International Journal of Services and Standards

ISSN online: 1740-8857 - ISSN print: 1740-8849
https://www.inderscience.com/ijss

Protective shields: the drivers of adopting information security standards and complementarity with different security standards

Chia-Ming Sun, Kui-Ying Lin, Yu-Hsin Lai

DOI: 10.1504/IJSS.2022.10052703

Article History:
Received: 11 July 2021
Accepted: 19 January 2022
Published online: 09 August 2023

Protective shields: the drivers of adopting information security standards and complementarity with different security standards

Chia-Ming Sun*, Kui-Ying Lin and Yu-Hsin Lai

Department of Accounting,
National Yunlin University of Science and Technology,
No. 123, University Rd., Section 3, Douliu, Yunlin, 640, Taiwan
Email: sunjm@yuntech.edu.tw
Email: queena_lin888@hotmail.com
Email: m10725024@gemail.yuntech.edu.tw
*Corresponding author

Abstract: Information security is a serious issue threatening businesses. Thus, effective strategies are needed to protect critical organisational information. Research indicates that organisations should implement IT governance and security using best practices from different frameworks rather than relying on individual existing frameworks. This study explores key factors influencing adoption and implementation of information security management systems from the perspective of the ISO 27001 certification process. We provide insight into how organisations seek support and guidance from different standards and frameworks. Using the grounded theory methodology, we interviewed fourteen participants with information security competence who work in manufacturing, financial or consulting services industries. We identified response themes relating to ISO 27001 adoption factors and implementation drivers. We also examined differences between ISO 27001 and CIS Controls. Our results suggest that effective integration of ISO 27001 certification and CIS Controls allows organisations to achieve best practices in IT governance and security.

Keywords: information security management systems; cyber security risk; information security standards; information security governance; ISO standards; ISO 27001 certifications; CIS controls.

Reference to this paper should be made as follows: Sun, C-M., Lin, K-Y. and Lai, Y-H. (2023) 'Protective shields: the drivers of adopting information security standards and complementarity with different security standards', *Int. J. Services and Standards*, Vol. 13, Nos. 3/4, pp.195–220.

Biographical notes: Chia-Ming Sun is an Associate Professor and currently as the Chair of the Accounting Department at the Yunlin University of Science and Technology in Taiwan. He has a PhD in Information Management from Chiao Tung University. His research interests include information technology governance, information technology auditing, business analytics, and enterprise information systems. He has industrial experience more than fifteen years and worked as an information system manager and IT consultant.

Kui-Ying Lin is a Doctoral student of the Department of Accounting at National Yunlin University of Science and Technology in Taiwan. Her research interests are auditing, accounting ethics, and information technology.

Yu-Hsin Lai works as an Information Technology Auditor in the PwC Taiwan. She received her master degree with concentration in Accounting from National Yunlin University of Science and Technology.

This paper is a revised and expanded version of a paper entitled 'The factors of adopting and implementing information security management systems with ISO 27001 certification' presented at *International Journal of Services and Standards (IJSS) Annual Conference 2021*, Yunlin, Taiwan, 21 August, 2021.

1 Introduction

In this modern society, national economies and businesses depend on information technology (IT) for survival. However, information security (InfoSec) incidents can generate substantial amounts of direct costs from repeated work, loss of data and interruption of operations, as well as indirect costs due to loss of consumer confidence and, subsequently, future business (Hasan et al., 2021). Thus, InfoSec has become a serious global issue threatening businesses and requiring effective strategies to protect critical organisational information (AlGhamdi et al., 2020; Hussain et al., 2020; Knapp et al., 2006).

Across the world, governing authorities and regulators have responded to this urgent issue with new legislations. For example, the Federal Information Security Management Act (FISMA) of 2002 requires each US federal agency to develop mandatory InfoSec risk management standards as a way to protect the economic and national security interests of US (White, 2010). In Europe, the EU General Data Protection Regulation of 2018 is a landmark in the evolution of the European privacy framework. It has six data protection principles: fairness and lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. In Taiwan, the Cyber Security Management Act (CSMA), announced in June 2018, is the core piece of legislation regarding cybersecurity (Burgers et al., 2021). The CSMA requires Taiwan government agencies and certain non-government agencies to adopt cybersecurity maintenance plans and report any cybersecurity incident to the relevant government authorities. Each competent authority has issued guidelines for adopting cybersecurity plans for businesses in their jurisdictions. Such guidelines typically refer to and recommend general security standards, including the Internal Standards Organization (ISO) 27001 information security management standard (Burgers et al., 2021).

These legislations and guidelines have driven interest in ISO 27001, which is especially popular among organisations in Taiwan. Regulation may be one of the main factors in the adoption of ISO 27001 certification. In addition, customer needs for cybersecurity assurance have put increasing pressure on managers to introduce ISO 27001 to their companies (Calder, 2016). Moreover, the intention of improving business performance may lead management to obtain ISO 27001 certification, which can be presented to target markets as a signal of high InfoSec quality (Fomin et al., 2008). Together, these three factors could greatly influence the adoption of ISO 27001. However, it remains unknown what motivates managers in Taiwan to adopt ISO 27001 standards. The first aim of this study is to fill this knowledge gap by exploring the influential drivers of ISO 27001 adoption.

ISO 27001, which can be applied to all sizes and types of industries, is defined as a set of principles about the implementation of an appropriate information security management system (ISMS). It is an international security standard to assist organisations to apply a risk-based approach to their security protection. This standard emerged in 1995 as BS-7799 and was revised in 2005 and 2013. Given the public concerns of InfoSec breaches, certification of compliance with the ISO 27001 standards may function as an ideal demonstration of security assurance, that is, a 'signalling tool' for InfoSec quality (Terlaak and King, 2006). ISO 27001 has assisted companies in developing and maintaining an ISMS and remains one of the most effective risk management tools for fighting off the billions of attacks occurring each year around the world (Mirtsch et al., 2020). Surveys of IT managers at Saudi organisations found that 78% of respondents view determining the effectiveness of their InfoSec controls as an important driver for implementing ISO 27001 certification (Nabi et al., 2010). However, the determinants of the effectiveness of information security controls remain unknown. Therefore, our second aim in this research is to investigate the main drivers for the effectiveness of implementing the ISO 27001 certification.

Although ISO 27001 clarifies what requirements organisations should follow, it does not provide guidance on how to implement the standard (Diamantopoulou et al., 2019). Pragmatically, the challenging issue for organisations to achieve ISO 27001 certification is how to establish and design suitable InfoSec policies and procedures for implementing ISO 27001. In fact, adopting other applicable and complementary InfoSec frameworks (e.g., CIS Controls, ISO 27002, ISO 27799 and PCI DSS) with ISO 27001 is a common practice for certified organisations. The CIS Controls (Center for Internet Security Critical Security Controls, previously referred to as the SANS Top 20 Controls, or CIS 20) are one of the most popular complementary security frameworks. In 2008, the National Security Agency (NSA) initiated work with the SysAdmin, Audit, Network, and Security (SANS) Institute and the Center for Internet Security to develop the CIS Controls for effective cyber defence (Security, 2019). The CIS Controls are a set of 20 controls and 171 sub-controls. It provides organisations with an overall planning approach for InfoSec protection (Groš, 2019). Specifically, the CIS Controls provide a list of security measures for implementers to protect their environment against cyberattacks.

The ISO 27001 certification mainly focuses on a comprehensive information security governance (ISG) framework to help its clients properly establish an ISMS ((AlGhamdi et al., 2020; Veiga and Eloff, 2007), and does not specify approaches to protection, detection and response to cybersecurity attacks. By contrast, the CIS Controls provide a detailed risk assessment for clients to prevent security incidents from happening. Therefore, it may benefit organisations to integrate the complementary ISO 27001 certification and CIS Controls as an InfoSec strategy to effectively reinforce their information security. An integrated system for information security management (ISM) is useful for understanding InfoSec and predicting management outcomes (Hong et al., 2003). As suggested by Shariffuddin and Mohamed (2020), organisations should roll ensure programs align with the best practices of IT governance and IT security rather than simply adapting individual IT security practices. In this regard, we argue for the integration of ISO 27001 certification with the CIS Controls as a way to achieve these best practices. As a result, our final research motivation is to examine whether the complementary supports and guidelines from ISO 27001 and the CIS Controls can help organisations, who face different security requirements and are at different stages of

capability maturity, achieve their ultimate goal of applying the best practices of enhancing cybersecurity.

