Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standards

Book · July 2020

DOI: 10.1201/9781315232355

2 authors:

Heru Susanto
Indonesian Institute of Sciences
135 PUBLICATIONS 774 CITATIONS

Mohammad Nabil Almunawar
Universiti Brunei Darussalam
143 PUBLICATIONS 1,907 CITATIONS

Information Security Management Systems

A Novel Framework and Software as a Tool for Compliance with Information Security Standards

Heru Susanto | Mohammad Nabil Almunawar

AAP APPLE ACADEMIC PRESS

CRC Press
Taylor & Francis Group

INFORMATION SECURITY MANAGEMENT SYSTEMS

A Novel Framework and Software as a Tool for Compliance with Information Security Standards

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

INFORMATION SECURITY MANAGEMENT SYSTEMS

A Novel Framework and Software as a Tool for Compliance with Information Security Standards

Heru Susanto, PhD

Mohammad Nabil Almunawar, PhD

AAP
APPLE
ACADEMIC
PRESS

Apple Academic Press Inc.
3333 Mistwell Crescent
Oakville, ON L6L 0A2 Canada

Apple Academic Press Inc.
9 Spinnaker Way
Waretown, NJ 08758 USA

Exclusive worldwide distribution by CRC Press, a member of Taylor & Francis Group
No claim to original U.S. Government works
International Standard Book Number-13: 978-1-77188-577-5 (Hardcover)
International Standard Book Number-13: 978-1-315-23235-5 (eBook)

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission and sources are indicated. Copyright for individual articles remains with the authors as indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the authors, editors, and the publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors, editors, and the publisher have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged, please write and let us know so we may rectify in any future reprint.

Trademark Notice: Registered trademark of products or corporate names are used only for explanation and identification without intent to infringe.

Library and Archives Canada Cataloguing in Publication

Susanto, Heru, 1965-, author
Information security management systems : a novel framework and software as a tool for compliance with information security standards / Heru Susanto, PhD, Mohammad Nabil Almunawar, PhD.

Includes bibliographical references and index.
Issued in print and electronic formats.
ISBN 978-1-77188-577-5 (hardcover).--ISBN 978-1-315-23235-5 (PDF)

1. Management information systems--Security measures.
2. Industries--Security measures--Management. 3. Risk assessment.
I. Almunawar, Mohammad Nabil, author II. Title.

HD61.5.S87 2017 658.4’78 C2017-905895-9 C2017-905896-7

CIP data on file with US Library of Congress

Apple Academic Press also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic format. For information about Apple Academic Press products, visit our website at **www.appleacademicpress.com** and the CRC Press website at **www.crcpress.com**

CONTENTS

ABOUT THE AUTHORS

Heru Susanto, PhD
Head and Researcher, Computational Science & IT Governance Research Group, Indonesian Institute of Sciences; Honorary Professor and Visiting Scholar at the Department of Information Management, College of Management and Hospitality, Tunghai University, Taiwan

Heru Susanto, PhD, is currently the head and a researcher of the Computational Science & IT Governance Research Group at the Indonesian Institute of Sciences. He is also an Honorary Professor and Visiting Scholar at the Department of Information Management, College of Management and Hospitality, Tunghai University, Taichung, Taiwan. Dr. Heru has experience as an IT professional and as web division head at IT Strategic Management at Indomobil Group Corporation. He has worked as the Prince Muqrin Chair for Information Security Technologies at King Saud University in Riyadh, Saudi Arabia. He received a BSc in Computer Science from Bogor Agricultural University, an MBA in Marketing Management from the School of Business and Management Indonesia, an MSc in Information System from King Saud University, and a PhD in Information Security System from the University of Brunei and King Saud University. His research interests are in the areas of information security, IT governance, computational sciences, business process re-engineering, and e-marketing.

Mohammad Nabil Almunawar, PhD

Senior Lecturer and Dean, School of Business and Economics, University of Brunei Darussalam (UBD), Brunei

Mohammad Nabil Almunawar, PhD, is currently a senior lecturer and the Dean of the School of Business and Economics, University of Brunei Darussalam (UBD), Brunei Darussalam. Dr. Almunawar has published more than 60 papers in refereed journals, book chapters, and presentations at international conferences. He has more than 25 years of teaching experience in the area of computer and information systems. His overall research interests include applications of IT in management, electronic business/commerce, health informatics, information security, and cloud computing. He is also interested in object-oriented technology, databases and multimedia retrieval.

