of business, business enabler</td>
</tr>
<tr>
<td>Responsible employees</td>
<td>Technical staff</td>
<td>Dedicated staff and technical staff (often in addition to the other duties)</td>
<td>Senior management and dedicated staff</td>
</tr>
<tr>
<td>Involved employees</td>
<td>Technical staff</td>
<td>Senior management, dedicated and technical staff</td>
<td>All employees with an organisation</td>
</tr>
<tr>
<td>Drivers</td>
<td>Technical-needs driven</td>
<td>Security-needs driven</td>
<td>Business-needs driven</td>
</tr>
<tr>
<td>Flow of security decisions</td>
<td>Bottom-Top (senior management is not concerned with technical aspects of security)</td>
<td>Bottom - Top (security measures are initiated by technical specialists, based on their experience and passed to senior management for approval)</td>
<td>Top - Bottom (security measures are initiated by senior management based on risk analysis and implemented by relevant departments)</td>
</tr>
</tbody>
</table>
Appendix 2: Comparison of the properties of Information Security and Information Assurance (Ezingeard, McFadzean & Birchall, 2005)

<table>
<thead>
<tr>
<th></th>
<th>Information Security</th>
<th>Information Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Need-to-know only and protection from unauthorized access</td>
<td>How can ongoing compliance be ensured against regulatory changes or regional variations?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>What would be the impact on reputation of a breach in confidentiality?</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Preventing accidental or malicious alteration, corruption, or deletion</td>
<td>Can users compare relative levels of reliability if data is conflicting?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>How does the organization reduce costs incurred through errors?</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Disaster recovery and business continuity to ensure ongoing operation of existing systems</td>
<td>How can we develop systems that will not be restrictive as the organization grows, enters new alliances, or develops new businesses?</td>
</tr>
<tr>
<td><strong>Identification and Authentication</strong></td>
<td>Password access control</td>
<td>Do users keep their passwords secret and change them regularly because they are told to or because they understand the importance of password safety?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>How can we develop better identification and authentication methods for our stakeholders?</td>
</tr>
<tr>
<td><strong>Non-repudiation</strong></td>
<td>Fraud prevention</td>
<td>How can security reduce the organization’s transaction costs?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can transactions be simplified for our customers to increase their value gained from dealing with us, without compromising security?</td>
</tr>
</tbody>
</table>
### Agency Theory Overview

<table>
<thead>
<tr>
<th>Key idea</th>
<th>Principal-agent relationships should reflect efficient organization of information and risk-bearing costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit of analysis</td>
<td>Contract between principal and agent</td>
</tr>
<tr>
<td>Human assumptions</td>
<td>Self-interest, Bounded rationality, Risk aversion</td>
</tr>
<tr>
<td>Organizational assumptions</td>
<td>Partial goal conflict among participants, Efficiency as the effectiveness criterion, Information asymmetry between principal and agent</td>
</tr>
<tr>
<td>Information assumption</td>
<td>Information as a purchasable commodity</td>
</tr>
<tr>
<td>Contracting problems</td>
<td>Agency (moral hazard and adverse selection), Risk sharing</td>
</tr>
<tr>
<td>Problem domain</td>
<td>Relationships in which the principal and agent have partly differing goals and risk preferences (e.g., compensation, regulation, leadership, impression management, whistle-blowing, vertical integration, transfer pricing)</td>
</tr>
</tbody>
</table>
Appendix 4: List of Interview questions

Participant Profile:

1. What is your role in the organisation?
2. What qualifications do you have?
3. What is your experience with Information Security Auditing?

Understanding their view of Information Security Auditing:

4. What does “Audit” mean in the scope of Information Security?
5. Could you explain in detail the process you use for performing Audits?
6. What sort of data, if any, do you collect during evaluation?
7. What are the skills that are required for performing a good audit?