Taken together, the aim of this study is to explore the main factors affecting the adoption of the ISO 27001 certification, the most important drivers for effectiveness of ISMS implementation and the determinants of choosing the right complementary supports and guidelines to effectively protect companies' information assets and ensure business continuity. To accomplish our research objectives, we employed qualitative semi-structured interviews with fourteen participants who have InfoSec competence and work in the manufacturing, financial, or consulting services industries of Taiwan. This qualitative research known as grounded theory enabled us to fully capture concepts relevant to IT professional experience in the real world of InfoSec practice. This gave us the power to gain remarkable and fresh insights into InfoSec performance in Taiwan.

The results enabled us to provide the following evidence.

1 The main factors in the adoption of ISO 27001 certification are: a need to comply with the thrust of regulations to avoid penalties for regulatory violations, a necessary response to customers' requirements to enhance their trust, and a clear endorsement of funding and consideration from the corporate executives.

2 The effectiveness of implementing an ISMS is attributable to the success of executing InfoSec policies through effective risk communication, the technical assistance of an experienced consultant to strengthen management systems within the organisation, a heightened employee awareness of InfoSec risks to support operational success of the ISMS, and the internal auditors' professional competence to perform diverse internal audit projects.

3 The ISO 27001 system provides independent certification for organisations to obtain affirmation from regulators, competent authorities, customers, and all corporate stakeholders, whereas the CIS Controls give immediate signals of the latest threat trends to be prioritised as 'must do first' projects. Our results suggest that organisations can achieve the best practices of IT governance and IT security by integrating ISO 27001 certification and the CIS Controls as a way to properly implement information systems and effectively reinforce InfoSec.

This paper contributes to the literature with the first evidence of the overall performance of adopting ISO 27001 standards and the CIS Controls in various industries of Taiwan. Our findings have implications for governing authorities, InfoSec system implementers, and InfoSec service consultants. First, the new concepts could provide relevant and useful information for authorities to amend or update their policies and guidelines. In addition, the new performance knowledge could help InfoSec implementers make informed decisions regarding the most suitable standards and controls for their organisations. Lastly, InfoSec service providers can obtain relevant information to design the most suitable services for their clients as a way to boost business.

The remainder of this paper is structured as follows. In Section 2, we review prior literature on InfoSec governance and management systems, international information security standards, and the CIS Controls. Section 3 presents the research design and procedures. We analyse and discuss findings in Section 4. Finally, Section 5 concludes.

2 Literature review

2.1 Information security governance and management systems

Posthumus and von Solms (2004) argue that ISG is the process of how InfoSec is emphasised at an executive level, is considered a facet of an organisation's broader corporate governance strategies and is connected to the board of directors because IT plays an integral role related to the storage, processing, and transmission of valuable information assets. In addition, von Solms (2005) claims that ISG consists of management commitment and leadership, organisational structures, user awareness and commitment, policies, procedures, processes, technologies, and compliance enforcement mechanisms. The joint effort of these aspects could maintain the confidentiality, integrity and availability of the company's electronic assets (AlGhamdi et al., 2020). Moreover, through the analysis of qualitative and quantitative data, Flores et al. (2014) found that ISG creates a platform to establish security knowledge sharing and that coordinating processes realises the effect of both the structure of the InfoSec function and the alignment of InfoSec management with business needs.

ISG has become an integral part of good IT and corporate governance (von Solms, 2005). ISG focuses on security issues posed by IT and involves the InfoSec) execution of top management and the board of directors, who decide how the organisation's InfoSec security guidelines and policies are properly created (Posthumus and von Solms, 2004). Nowadays, the demands for these types of policies are regularly considered the best internationally accepted practices for ISM, which must properly respond to risk and ensure that information assets maintain confidentiality, integrity and availability to legitimate users. As a result, these information security policies have become an essential part of requirements for good IT governance as well as good corporate governance. With growing attention on InfoSec regulations and standards, ISM has focused not only on the previously emphasised operational management of technology, but also on the expansion of compliance with InfoSec policies, regulations, or standards (Ifinedo, 2014; von Solms, 2005). The latter has become a central focus of information security governance.

2.2 International information security standards

The ISO/IEC 27000-series from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) focus on standardised operational procedures for ISM. ISO 27001 enable organisations to obtain an ISMS certification through independent third-party audit institutions (Schweizerische, 2013). For fast growing companies, third-party certification can strengthen the effectiveness of entrepreneurs' goodwill and their internal controls and thus help entrepreneurs win affirmation from all corporate stakeholders (Mataracioglu and Ozkan, 2011). As a result, ISO 27001 has become popular and the number of third-party certifications issued has continually grown in recent years (Hsu et al., 2016; Velasco et al., 2018).

The ISO 27001 standard was last revised in 2013. The primary norm of the standards is to establish and implement an ISMS and create proper documentation to ensure that the operation within an organisation is efficient and effective (Boehmer, 2008; Gillies, 2011). In general, ISO 27001 requires implementers to follow the general application requirements of ISO to develop the system through the four phases of plan-do-check-act (PDCA), also known as the Deming Circle, which was first proposed by US quality

management expert Deming. The main purpose of an ISMS is to handle risk management and include people, data, equipment, access, system security and environmental security in the scope of information security. The ISMS also provides planning, establishment, implementation, operation, supervision, auditing, maintenance and improvement for the ISMS model (Gillies, 2011).

The implementation of ISO 27001 for an enterprise's security safeguards brings the company several advantages. The first is that ISO 27001 certification can be presented as a public verification of an organisation's ability to safeguard its information security (Roy, 2020). In addition, certification can ensure that an organisation's ISMS and its security policies continue working properly in a rapidly evolving environment and adapt to quickly changing risk exposures (von Solms, 2005).

However, there can be a pendulum effect from certification as organisations invest more human capital and funds into the establishment and certification of the ISMS. Some scholars suggest that, from the management perspective, ISG investment is insufficient (AlGhamdi et al., 2020). Moreover, the uneven allocation of funds and resources can substantially affect the benefits of information security investment (Hsu et al., 2016). In addition, the downside of using ISO 27001 for IT governance is that the system fails to provide implementers with clear instructions of how to do certain things. Consequently, the control objectives are more focused on the issue of what must be done rather than how to do them effectively. It also provides companies with insufficient guidance because of its incomplete list of controls and its lack of support for cybersecurity threats (Diamantopoulou et al., 2019; Roy, 2020; Soomro et al., 2016).

2.3 The CIS controls

In 2008, the NSA initiated a cooperative effort with the SANS Institute and the Center for Internet Security to develop the *CIS Critical Security Controls for Effective Cyber Defense*, known as the CIS Controls (Groš, 2019; Security, 2019). The CIS Controls target the loss of critical information from data breaches or cybersecurity attacks and publish cybersecurity frameworks and best practices that directly address the attackers' actions, newly developed technologies and changing business demands. The CIS Controls provide organisations with overall planning for the InfoSec protection (Security, 2019).

The CIS Controls were developed over ten years ago by a group of IT experts who applied their first-hand experience of dealing with offence or attacks by creating globally accepted best practices for security. The experts have worked in a wide range of sectors, including retail, manufacturing, healthcare, education, government and defence. The CIS framework gives a short list of items that prioritise control measures within multiple frameworks to assist enterprises in prioritising cyber defence actions. It also ensures that these measures are manageable to help users apply the framework to address attacks following the principle that 'offense must inform defense' (Security, 2019). Moreover, the content of the controls is automatically adjusted according to changes in current attack patterns, such as identity authentication, encryption and application whitelisting. The system also makes clearer, stronger and more sustainable recommendations.

The control methods listed in the CIS Controls can be categorised as basic, fundamental, and organisational. The basic controls include the most critical control items. To meet this elementary requirement of network defence readiness, all organisations should implement these control items to build a strong foundation for the

overall defence mechanism. The fundamental controls are considered the best practice for security technology and provide more significant benefits for enterprises. In comparison with the basic and fundamental controls, the organisational controls focus more on people and processes related to cybersecurity (Security, 2019).

Table 1 compares the ISO 27001 standards with the CIS Controls in terms of concepts, purposes and controls.