Dr. Almunawar received his bachelor degree in 1983 from Bogor Agricultural University, Indonesia; his master's degree (MSc in Computer Science) from the Department of Computer Science, University of Western Ontario, London, Canada, in 1991, and a PhD from the University of New South Wales (School of Computer Science and Engineering, UNSW), Australia, in 1998.

LIST OF ABBREVIATIONS

5S2IS	five stages to information security
8FPs	eight fundamental parameters
9STAF	nine state of the art framework
ADODB	ActiveX Data Object DataBase
BAU	business as usual
BoD	Board of Directors
BoM	Board of Managers
BS	British Standard
CIA	Confidentiality Integrity Authority
CMM	capability maturity model
CMMI	capability maturity model integration
CNSS	Committee on National Security Systems
COBIT	control objectives for information and related technology
COM	component object model
COSO	Committee of Sponsoring Organizations
DCOM	distributed component object model
DDoS	distributed denial of service attacks
DMZ	demilitarized zone
ECs	essential controls
ENISA	European Network and Information Security Agency
FGD	focus group discussion
FGIS	The Framework for the Governance of Information Security
GISPF	The Government Information Security Policy Framework
GUI	graphical user interface
ICM	implementation checklist method
ICT	Information and Communication Technology
IEC	International Electronic Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	internet protocol
IPR	intellectual property right

IRM	information risk management
IS	information systems
ISA	information security awareness
ISACA	Information Systems Audit and Control Association
ISBS	Information Security Breaches Survey
ISF	integrated solution framework
ISM	Integrated Solution Modeling Software
ISMS	Information Security Management System
ISO	International Standard Organization
ISP	internet service provider
ITG	Information Technology Governance
ITGA	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
ITMO	Information Technology Manager and Officer
ITSCM	Information Technology Service Continuity Management
ITSM	Information Technology Services Management
MISA	Multimedia Information Security Architecture
NIST	National Institute of Standard and Technology
OCX	object linking and embedding control extension
OLE	object linking and embedding
OPM3	organizational project management maturity model
P-CMM	people capability maturity model
PCIDSS	Payment Card Industry Data Security Standard
PDCA	Plan Do Check Action
PMBOK	project management body of knowledge
PMC	Prince Muqrin Chair for Information Security Technologies
PMMM	project management maturity model
PRINCE2	Projects in Controlled Environments – Version 2
PWC	Price Waterhouse Cooper Consultants
QGIA	Queensland Governance of Information Assurance
QGISPF	Queensland Government Information Security Policy Framework
REM	release and evaluation methodology
RISC	readiness and information security capabilities
RM	research methodology

RMA	release management approach
SAM	security assessment management
SDA	spiral development approach
SDLC	Software Development Life-Cycle
SEPG	Software Engineering Process Group
SIEM	security information and event management
SIM	security information management
SMM	security monitoring management
SOA	service oriented architecture
SoA	statement of applicability
SP	software performance
SPP	software performance parameter
SQ	software quality
SQL	structure query language
SSAD	Security Systems Analyst and Developer
STOPE	Stakeholder Technology Organization People Environment
TCP	transmission control protocol
TOGAF	The Open Group Architecture Framework
URS	user requirement specification
VB	Visual Basic
VOOP	visual object oriented programming
WFA	waterfall approach
WSP-SM	waterfall software process-spiral model development

LIST OF TABLES

LIST OF FIGURES

PREFACE

Information security contributes to the success of organizations, as it gives a solid foundation to increase both efficiency and productivity. Many business organizations realize that compliance with the information security standards will affect their business prospects. Securing information resources from unauthorized access is extremely important. Information security needs to be managed in a proper and systematic manner as information security is quite complex. One of the effective ways to manage information security is to comply with an information security management standard. There are a number of security standards around; however, ISO 27001 is the most widely accepted one. Therefore, it is important for an organization to implement ISO 27001 to address information security issues comprehensively. Unfortunately, the existing ISO 27001 compliance methods are complex, time consuming and expensive. A new method, preferably supported by an automated tool, will be much welcomed.

One of the key components for the success of information security certification is by using a framework. This framework acts as a tool to understand the process and technical aspects. Unfortunately, existing frameworks do not provide fixed and practical models for RISC (Readiness and Information Security Capabilities) investigation, which is investigation conducted to find out an organization's readiness and information security capabilities regarding ISO 27001.