Table 1 Comparisons between ISO 27001 and CIS controls

Information Security Standards		
	ISO 27001	*The CIS controls*
Issuers	The International Organization for Standardization (ISO)	The Center for Internet Security and the SANS Institute
Frameworks	ISO/IEC 27001-Information Security Management System Certification	CIS Critical Security Controls (CIS CSC) or CIS 20 Controls (CIS 20)
Purposes	To ensure that the operation within an organisation is efficient and effective.	To construct network defence systems
Concepts	To follow four-phrase-normative requirements – plan-do-check-act (PDCA)	Offence informs defence Prioritisation of operational processing Measurements and metrics Continuing diagnostics and mitigating offence Automation
Level of focus	Management perspective	Technical perspective
Control items	14 scopes of controls with 35 control objectives and 144 control items	20 critical security controls with 171 sub-controls*

(*) Remark: Our research interview protocol is based on CIS Controls V7.1(Security, 2019), which was announced in 2019. The newest version is V8, as revised in April 2021 during our paper submission. CIS Controls V8 defined 18 top-level Controls and 153 Safeguards (formerly sub-controls).

3 Research design

This study aims to identify the key factors affecting the adoption and implementation of ISO 27001 certification and to providing new insights into the complementary effects of implementing multiple information security standards in diverse industries. On the basis of the ISO 27001 standards and the CIS Controls, we mainly examine this concept with evidence from Taiwan.

The next two subsections describe the research method and the research design and procedures.

3.1 Research method

Qualitative research utilises an open and flexible design to collect and interpret data and can be used for different purposes and structures (Corbin and Strauss, 2014). This study employs a type of qualitative research known as grounded theory, which is a social research methodology for an iterative process of data collection and analysis (Corbin and Strauss, 1990; Glaser and Strauss, 2017). The key feature of grounded theory is constant revision during the research through repeated interviews, observations or documents. Therefore, grounded concepts in the reality of data are identified and verified to guard against researcher bias in terms of observation congruence or compatibility (Corbin and Strauss, 1990).

We chose the classic grounded theory methodology to apply to the new field of ISM. Gioia et al. (2013) claim that, unlike deductive research, which advances in knowledge that is delimited what we can know, inductive study with qualitative rigour can develop new concepts and ideas from credible interpretations of data.

In the process of applying grounded theory, Parker and Roffey (1997) emphasise that theoretical sensitivity is needed to recognise new insights through selecting and understanding the data. To enhance theoretical sensitivity, researchers have to continually interact with the data collection and analysis by applying techniques such as questioning, coding, reviewing literature, theoretical sampling, challenging assumptions and making constant comparisons (Kirk and van Staden, 2001).

Using the literature review in the previous section, we applied a theoretical sampling process in the data collection. Theoretical sampling, unlike statistical sampling in positivist quantitative research, is used in grounded theory research as a process of data collection for generating an emerging theory by first collecting, coding, and analysing the data and then determining the subsequent data collection (Glaser and Strauss, 2017). After thoroughly reviewing worldwide literature related to information security standards and governance, we used qualitative semi-structured interviews as a primary source of data collection because this technique allows the interviewees a high degree of freedom to explain their thoughts and to highlight areas of their expertise in terms of experiencing the application of InfoSec standards. For the semi-structured interviews, we designed open-ended questions and interview guides according to the aims of this research. To support in-depth exploration of the actual situations of implementing standards by enterprises and organisations, the preliminary structure of the interview process was created as a step-by-step guideline.

After the interviews, we followed the classic grounded theory methodology developed by Glaser and Strauss (2017) to analyse the interview responses. The transcripts were analysed, generalised and compared to reveal recurring themes or categories (Glaser and Strauss, 2017). This approach to the handling of qualitative data allowed the formulation of illustrative propositions about the effects of applying InfoSec standards.

With theoretical sampling, we do not use the amount of data to determine whether we've collected enough data. Rather, we collect data until we reach theoretical saturation (Glaser and Strauss, 2017), which occurs when adding additional data does not contribute any more properties to the existing categories, in our case, built from the interview transcripts.

3.2 Research procedures

This study used the classic grounded theory method developed by Glaser and Strauss (2017) to guide the full process of this research from emerging research questions to answering the question with substantive theories and new concepts.

3.2.1 Preparation stage

At this stage, we developed open-ended questions for the interview protocol based on our research objectives. The interview protocol was given to two independent raters who were not associated with the research project, but who had substantial understanding of this research. The research team assessed the interpretation of the interview content and discussed minor discrepancies. The discrepancies were then resolved and the thematic frequencies were finalised.

This preparation facilitates the overall process by providing clear guidance for interviewees to quickly familiarise themselves with the research scenarios and supporting the intended research data to be obtained efficiently and effectively. The main themes for the theoretical concepts were the process of implementing InfoSec standards, compliance with the standards, the effect of information auditing and the impact of InfoSec standards on organisations/institutions from the management perspective. In the process, all interviewees gave permission for the conversations to be recorded under the condition of strict confidentiality in order to elicit honest responses to sensitive topics.

3.2.2 Data collection

We selected 14 participants for interview based on their InfoSec skills or consultancy and InfoSec audit experience. We expected that such professionals could provide rich insights into the adoption and implementation of the ISMS with diverse InfoSec standards and frameworks. We conducted semi-structured open-end question interviews with each participant. The participants were InfoSec staff and audit directors, managers or consultants from 12 companies with an average tenure of 18.5 years from three industries: finance, manufacturing and consultancy services (Table 2). Each interview lasted around 1–1.5 h.

Using the pre-designed interview protocol, we employed the qualitative interview method to invite participants to discuss their experiences of their organisation or clients implementing international InfoSec standards.

3.2.3 Data analyses

The recorded interviews were professionally transcribed and the transcripts were coded into classifications related to the research questions. Then, the categorised data were analysed by means of comparative methods and analytic deduction to reveal recurring themes. This iterative process of constant comparison, multiple reading, note taking, coding and creating categories aimed to ultimately lead to the emergence of the core concepts from the data. Therefore, we were able to suggest the discovery of new concepts impacting InfoSec standards for organisations. The recurring themes were categorised and arranged in alphabetical order. Meaningful interviewee quotations were numbered. Thus, the following sections refer to each quotation in parentheses as (a theme category, a hyphen and a number), such as (A-1). Italics hereinafter denote these quotations.

Table 2 Interviewee profiles

No.	*Industry type*	*Background*	*Title*	*Tenure*
1	Manufacturing	IT	Director	15 years
2	Manufacturing	InfoSec audit	Assistant Manager	15 years
3	Finance	IT/InfoSec	Technical Manager	18 years
4	Manufacturing	InfoSec audit	Director	23 years
5	Manufacturing	IT	Senior Engineer	17 years
6	Finance	InfoSec	Manager	18 years
7	Consulting services	InfoSec	Manager	25 years
8	Manufacturing	InfoSec audit	Chief Auditor	28 years
9	Manufacturing	IT	Director	20 years
10	Finance	InfoSec	Specialist	15 years
11	Finance	InfoSec	Supervisor	25 years
12	Consulting services	InfoSec	Assistant manager	10 years
13	Consulting services	InfoSec	Senior manager	15 years
14	Manufacturing	InfoSec audit	Manager	15 years

4 Analysis results and discussion

Sections 4.1–4.3 respectively provide detailed analysis of the interviews based on three main themes:

1 the main factors affecting the adoption of ISO 27001 certification

2 the key drivers of effectiveness of implementing ISO 27001 certification

3 the differences in various industries from the perspectives of controls and security standards.

The text of the integrated interviews recorded in the process was analysed in accordance with the three steps of the grounded theory.

4.1 The main factors affecting the adoption of ISO 27001 certification

From the grounded theory coding, we attribute the effect of adopting ISO 27001 certification to three main aspects: complying with the thrust of regulations, responding to customers' requirements and enhancing their trust, and measuring the top management's cognition and the cost-effectiveness of ISO 27001 implementation.

4.1.1 Complying with the thrust of regulations

Although compliance with specified InfoSec regulations differs from industry to industry, InfoSec requirements from regulators or competent authorities have gradually increased in recent years. Financial institutions, for example, are highly supervised and significantly affected by regulatory specifications. In particular, they are stipulated to establish an independent InfoSec department and its supervisor is responsible for

planning, monitoring, and promoting the ISMS. By contrast, the general manufacturing sector is subject to relatively low regulatory requirements. As a result, the availability and continuous operation of information systems is the essential and fundamental purpose of adopting the ISO 27001 certification for most manufacturing companies.

For general enterprises, however, InfoSec requirements have gradually expanded from basic availability to compliance with increased regulatory requirements (A-2). Most organisations, especially financial institutions, healthcare providers or government agencies, must comply with various regulations related to the issues of data protection, privacy and IT governance. The implementation of an ISMS, such as through ISO 27001 certification, can provide suitable methodologies for organisations to operate the ISMS effectively. The ISMS is often based on an add-on management system to institutionalise their InfoSec policies and guidelines.

Some companies intend to avoid penalties for regulatory violations (A-3) so they fully comply with the reviewing procedure of regulations (A-4) and with the clearly specified requirements of ISMS standards (A-5). In addition, they periodically review the level of implementation of the ISMS as a way of reducing their InfoSec risk. The following are excerpts from interviews with two participants (a supervisor and a specialist) who have InfoSec competence and work at financial institutions.

> "The ISMS standards are regarded merely as part of the internal control system; more emphasis should be placed on the process of information security risk assessment (ISRA). The ISO 27001 certification is not only used as procedural controls and also to help examine whether the regulations are actually and fully followed or executed (A-4)."

> "In management, the InfoSec framework is gradually strengthened through complying with standards and specified requirements because, for a bank, an avoidable or careless mistake of a security incident can cause not only considerable damage to the corporate image, but also a possible loss of hundreds of millions of New Taiwan dollars in the end. Generally speaking, the strategy of implementing ISMS provides the real benefits for a bank indeed (A-5)."

4.1.2 Responding to customers' requirements and enhancing their trust

Nowadays, both current and potential customers are increasing their demands for assurances from merchants or entrepreneurs that they fulfil the requirements of InfoSec standards (B-1). A senior manager from InfoSec consulting services expressed his knowledge about the issue as follows.

> "For major enterprises, the main motive in implementing the ISO 27001 certification comes from both the requirements of governmental regulations and the requirements of customers' demands for the assurance from vendors or sellers who must fully comply with the InfoSec standards. Only a small number of corporations implement the ISO 27001 certification autonomously and expectantly (B-1)."

Obtaining ISO 27001 certification has positively promoted the growth of customers' trust and companies' credibility on the markets (B-1). Each customer may have their own custom security questionnaire, so companies can reduce their efforts by using the same

set of certified ISMS procedures (B-3). A manager with competence in information systems audit in the manufacturing field stated:

> "Last year, some customers claimed that they would not continue placing orders to us if our company had no relevant information security certification. As a result, we were forced to get certified by the customers' demands. However, the customer information is usually separated from and not related to all other company's information systems so customers are deeply concerned only about the assurance of the InfoSec system directly related to themselves. So, we tried to reduce the scope of certification (B-2)."

The program of ISO 27001 certification can greatly help companies differentiate themselves from their competitors, retain existing customers and attract new customers, all of which are effective business strategies (B-4). A standardised model of certification allows customers to understand that the enterprise has the ability to enhance the ISMS with continuous improvement. A specialist with InfoSec competence working in a financial institution described the situation as follows:

> "Banks are in a highly specialised industry, so earning customer trust is very important to the success of a bank. Therefore, the ISO 27001 certification gives the bank the benefits in promoting the online banking with credit for the success (B-3)."

4.1.3 Top management's consideration of penalties and cost-effectiveness

The common key factors of investing in institutionalising InfoSec policies in various industry sectors are highly dependent on the perceptions and considerations of top management. In the financial sector, for example, the board of directors and the chief executive officer strongly feel the significant and constant pressure from supervisory authorities, the risk of possible high penalties for violations and the negative impact of security incidents on corporate reputations. As a result, they are typically willing to invest heavily in the ISO 27001 standards as a protective shield against external parties and supervisory authorities (E-1).

By contrast, operation-level management in the manufacturing sector is more keenly concerned with the cost-effectiveness of ISO 27001 investments. The ISMS involvement is expected to meet only the basic requirements and the IT department is considered fully responsible. In business operations, many managers or executives believe that InfoSec investments are not directly related to revenues. Their beliefs, in turn, lead to insufficient consideration of the ISMS from their top management (E-2). In recent years, this situation has slightly improved as the number of hacking incidents has increased substantially and the pressure from customers has grown. A director with an information supervisory background from a manufacturing company said:

> "For us, the senior managers have still mainly focused on business operations and believed not only that it was too costly for the IT department to improve the ISMS, but also that the InfoSec improvement brought our company no direct link to the growth of revenues or the increased number of orders. As a result, when we touted for the implementation of the ISMS, our top management seemed to lack enthusiasms for the adoption of the ISMS project (E-2)."

Senior managers believe that the primary purpose of implementing ISO 27001 is to meet the requirements of the supervisory authorities or customers. In addition, ISO 27001

certification brings the company intangible benefits which are immeasurable from the perspective of cost-effectiveness, so management are very cautious about overcommitment to or overinvestment in the ISMS project to avoid wasting valuable resources (E-3). Therefore, most companies prefer to quickly obtain the ISO 27001 certification. This hasty decision may ultimately lead to insufficient institutionalising of InfoSec policies. A senior manager with an InfoSec consultancy background in the consulting services industry expressed it as follows.

> "Many companies have encountered inadequate IS implementation because their only consideration of obtaining the ISO 27001 certification was to win contracts from customers. Therefore, they naturally applied the cost-effectiveness to evaluate their investment in the ISMS and they had no intension of investing too much resource in the system; as a result, the implementation of their information system was limited to a small scale in the end (E-3)."

However, the management approach of ISMS implementation still attracts top management's attention. Because the difference in professional knowledge and backgrounds leads to varying perceptions of InfoSec improvement, it is not easy for senior managers to distinguish between the effect of various technology controls and management controls. As a result, the management-oriented ISO 27001 with its externally recognised certification is highly likely to succeed in winning support from corporate executives to allocate resources for certification projects (E-4). Despite strong support from corporate executives, insufficient resources can undermine the aim of actually improving the ISMS, resulting in shattered high expectations relating to certification (E-5). A senior manager with an InfoSec audit background who works in manufacturing stated:

> "If a company has not yet created an internal climate of the ISMS, the bosses (corporate executives) will not view the InfoSec control activities as high at the top of their agenda; instead, they always consider the corporate performances their most important consideration in terms of allocating resources. The situation of competing for the allocation of scarce funds and resources is very common in most institutions and even in government units. This is why there is a big gap between the actual ISMS implementation and the expected/desired outcomes (E-5)."

4.2 Key drivers of effectiveness of implementing ISO 27001 certification

We discuss the following four main drivers of implementation effectiveness: risk communication and process improvement, the consultation with external experts, InfoSec awareness and training for employees, and sufficient auditing personnel with regulatory compliance skills.

4.2.1 Risk communication and process improvement

Throughout the whole process of implementing the ISMS, risk communication is critical for the ISRA process, risk mitigation, incident response plans and following continuous improvement initiatives. In the ISRA process, for example, each person has different considerations for risk scenarios. The reality of how to ensure that implementing the ISO 27001 project actually achieves the maximum overall benefits to the organisation is the most serious challenge of risk communication during the process. The consultants

interviewed believe that it is necessary for personnel to continuously update the list of risk events and to constantly rehearse the proper reaction to InfoSec incidents (also known as scenario training), which is a technique that can enhance the perception of risk scenarios (F-1, F-2). The updated information and scenario training help to evaluate the overall ISRA and thus mitigate avoidable human errors that can lead to substantial losses for corporate operations (F-3). This perspective was described by two participants respectively below.

A specialist in the financial sector stated:

> "For the ISRA, different people face different risk scenarios so it takes a long time to communicate the ideas of the ISRA, overcome many obstacles, mitigate serious disagreements, and ultimately hope to reach an agreement on enhancing the information security. It is very difficult to reach a general consensus (of all parties involved) in the process; in fact, each business unit has its own position that will affect the overall ISRA results in the end (F-1)."

A senior manager in consulting services said:

> "The most needed improvement in the bottom-up IRSA is at the practical level because most company personnel do not like to constantly update the risk profiles. Understandingly, updating records based on each risk incident is very cumbersome and time-consuming processes and thus become a burdensome workload of employees (F-2)."