This study proposes a novel framework called the Integrated Solution for Information Security Framework (ISF). ISF was developed to tackle issues that are not properly addressed by existing security frameworks for RISC investigation and provides an easy and practical model for information system security according to ISO 27001. Based on ISF, a semi-automated tool is developed to assess the readiness of an organization to comply with ISO 27001 and subsequently use the tool to assess the potential threats, strengths and weaknesses for efficient and effective implementation of ISO 27001. This tool is called Integration Solution Modeling Software (ISM), which is based on ISF, to assist organizations in measuring the level of compliance of their information systems with ISO 27001. The software consists of two major modules: e-assessment to assess the level of compliance with ISO 27001; and e-monitoring to monitor suspected activities that may lead to security breaches.

ISM provides the ability to enhance organizations beyond usual practices and offers a suitable approach to accelerate compliance processes for information security. ISM brings a possibility to enhance organizations by enabling them to prepare for the processes of security standardization by conducting self-assessment. A new approach in ISM helps organizations improve their compliance processes by reducing time, conducting RISC self-assessment, handling SoA preparation, monitoring networks, and suspect detection monitoring.

To see the effectiveness of ISF and ISM, we conducted a comprehensive ISM testing and evaluation. The result is very promising as ISM is highly regarded and accepted as a useful tool to help companies systematically plan to acquire ISO 27001 certification. User responses towards the performance, quality, features, reliability, and usability (called by eight fundamental parameters – 8FPs) are high. Overall score according to 8FPs is 2.70 out of 4, which means close to "highly recommended." ISM performs RISC investigation within 12 hours, which is much better then implementation a checklist method (ICM – the currently existing method to measure RISC level in the organization) approaches that require approximately 12 months for the investigations. This means that our framework is effective, and certainly its implementation is useful for organization to assess their compliance with ISO 27001 and to set a clear strategy to obtain ISO 27001 certification with confidence.

COMMENTARIES

Comments on published papers from academicians, editors, and professionals are delineated below. Those papers are part of this work.

"I recommend this work on this topic. The authors have lots of knowledge, and the topic is important. Security in IT usually is access controlled and consists of authentication and authorization."

—Prof. Dr. Günter Müller
Institute of Computer Sciences and Social Studies,
Department Telematics,
University of Freiburg, Germany

"We consider the content and your approach very valuable. We came to the conclusion that the level of knowledge you have lead to a good chance to overcome the hurdles of the next steps. We are confident with your work will have the chance to become a really appreciated contribution to the scientific and practical IS community."

—Prof. Dr. Martin Bichler
Department of Informatics,
Technische Universität München, Germany

CHAPTER 1

INTRODUCTION

CONTENTS

1.1 STUDY OVERVIEW

We are living in the information age, where information and knowledge are becoming increasingly important and no-one denies that information and knowledge are important assets that need to be protected from unauthorized users such as hackers, phishers, social engineers, viruses, and worms that threaten organizations on all sides, through intranet, extranet, and the Internet. The rapid advancement of information and communications technology (ICT) and the growing dependence of organizations on ICT continuously intensify concern on information security (Von Solms, 2001). Although, most ICT systems are designed to have a considerable amount of strength in order to sustain and assist organizations in protecting information from security threats, they are not completely immune from the threats (Furnell, 2005). Organizations pay increasing attention to information protection as the impact of information security breaches today have a more tangible effect (Dlamini et al., 2009; Furnell et al., 2006; Furnell & Karweni, 1999).

Cherdantseva et al. (2011) and Pipkin (2000) looked at information security from the business standpoint and argued that information security needs to be considered as a business enabler and become an integral part of business processes. Von Solms (2005), Tsiakis & Stephanides (2005), and Pipkins (2000) stated that information security may help to raise trust in an organization from customers and it should be understood that security of information brings many advantages to business (e.g., improved efficiency due to the exploitation of new technologies and increased trust from partners and customers). Saint-Germain (2005) argued that an important driver for information security management system adoption is to demonstrate to partners that the company has identified and measured their security risks, implemented a security policy and controls that will mitigate these risks, also to protect business assets in order to support the achievement of business objectives (Boehmer, 2008; Dhillon, 2007; Furnell et al., 2006; Saleh et al., 2007a, 2007b).