At the time of implementing the ISO 27001 certification, the meticulous requirements of developing the ISMS and the scope for required improvement were highly related to the industry characteristics and to each organisation's ISG capability maturity level. In the case of manufacturing, the main considerations were driven by cost-effectiveness and the necessity of controlling measures to within acceptable risk tolerance. By reviewing the control list of ISO 27001 recommendations, controlled items unrelated to the business may be excluded based on their applicability or postponed to improvement plans according to the level of risk (G-1). Through the PDCA cycle of the ISO 27001 annual review, the continuously accumulated experience from handling security incidents can gradually improve (G-2). A director with an information supervisory background in the manufacturing sector stated:

> "If we (an ISO 27001 implemented company) believe that the current level of InfoSec risks is acceptable or tolerable, the consultants will not insist that we take the proposed controls of the IS standards or the controls adopted by other institutions. They do not require us to immediately rectify the identified deficiencies but hope to be convinced that they can help us arrange a medium-and-long-term plan for improving the ISMS in the near future (G-1)."

On the other hand, the ISG of financial institutions is usually at or beyond the 'defined' stage of capability maturity, and so the applicability of the ISO 27001 standards is considerably higher than other industries. Very few of the controlled items under the ISO 27001 recommendations are excluded in this sector (G-3). For financial institutions, the benefits of implementing ISO 27001 are the promotion of overall InfoSec risk management, the comprehensive review of existing control procedures to determine whether they are appropriate, and the support to improve the existing control processes

and enhance control effectiveness (G-4). A specialist with an InfoSec background from a financial institution said:

> "A financial institution itself is at a more mature stage of the ISMS development; the most control items of the ISO 27001 standards have already been implemented. Just the procedures and the clarity of defining the documentation are not yet clearly well-established. More specifically, the ISO 27001 can help us clarify the suitability of control procedures and the definition of documenting the needed records (G-4)."

4.2.2 Consultation with external experts

A full understanding of the current conditions and the evolving threat landscape is a critical part of a consultant's expertise with ISMS implementation. A good consultant has the ability to translate InfoSec risks into real business terms. Companies have to not only be keenly aware of the real risks that they face, but also be in a much better position to develop a solid business case to secure a sufficient budget for implementation of the ISO 27001 project. The purpose of implementing ISO 27001 is not only to institutionalise the organisation's risk management system, but also to make a proper, simultaneous selection of practical technical programs. A consultant should help strengthen the management systems in the organisation (C-1). A director of information technology department from a manufacturing company stated:

> "Consultants will give specific technical requirements or a clear determinant of whether the written documentation is complete. The benefits of hiring a consultant are not only to give management the needed advice, but also to provide specific suggestion of how to properly enhance the system (C-1)."

It is very important for a consultant to provide a company with an intense training program to raise employees' awareness and understanding of the ISMS, as well as practical operational procedures to enhance control effectiveness. However, if a company only intends to obtain ISO 27001 certification at a basic level, it will only get a record of documentation, but will not achieve significant improvement in actual operations. Although documentation is an important part of an effective ISMS, implementing the standard is much more involved than just writing up a set of policies and procedures (C3). Consultants must consider the industry characteristics when giving their clients recommendations for targeted activities or control procedures (C-2). A supervisor with an information security background and from a financial institution described this issue as follows:

> "Experienced consultants know how to help a company effectively assess and identify the necessarily addressed risk factors of running the current InfoSec system. No matter whether it is the issue of technical measures or the important control procedure, the professional counselling and coaching will contribute to not only the success of obtaining the certification, but also the overall improvement of the ISMS (C-2)."

4.2.3 Employees' InfoSec awareness and training

The success of implementing the ISMS and the effectiveness of running the system are usually attributed to the strengthened employees' InfoSec awareness by training. However, for most publicly listed companies who already have well-defined internal control systems, some employees put up a strong resistance to the establishment of the

ISMS on top of the existing control systems (D-1). Although the ISO 27001 standard helps organisations establish a clearer and more systematic approach to manage the ISMS, and the institutionalised approach can make the process of the ISMS more rigorous, reliable, and precise. The implementation of the ISMS may place a workload burden on staff, generating negative impacts on operational efficiency and effectiveness. A supervisor with an information security background and from a financial institution stated:

> "During the implementing process, most people mistakenly consider the ISO 27001 an independent operating system so they do not understand why it needs to develop the ISO 27001 system on top of the internal control systems. They also believe that the InfoSec department should bear the full responsibility for most control activities. As a result, the inappropriate integration of the ISMS with the internal controls has led to a huge human burden on employees whose work pressure has amounted (D-1)."

Employees with inadequate knowledge of the ISMS will not only have reduced willingness during the ISMS implementation, but also have a negative impact on the extent of InfoSec control activities. More seriously, taking the edge off the violation without continuous improvement or the failure to actively respond to InfoSec incidents can lead the ISMS to become rigid and vulnerable to risks. The perspectives of two participants from the manufacturing sector are below.

> "In the team of implementation, none of the teammates has experience with ISO 27001 certification and thus take a long time for them to familiarise themselves with the new system and to develop the necessary expertise. However, the difficulty is that each team member is also responsible for his/her original tasks or projects, so each of them has to spare his/her working hours to receive the needed training for the new role. The lack of specialists or talents in the ISMS will negatively affect the quality of implementing the ISO 27001 certification (D-2)."

> "I believe that the gap between the actual outcome and the expectation can be attributed to people (the general employees) whose security awareness should further be strengthened. You often find that the identified control deficiencies must not be rectified until the next audit or until the auditor's ongoing initiative. The fundamental problem is that he (a general employee) does not take this InfoSec risk very seriously (D-3)."

4.2.4 Sufficient auditing personnel with regulatory compliance skills

The scope of internal audit projects is often very diverse within the internal control system. Thus, the internal auditors' professional competence with InfoSec audit is slightly inadequate for most enterprises. In addition, the timing pressure of field audit induces the auditors to focus only on individual item validation and to fail to examine the related procedures as part of a holistic picture. These phenomena highlight deficiencies relating to current InfoSec audit personnel (H-2). Internal auditors are usually unfamiliar with the technical details, so the biggest challenge for auditors is how to effectively communicate with IT staff and clearly explain the technical requirements of regulation and standards to InfoSec related parties (H-3). Sometimes, using checklists provided by the InfoSec

consultants as auxiliary documents is necessary for internal auditors to facilitate or enhance the efficiency of the audit (H-4). A specialist with an information security background and from a financial institution described the situation as follows:

> "In the real world, an auditor cares deeply about…that is to say he usually does not know much about the technical details of information security… Auditing is a slow and laborious process. Even when IT staff provide him with corroborative evidence for their cases, he may also not understand how to interpret the evidence. According to the specification, it is challenging for an auditor (even for IT experts) to know how to accurately assess the substantive InfoSec risk involved with technical aspects (H-3)."

Even for more professional third-party auditors, there are often time constraints on the completion of the certification within the established timeframe and on the fulfilment of audits. The question of whether sampling methods are appropriate and the fact that the sample size may not be sufficient for the audits can lead third-party auditors to ineffectively assess current InfoSec risks (H-5). A senior manager with an information security background and from the consulting services sector stated:

> "Some accredited ISO 27001 certification bodies have relatively insufficient time to perform the certification, so they usually use a small number of templates to assess the validity of the validation control tasks and then decide whether to issue a certificate or not. This hasty certification process can lead to an insufficient aspect of the actual level of implementation. For example, the auditors' decisions on compliance can be affected by the time constraints. Consequently, an alternative case is that the certification company provide the samples by themselves for the certification body to assess its qualification. In such cases, even though the population doesn't meet the requirement of standards, the auditor will give the organisation an estimate of full compliance based on the samples he has (C-4)."

4.3 Industry differences regarding controls and security standards

InfoSec controls include three different facets, namely, procedures, people and technology (Posthumus and von Solms, 2004). The scope, content and importing methods are covered by different information security standards that are considered differently in design. Consequently, this subsection summarises the interview results regarding the following two topics:

1 the similarities and differences among industries in implementing different types of InfoSec controls

2 differences and complementariness of ISO 27001 and the CIS Controls.

4.3.1 Similarities and differences among industries in adopting different types of InfoSec controls

1 *Procedure controls*

Although the types of risks posed and the magnitude of risks accepted may differ considerably in various industries, the common advantage of implementing ISO 27001 is that a documented management process is explicitly established to clarify the procedures for the operation of the ISMS; therefore, it is easy to facilitate discussion and to comply with the standards. Additionally, through the well-established information system

policies, InfoSec personnel are explicitly required to carry out periodic control self-assessment (CSA) and independent internal audit. As a result, the established ISMS gives an explicit basis for compliance with the standards to the IT staff or employees of all departments. A participant from a manufacturing company stated:

> "Although the scope of certification did not cover company-wide information systems and operating procedures at the beginning of the ISO 27001 implementation, all procedures and activities were still expected to gradually and fully comply with the ISO 27001 requirements. We would gradually expand the ISMS coverage as a way to cope with mounting pressure and requirements from the clients. Adding or reinforcing all control procedures would help strengthen the effectiveness of the information security management (G-2)."

Moreover, the ISO 27001 standard allows organisations to have flexibility to construct their required self-designed control procedures. However, ISO 27001 is generally more applicable to organisations who are at the third (i.e., 'defined') level or above within the Capability Maturity Model (CMM). For the manufacturing or technology industries with their relatively streamlined business processes and frequent changes in organisational structures, the initial adopted procedural controls (e.g., accessible controls or system development) impose increased workloads of documentation tasks on many personnel. These organisations need more time to adapt and to strike a better balance between controls and agility. A bank information security auditor describes it as follows:

> "A financial institution itself is at a more mature stage of the ISMS development; as a result, the most defined technical CIS Controls items have already been implemented. Just the procedures and the clarity of defining the documentation are not yet precisely well-established. More specifically, the ISO 27001 can help us clarify the suitability of control procedures and the definition of documenting the needed records (G-4)."

For the financial industry at more mature CMM levels, the review of procedural changes is more rigorous; the related records of management changes and the controls are also more stringent. Therefore, the relevant procedural controls of implementing ISO 27001 can win relatively higher acceptance. An advantage is that the review of control activities and the documentary definition can help clarify the detailed requirements for relevant personnel with the aid of communication and promotion. Conversely, a disadvantage is that, because the changes in management processes are more difficult and cumbersome, the process design is more prone to rigidity and inflexible to change. This effect substantially reduces the organisation's responding speeds and, ultimately, its operational efficiency. A participant from a manufacturing company said:

> "Because an internal control statement is required, we have to periodically carry out control self-assessment (CSA) including the test of many existing control items. From the perspective of the ISO 27001 risk assessment, the original rules of the existing control items might not meet the suggestions of the latest risk assessment. However, any changes in internal control systems are required to be reviewed and approved by the board directors in advance, so the rigid and inflexible internet control system was the frequent case and the system ultimately become symbolic (G-5)."

2 *Personnel controls*

The results from the coding analysis of interviews indicate that common benefits of introducing ISO 27001 in various industries come from a heightened awareness about InfoSec and the controlled items required to confirm the needed investment to ensure InfoSec within the organisation, including resources and educational training programs. Additionally, improving awareness supports the goal of getting independently certified and, thus, obtaining support from regulators, competent authorities, customers and all corporate stakeholders. Consequently, the risk-based ISO 27001 standards help win management's attention to the project and increase the inputs of people from different departments of the company. An IT supervisor from a manufacturing company stated:

> "Although CIS Controls offer great details in implementation, they involve too much technical controls. Therefore, I believe that CIS Controls do not have much resonance with the senior executives. Conversely, the implementing approach and the level of coverage of the ISO 27001 standards, which focus on the participation of people, make the ISO 27001 standards easier to be understood and recognised by the top management (J-2)."

At the personnel level, however, InfoSec risk awareness differs considerably and the risks of information controls are not easy to measure. As a result, there are key challenges in promoting ISO 27001 resulting from the persistence of security information gathering, security risk communication and subsequent implementation of personnel-related control items. Senior executives' expectations of getting certified within a short period may add pressure to InfoSec personnel to execute the ISRA process and risk responses within a limited timeframe. This unfavourable outcome can be attributed to the limitation of investment resources or the failure of proper resource allocation. In fact, a focus on the short-term goals of certification and reducing the required audit tracking items can reduce the capability of InfoSec safeguards against security incidents, thus reducing the substantial benefits of ISMS implementation.

3 *Technology controls*

Regarding technology controls, respondents from various industries all pointed out that, because the ISO 27001 standard encourages top-down security policies and control procedures of risk management as the core framework, it is a more management-oriented system at a broad and foundational level. The standard lacks sufficient consideration for cyber security or holistic planning guidelines and strategies to defend against cyber-attacks. For example, most financial institutions are exposed to growing external threats with cyber security risk; thus, emphasising regulatory compliance and current internal control procedures is insufficient to fully address InfoSec risks. If the organisation solely addresses the written management procedures for personnel, the focus on internal policies and legal will risk ignoring the real technical risk in complex information systems. A respondent from a manufacturing company stated:

> "From the viewpoint of technical controls, I believe that CIS Controls are much easier to be understood than ISO 27001 standards are. The framework of CIS controls is clearer than that of ISO 27001 standards as well. The vagueness of ISO 27001 standards often leads to great difficulty in planning and deploying the overall technical aspects. As a result, to understand the details of implementing ISO 27001 standards, you have to consult the innumerable volumes of ISO 27001 instructions as a reference of how to act or to do the job.

> In consideration of the operating guidance, I regard the core control items of CIS controls, which are much more concise and systematic, as the advantage of CIS controls which provide relatively more clear instructions for users in general (J-1)."

Conversely, manufacturing companies with relatively insufficient resources and at the initial stage of ISMS implementation are usually unsure how to comply the ISO 27001, which does not have a clear definition or guidelines on technical details. Thus, they depend on other InfoSec guidelines or standards in conjunction with ISO 27002 documentation, or they seek technical support from experienced InfoSec consultants. However, if the investing resources are limited or if corporate executives regard the obtainment of the ISO 27001 certification as the main goal of the ISMS implementation, the InfoSec department may suffer investment restraints on technical controls or long delays in prioritising the necessary improvement of technical controls. An InfoSec supervisor from a manufacturing company described this issue as follows:

> "Since the technical aspects are still at the early stage of implementation, the capability of handling the relevant controls is still relatively insufficient. Therefore, the operations are less likely to face problems related to the aspect of implementing procedures. However, for the perspective of technology, we still need the external consultants to give more specific checklists or technical instructions because, even if the operating systems are the same, the difference in control targets can lead to differences in the system setting as well. In addition, the limitation of initial investment resources at implementing stage leads to merely obtain the ISO 27001certification as the primary goal of adopting the ISO 27001; therefore, insufficient resources to establish the necessary technical controls are resulted in the end (H-4)."

4.3.2 Complementariness of various InfoSec standards

On the basis of our interview questions, we compare ISO 27001, which mainly focus on risk management, with the CIS Controls, which seriously consider the core technology controls, including order of priority, for cyber security protection. Interviewees were invited to comment critically on the different InfoSec standards as a way to help better understand the distinction between the two, including promotion of control implementation with management and technical aspects.

The ISO 27000-series standards consider risk management as the framework of implementation, focuses on an organisation's risk management procedures to discuss and analyse InfoSec risks, provides principles for building an ISMS, helps organisations manage and protect their information assets, and ensures that the security expectations of customers and stakeholders are satisfied. However, it does not provide any explicit instructions or details for the InfoSec control items. Most InfoSec consultants often recommend their clients simultaneously adopt the ISO 27002 guidelines as a reference document for implementing the ISO 27001 control items.

Currently, as the versions are updated, the inclusive control items of most InfoSec standards gradually increase, adding to the burden of implementation. Additionally, management-based information security standards examine the effectiveness and residual risks of the information security protection with each control item. By contrast, when the CIS Controls were originally designed, they considered the highest-impact issues rather than aiming for completeness. The CIS Controls focus on a smaller number of actionable controls with high payoff, aiming for a 'must do first' philosophy. These actionable

control items have step-by-step explicit instructions to create a security infrastructure powerful enough to keep hackers out of networks and systems. Linking all critical controls will enable a more effective and integrated system than simply complying with a couple of diverse controls with overlapping regulatory requirements.