Cherdantseva & Hilton (2013), and Sherwood et al. (2005) adopted a multidimensional and enterprise-wide approach to information security and proposed to include a wider scope of information security covering various aspects of business such as marketing and customer service. Information security is no longer considered purely from a technical perspective, but also from a managerial, system architect's and designer's points of view and it could enable businesses to increase competitiveness (Sherwood et al., 2005), economic investment (Anderson, 2001; Gordon & Loeb, 2002; Tsiakis & Stephanides, 2005), products or services to world markets transparently and in compliance with prevalent standards, such as ISO 27001 and ISO 17799 (Theoharidou et al., 2005).

It is clear that information security needs to be managed properly as related issues are quite complex. Several information security management system standards were developed to assist organizations in managing the security of their information system assets. It is important to adopt an information security management system (ISMS) standard to manage the security of organization's information assets effectively. In contrast, Standish Group (2013) stated that many ICT projects in the US, including ISMS standardizing and ISO 27001 compliance in major organizations, faced difficulties, with many having reported failure and only around one in eight (13%) ICT projects attempting to standardize information security were successful. Othman et al. (2011), and Fomin et al. (2008) stated that technical barriers, the project owner's 'absence of understanding processes, technical aspects, lack of internal ownership and neglect of certain aspects were major problems that caused the delay for these ISMS and ISO 27001 projects. An organization may face challenges in implementing an ISMS standard without proper planning, and any obstacles could create roadblocks for effective information security adoption (Kosutic, 2010, 2013), such as:

- *Financial issues*. At first sight, it may seem that paperwork should not cost too much, until the stakeholder realizes that they have to pay for consultants, buy literature, train employees, invest in software and equipment.
- *Human resources issues*. The expertise dedicated to implement ISMS is unavailable.
- *Participation issues*. An ISMS adoption project may be seen as solely the initiative of an ICT department rather than the engagement of the entire organization.
- *Communications issues*. Lack of proper communication at all levels of the organization during the ISMS certification process.
- *Technical issues*. Translation of the technical terms and concepts of a chosen ISMS standard is required. Essential controls dealing with the standard are very technical and will not be readily understood by the board of management as decision maker, making it difficult to be implemented by an organization. Therefore, those terms need to be refined, otherwise the controls will tend to be somewhat disorganized and disjointed.
- *Selection and adoption issues*. Difficulty in selecting a suitable ISMS standard for related organizations. There are several standards for IT Governance which lead to information security such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO 27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT. It indicates that an organization has to choose the best standard that is suitable for their business processes and also well-recognized by their partners, clients, customers, and vendors.

As mentioned above, several challenges arise when implementing the standard. One of the key components to understanding the process and technical aspects is by using a framework to support ISMS and ISO 27001 projects. Although the development of ICT security frameworks has gained momentum in recent years, more work on approaches to security framework are still needed, as the current frameworks do not provide measurements to assess the readiness level of organizations to adopt an ISMS standard (Calder & Watkins, 2012; Calder et al., 2010; Fomin et al., 2008; Potter & Beard, 2010).

To fill the gap, this study proposes a novel approach and develops a system that can measure the closeness of an organization's information security status with an ISMS standard (a compliance level). This framework is designed in such a way to derive an integrated solution to overcome the organization's technical barriers and difficulties in understanding, investigating, and complying with an ISMS standard (ISO 27001). This framework, called Integrated Solution Framework (ISF), helps organizations map the assessment issues, controls, and clauses of ISO 27001 to its related domain and acts as a measurement tool for assessing the information security compliance level of organizations toward ISO 27001.

ISF consists of 6 main components identified as domains, namely: organization (domain 1), stakeholders (domain 2), tools & technology (domain 3), policy (domain 4), culture (domain 5), knowledge (domain 6). Those are associated with the critical components within an organization that relates to information security circumstances, and further ISO 27001 compliance stages. The explanations for each domain are expanded in Chapter 4: Proposed Framework.

Based on ISF, the assessment and monitoring software was developed, called Integrated Solution Modeling (ISM). This software measures the RISC[1] level of an organization towards ISO 27001, analyzes security events in real time, and collects, stores, and reports for regulatory compliance. The software has two main functions:

1. Security assessment management (SAM/e-Assessment). Log management and compliance reporting. SAM provides the collection, reporting and analysis of assessment data that will show the

[1] Readiness and Information Security Capabilities

strength and weakness points and increase priority on low achievement points to support regulatory compliance.

2. Security monitoring management (SMM/e-Monitoring). SMM monitors real-time activity, firewall and network management to provide monitoring and identify potential security breaches. ISM collects network activity data in real time so that immediate analysis can be done.

To make sure the effectiveness of the framework (ISF) and its implementation (ISM) in assisting organizations, we conducted comprehensive testing on the reliability, usability, and performance in respondent organizations in the field of telecommunications, banking & finance, airlines, and ICT-security consultancy. The results of the testing and evaluation were further analyzed using software performance parameters (SPP) and release and evaluation management (REM) to find out the software performance, features and quality, to obtain a RISC measurement (Bakry, 2003a, 2003b; Herbsleb et al., 1997). There are eight defined parameters to measure the performance and features of the framework and software (Bakry 2001, 2004; Gan, 2006; McCall et al., 1977a, 1977b) as follows: (1) How ISM functions in information security self-assessment; (2) The benefits brought by ISM in helping organizations understand ISMS standard (ISO 27001) controls; (3) How ISM can be used to find out information security terms and concepts; (4) ISM features; (5) ISM graphical user interface and user friendliness; (6) Precision of the analysis produced by ISM; (7) Final result precision produced by ISM; (8) ISM performance.

1.2 THE SCOPE OF THE PROBLEM AND MOTIVATIONS

There are many important questions associated with organizations and security standards in relation to security awareness and compliance. This study proposes a framework as a solution for the technical aspects of the research questions:

1. What are the main barriers in implementing ISMS within an organization?
2. What are the differences between existing state-of-the-art frameworks and solutions to formal and quantitative investigation of RISC parameters, and what are their weaknesses?

3. How significant the proposed framework will reduce the learning and preparation time as the organization enhances itself for ISO 27001 compliance?
4. What are the main advantages for an organization in self-assessing using ISM to obtain the RISC measurement regarding ISO 27001 certification?

The motivation of this study is to improve the overall ability of organizations to participate, forecast, and actively assess their information security circumstances. Enhancement is one of key indicators for improving readiness and capabilities of information security. The organization's enhancements provide users the ability to conduct self-investigation and real-time monitoring of network activities. The current RISC investigation tool uses the ICM[2] approach. In some case studies, organizations spent approximately 12 months to conduct RISC investigation. On the other hand, Kosutic (2012) stated that for RISC investigation of compliance processes, organizations commonly take between 3–36 months.

Many organizations experience difficulty in implementing and complying with an ISMS standard, including obstacles faced when measuring the readiness level of an organizational implementation, document preparation as well as the various scenarios and information security strategies to deal with (Susanto et al., 2011a; Siponen & Willison, 2009). An organization may face internal and external challenges in implementing an ISMS standard. Without proper planning, the following obstacles could create a barricade for effective information security implementation (Furnell, 2005; Kosutic, 2012; Susanto et al., 2011a, 2012b, Von Solm, 2001):

1. Expertise and employment of it may be beyond an organization's capability.
2. Difficulty in selecting existing information security standards, for instance in choosing out of PRINCE2, OPM3, CMMI,P-CMM, PMMM, ISO 27001, BS7799, PCIDSS, COSO, SOA, ITIL or COBIT. Each standard plays its own role and position in ISMS, such as (1) information security associated with the project management and IT governance, (2) information security

[2] Implementation Checklist Method.

related to business transactions and smart cards, and (3) overall information security management system as the main focus of the standard.

3. Compliance with an ISMS standard such as ISO 27001 requires all employees to embrace new security controls introduced by the standard.

1.3 RESEARCH POSITIONING

This study is related to information security management system standards, risk management associated with information security and information security awareness within an organization. The details are explained in the following subsection.

1.3.1 INFORMATION SECURITY MANAGEMENT SYSTEM

An ISMS is a set of policies concerned with information management and ICT risks. The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. As with management processes, an ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment (Kelleher & Hall, 2005). The establishment, maintenance, and continuous update of the ISMS provide a strong indication that an organization is using a systematic approach for the identification, assessment, and management of information security risks and breaches.