Although the CIS Controls have the aforementioned advantages, respondents raised concerns about its implementation. Because financial institutions are generally at a higher ISG maturity level, their investments in the technical aspect of related controls are typically quite sufficient (K-1). Enterprises usually implement the ISMS with the expectation of enhancing customers' trust by obtaining ISO 27001 certification. Consequently, respondents working at financial institutions showed a strong preference for ISO 27001 adoption from this perspective. Moreover, the CIS Controls are more technology-oriented than management-oriented, so it is difficult for corporate executives to assess the effectiveness of implementing the CIS Controls. This raises many hurdles to obtaining support from top management (K-2). A respondent from a consulting service provider stated:

> "I believe that, unlike ISO 27001 standards, CIS Controls are considered a more explicit framework of InfoSec standards and their recommended control items are relatively clear for adoption, thus making the implementation of CIS Controls more smooth. However, a portion of their control items may have the problem of suitability so proper adjustments (modifications) are needed to accommodate the different consideration of organisations' specific industries and of their peculiar demands for the implementation of CIS Controls (K-1)."

Synthesising results from participants in the finance sector, we found that a disadvantage of implementing the CIS Controls is that they give organisations less managerial guidance on how to evaluate investment in technological resources. Although an explicit framework of technical guidance for InfoSec staff is very helpful, the specific requirements for technology controls are not conducive to personnel communication among different organisational departments. However, there is also the possibility of reducing the scope of implementation and to regard InfoSec as the technical task of a single InfoSec unit. This is ultimately less likely to win support and funding from corporate executives. An InfoSec auditor of a manufacturing company pointed out:

> "The drawback of CIS Controls is that, in comparison with ISO 27001 standards, CIS Controls do not have much resonance with the senior executives. The corporate executives are more likely to regard the CIS Controls items as the highly relevant IT items and believe that the IT departments should bear full responsibility to do their tasks. As a result, the executives are not likely to invest any extra efforts and resources to promote the CIS Controls (K-2)."

By contrast, from the perspectives of the manufacturing and consulting services sectors, the CIS Controls provide a technical guideline with a set of 20 controls and 171 sub-controls and give implementers detailed recommendations to follow in a series of phases as well as support for how to choose suitable controls from the self-selected sub-grouping of the CIS Controls hierarchy. The detailed itinerary of planning and implementation of technology controls given by the CIS Controls is relatively clear and more in depth than that given by the ISO 27001 (J-1, J-2). The CIS Controls favourably facilitate the more rapid adoption of InfoSec controls and explicitly define a systematic approach and prioritisation. Regarding update frequency, the CIS Controls annually make detailed adjustments based on the latest threat trends determined by experts through voting and

discussion. As a result, the guidelines of the CIS Controls are immediate (J-3) and can be used to prioritise emergent InfoSec issues. The content of the CIS Controls, unlike that of ISO 27001, provides detailed information and can be adjusted according to organisation sizes (J-4). A respondent from a consulting services provider stated:

> "The continuity of assistance from both the external auditors and the consultants is needed during the subsequent investments of resources as a way to gradually improve the systems. In this case, CIS Controls are considered an excellent entry point of investments because the sequences (steps) of their framework implementation, the causality between control items, and the importance of related to items are clearly described in their instructions (J-4)."

However, interviewees noted that, unlike the breadth of the ISO 27001 controls, which are more complete (K-3), the CIS Controls capture major issues but are incomplete. In addition, the CIS Controls do not have the feature of independent certification, which gives the organisation external recognition (K-4). Mapping items from both the CIS Controls and ISO 27001, we found that, although the CIS Controls mostly have control items corresponding to the ISO 27001 controls, but the CIS Controls are more simple and only cover some of the ISO 27001 control scopes. In other words, only importing all CIS Controls alone can rapidly and significantly reduce security risks, but this will not fully meet the ISO 27001 certification requirements. An InfoSec auditor from a manufacturing firm stated:

> "In comparison of both InfoSec frameworks, ISO 27001 standards provide implementers with a wide-covered scope of targets but without explicit instructions whereas CIS Controls help IT technicians clearly understand their specific objectives and practices, but CIS Controls do not cover all projects (items) in the ISO 27001 standards (K-3)."

5 Conclusion

5.1 Summary of research results

This study explored the main factors affecting the adoption of ISO 27001 certification, the most important drivers for effectiveness of implementing the ISMS, and the determinants of how organisations seek complementary support and guidelines from different InfoSec standards and frameworks. The main findings of this study are summarised as follows.

First, the main factors for the adoption of the ISO 27001 certifications come from a need to comply with the thrust of regulations to avoid penalties for regulatory violations, a necessary response to customers' requirements to enhance their trust as a way to boost business, and a clear endorsement of funding and consideration from corporate executives who sense that the benefits of adopting the ISO 27001 system far outweigh the costs of the project. Second, the effectiveness of implementing the ISMS was driven by effective risk communication that takes the critical aspects for the ISRA process, risk mitigation, incident response plans and continuous improvement tracking, experienced consultants who have the ability to translate InfoSec risks into real business terms to help strengthen organisational management systems, a heightened employee awareness of

InfoSec risks and internal auditors' professional competence to complete diverse internal audit projects, noting that internal auditors are usually unfamiliar with the technical details.

We considered differences in various industries regarding the ISO 27001 standards. Regarding procedure controls, ISO 27001 gives a well-documented management process to clarify the procedures for the operation of the ISMS, comply with the standards and allow organisations to construct self-designed control procedures. However, ISO 27001 is more applicable to organisations at the third or above CMM level and so for manufacturing or technology industries with relatively streamlined business processes, the initially adopted procedure controls actually impose increased workloads of documentation tasks. For the more mature financial industry, the review of control activities and the documentary definition can help clarify the detailed requirements to assist communication and promotion, but the process design is more prone to rigidity and more inflexible to change.

For personnel controls, the common benefits of ISO 27001 introduction in various industries come from a heightened awareness about InfoSec and the required control items to confirm the needed investment in InfoSec within the organisation, including resources and educational training programs. However, senior executives' short-sightedness of aiming to quickly obtain certification can lead to limitation of investment resources, failure of proper resource allocation and reduced capability of InfoSec safeguards against security incidents, decreasing the benefits of ISMS implementation.

For technology controls, the core framework of the ISO 27001 is the top-down security policies with many diverse control scopes and objectives with concise descriptions. Thus, the system is management-oriented at a broad and foundational level, and has insufficient consideration of cyber security or holistic planning and approaches to prevent cyber-attacks. For example, most financial institutions at a more mature CMM stage are exposed to growing external threats with cyber security risk. Conversely, manufacturing companies with relatively insufficient resources are usually confused about how to comply with ISO 27001 and they either depend on other InfoSec guidelines or standards in conjunction with the ISO 27001 documentation or seek technical support from experienced InfoSec consultants. The focus on quick certification typically leads to the imposition of investment restraints on technical controls or long delays in prioritising the necessary improvement of technical controls.

Finally, we performed a comparative analysis of two key InfoSec standards. The ISO 27001 series regards risk management as the framework of implementation, focuses more on an organisation's risk management procedures, provides principles for building the ISMS, helps organisations protect their information assets and aims to satisfy the security expectations of customers and stakeholders. However, the ISO 27001 system does not provide any explicit instructions for InfoSec items. On the other hand, the CIS Controls focus on a smaller number of actionable controls with high payoff, aiming for a 'must do first' philosophy and with step-by-step explicit instructions to create a security infrastructure powerful enough to keep the hackers out of networks and systems. However, the CIS Controls are more technology-oriented than management-oriented so it is difficult for corporate executives to assess the effectiveness of adopting the CIS Controls. This can lead to executives imposing investment restraints on the CIS projects. Financial institutions with a higher ISG maturity level may have already sufficient investment in technical controls. By contrast, in the manufacturing and consulting services sectors, the CIS Controls give implementers detailed recommendations with

phases to help them choose suitable controls from the CIS Controls hierarchy, help facilitate the more rapid adoption of InfoSec controls and provide an immediate signal of threat trends for organisations to prioritise emergent InfoSec issues. Although adopting the CIS Controls alone can significantly reduce security risks, they do not have the benefits of certification. Thus, integration of the ISO 27001 certification and the CIS Controls is a promising approach.

5.2 Recommendations and contributions

The ISO 27001 system provides independent certification for an organisation to obtain verification from regulators, competent authorities, customers and all corporate stakeholders, boosting business, whereas the CIS Controls give immediate signals of the latest threat trends to be prioritised as a 'must do first' project. The integration of both systems would result in the most benefits for organisations in various industries. Although financial institutions have higher ISG maturity and sufficient investment in technical controls, they are still exposed to growing external threats with cyber security risks. Thus, we suggest that organisations should be able to achieve best practices of IT governance and IT security by integrating ISO 27001 certification and the CIS Controls as a way to properly implement information systems and effectively reinforce InfoSec.

To the best of our knowledge, this study represents the first investigation of the overall performance of implementing the ISO 27001 certification and the CIS Controls in Taiwanese organisations. Our findings could have implications for InfoSec system implementers and service providers. The implementers may design or identify a suitable InfoSec program by taking the benefits and drawbacks of each system into consideration to make informed decisions on projects. Service providers may get the most relevant information to design suitable services for their clients that would boost business.

5.3 Limitations and future research

A potential limitation of this study is that results from the small sample size of fourteen participants and time available for interviews might not be representative of the overall population, and thus the results may not be fully generalisable. Future research may use a pragmatic approach that combines qualitative and quantitative data gathering to substantially increase the sample size and encourage a richer understanding of the performance of InfoSec programs.

Another possible limitation is that some respondents had insufficient knowledge and experience about the CIS Controls. Future research may design a sophisticated experiment to first educate participants about the CIS Controls and then invite them to critically comment on the difference between the two standards. The comparative analysis of the results would be more accurate if more participants had sufficient knowledge to make a meaningful comparison between the two standards.

The last avenue for future research is a two-step process of creating budgets for various projects, each integrated with a different number of standards, and then comparing the costs between budgets. The results from this cost-effective analysis would be very useful in assisting implementers to make value-based informed decisions when budgeting for their InfoSec projects.

References

AlGhamdi, S., Win, K.T. and Vlahu-Gjorgievska, E. (2020) 'Information security governance challenges and critical success factors: systematic review', *Computers and Security*, Vol. 99, December, pp.1–39.

Boehmer, W. (2008) 'Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001', *Paper Presented at the 2008 Second International Conference on Emerging Security Information, Systems and Technologies*, Sep, Cap Esterel, France, IEEE, pp.224–231, DOI: 10.1109/SECURWARE.2008.7.

Burgers, T., Hellmann, M. and Romaniuk, S.N. (2021) 'In the line of fire: Taiwan's legal, political, and technological cybersecurity posture', *Routledge Companion to Global Cyber-Security Strategy*, Routledge, pp.276–283.

Calder, A. (2016) *Nine Steps to Success: An ISO27001: 2013 Implementation Overview*, 3rd ed., IT Governance Ltd., UK.

Corbin, J. and Strauss, A. (1990) 'Grounded theory research: procedures, canons, and evaluative criteria', *Qualitative Sciology*, Vol. 13, No. 1, pp.3–21.

Corbin, J. and Strauss, A. (2014) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Los Angeles.

Diamantopoulou, V., Tsohou, A. and Karyda, M. (2019) 'From ISO/IEC 27002: 2013 information security controls to personal data protection controls: guidelines for GDPR compliance', *Computer Security*, Springer, Switzerland, ESORICS 2019 Workshops, pp.238–257, https://doi.org/10.1007/978-3-030-42048-2_16

Flores, W.R., Antonsen, E. and Ekstedt, M. (2014) 'Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture', *Computers and Scurity*, Vol. 43, June, pp.90–110.

Fomin, V.V., Vries, H. and Barlette, Y. (2008) 'ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption', *Paper Presented at the Euromot 2008 Conference*, Nice, France, pp.1–13, https://hdl.handle.net/20.500.12259/37814

Gillies, A. (2011) 'Improving the quality of information security management systems with ISO27000', *The TQM Journal*, Vol. 23, No. 4, pp.367–376.

Gioia, D.A., Corley, K.G. and Hamilton, A.L. (2013) 'Seeking qualitative rigor in inductive research: notes on the gioia methodology', *Organizational Research Methods*, Vol. 16, No. 1, pp.15–31.

Glaser, B.G. and Strauss, A.L. (2017) *Discovery of Grounded Theory: Strategies for Qualitative Research*, Routledge, New York.

Groš, S. (2019) *A Critical View on CIS Controls*, arXiv preprint arXiv: 1910.01721.

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021) 'Evaluating the cyber security readiness of organizations and its influence on performance', *Journal of Information Security and Applications*, Vol. 58, p.102726 [online] https://www.sciencedirect.com/science/article/pii/S2214212620308656 (Accessed 15 June, 2021).

Hong, K.S., Chi, Y.P., Chao, L.R. and Tang, J.H. (2003) 'An integrated system theory of information security management', *Information Management and Computer Security*, Vol. 11, No. 5, pp.243–248.

Hsu, C., Wang, T. and Lu, A. (2016) *The Impact of ISO 27001 Certification on Firm Performance. Paper Presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS)*, March, Koloa, Hawaii, pp.4842–4848, DOI: 10.1109/HICSS.2016.600.

Hussain, A., Mohamed, A. and Razali, S. (2020) 'A review on cybersecurity: challenges and emerging threats', *Paper Presented at the Proceedings of the 3rd International Conference on Networking, Information Systems and Security*, March, New York, USA, pp.1–7, https://doi.org/10.1145/3386723.3387847

Ifinedo, P. (2014) 'Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition', *Information and Management*, Vol. 51, No. 1, pp.69–79.

Kirk, N. and van Staden, C. (2001) 'The use of grounded theory in accounting research', *Meditari Accountancy Research*, Vol. 9, No. 1, pp.175–197.

Knapp, K.J., Marshall, T.E., Rainer, R.K. and Ford, F.N. (2006) 'Information security: management's effect on culture and policy', *Information Management and Computer Security*, Vol. 14, No. 1, pp.24–36, https://doi.org/10.1108/09685220610648355.

Mataracioglu, T. and Ozkan, S. (2011) *Governing Information Security in Conjunction with COBIT and ISO 27001*, arXiv preprint arXiv: 1108.2150.

Mirtsch, M., Kinne, J. and Blind, K. (2020) 'Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis', *IEEE Transactions on Engineering Management*, Vol. 68, No. 1, pp.87–100.

Parker, L.D. and Roffey, B.H. (1997) 'Methodological themes: back to the drawing board: revisiting grounded theory and the everyday accountant's and manager's reality', *Accounting, Auditing and Accountability Journal*, Vol. 10, No. 2, pp.212–247.

Posthumus, S. and von Solms, R. (2004) 'A framework for the governance of information security', *Computers and Security*, Vol. 23, No. 8, pp.638–646.

Roy, P.P. (2020) 'A high-level comparison between the NIST cyber security framework and the ISO 27001 information security standard', *Paper Presented at the 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, February, Durgapur, India, IEEE, pp.1–3, DOI: 10.1109/NCETSTEA48365.2020.9119914.

Schweizerische, S. (2013) *Information Technology-Security Techniques-Information Security Management Systems-Requirements*, ISO/IEC International Standards Organization.

Security, I. and C.f (2019) *CIS Controls, Version 7*.1, 2019 ed., Retrieved from http://www.cis.org

Shariffuddin, N. and Mohamed, A. (2020) 'IT security and IT governance alignment: a review', *Paper Presented at the Proceedings of the 3rd International Conference on Networking, Information Systems and Security*, March, New York, USA, pp.1–8, https://doi.org/10.1145/3386723.3387843

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: a literature review', *International Journal of Information Management*, Vol. 36, No. 2, pp.215–225.

Terlaak, A. and King, A.A. (2006) 'The effect of certification with the ISO 9000 quality management standard: a signaling approach', *Journal of Economic Behavior and Organization*, Vol. 60, No. 4, pp.579–602.

Veiga, A.D. and Eloff, J.H. (2007) 'An information security governance framework', *Information Systems Management*, Vol. 24, No. 42, pp.361–372.

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P. and Moscoso-Zea, O. (2018) 'Benefits of implementing an ISMS according to the ISO 27001 standard in the Ecuadorian manufacturing industry', *Paper Presented at the 2018 International Conference on Information Systems and Computer Science (INCISCOS)*, November, Quito, Ecuador, pp.294–300, DOI: 10.1109/INCISCOS.2018.00049.

von Solms, B. (2005) 'Information security governance: COBIT or ISO 17799 or both?', *Computers and Security*, Vol. 24, No. 2, pp.99–104.

von Solms, S.B. (2005) 'Information security governance–compliance management vs operational management', *Computers and Security*, Vol. 24, No. 6, pp.443–447.

White, D.M. (2010) 'The federal information security management act of 2002: a Potemkin village', *Fordham L. Rev*., Vol. 79, p.369.