The chief objective of ISMS is to implement the appropriate measurements in order to eliminate or minimize the impact that various security related threats and vulnerabilities might have on an organization. ISMS will enable implementation of desirable characteristics of the services offered by the organization (i.e., availability of services, preservation of data confidentiality and integrity, etc.). However, the implementation of an ISMS entails the following steps: definition of security policy, definition of ISMS scope, risk assessment, risk management, selection of appropriate controls, and statement of applicability (Calder & Watkins, 2010; Potter & Beard, 2012). To be effective, efficient, and influential towards an organization's business processes, ISMS implementation must follow scenarios such as:

- It must have the continuous, unshakeable and visible support and commitment of the organization's top management;
- It must be an integral part of the overall management of the organization related to and reflecting the organization's approach to risk management, the control objectives and controls and the degree of assurance required;
- It must have security objectives and activities based on business objectives and requirements and led by business management;
- It must fully comply with the organization's philosophy and mindset by providing a system that instead of preventing people from doing what they are employed to do, it will enable them to do it in control and demonstrate their fulfilled accountabilities;
- It must be based on continuous training and awareness of staff and avoid the use of disciplinary measures;
- It must be a never ending process.

There are several ISMS standards that can be used as benchmarks for information system security. An organization can choose one of these standards to comply with. The big five of ISMS standards (Susanto et al., 2011a) are ISO 27001, BS 7799, PCIDSS, ITIL and COBIT. Susanto et al. (2011b) stated that ISO 27001 is the ISMS standard most widely used globally. ISO 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system – an overall management and control framework – for managing an organization's information security risks.

Moreover, ISO 27001 consists of protection against the following aspects: *Confidentiality* ensuring that information can only be accessed by an authorized person and ensure confidentiality of data sent, received and stored; *Integrity* ensuring that data is not altered without the permission of authorized parties, to maintain the accuracy and integrity of information; *Availability* guarantees that data will be available when needed ensure that legitimate users can use the information and related devices.

1.3.2 MANAGING RISK ASSOCIATED WITH INFORMATION SECURITY

Risk Management is a recurrent activity that deals with the analysis, planning, implementation, control and monitoring of implemented measures and enforced security policies (Blakley et al., 2001). It is the process of implementing and maintaining appropriate management controls including policies, procedures and practices to reduce the effects of risk to an acceptable level. The principles of risk management can be directed both to limit adverse outcomes and to achieve desired objectives. Risk management regulates risks toward information and knowledge assets from any internal-external disclosure and unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction within an organization. Managing risk associated with information assets is called Information Risk Management (Humphreys et al., 1998).

Moreover, information risk management[3] adapts the generic process of risk management and applies it to the integrity, availability and confidentiality of information assets and the information environment. Information risk management should be incorporated into all decisions in day-to-day operations. Information risk management deals with methodologies and incorporates the typical analysis, assessment, audit, monitoring, and management processes. The details of each stage are as follows (Blakley, 2001; Kelleher & Hall, 2005):

1. **Analysis** examines a given situation, checking for obvious deficits according to professional experience or even common sense. The examination can be structured and repeatable. An information security penetration test and vulnerability scan is an analysis whose purpose is to identify whether the perimeter is vulnerable, identifies flaws, and determines if such a flaw really poses a problem for the organization.
2. **Assessment** identifies a problem and describes how much of a problem it is. A related term in ICT security is vulnerability assessment. As an extension of a vulnerability scan, a vulnerability assessment sets the results of a scan into the context of the organization and

[3] Managing risk associated with information assets is called information risk management. It consolidates property values, claims, policies and exposure of information and management reporting capabilities (Humphreys et al., 1998).

assigns an urgency level. In general, an assessment uses a structured approach, is repeatable, and describes the level of a problem.

3. **Audit** compares a given situation with some sort of standardized situation; an external standard (for instances, a law, or an industry standard) or an internal one (e.g., a policy document). The results of an audit explain how much reality deviates from an expected or required situation.
4. **Monitoring** is an operational activity which introduces the notion of time, as the process of monitoring is real-time and continuous. Proper monitoring requires an established approach to be able to show trends and activities consistently and efficiently.
5. **Management** is a strategic activity. It involves understanding the situation (analysis), determining the extent of the problem (assessment), standardizing the examination (audit), and continuing these activities over time (monitoring). Moreover, it adds the components of remediation, initiating and tracking changes, also includes the necessary communication within the organization.

1.3.3 INFORMATION SECURITY AWARENESS

Information security awareness (ISA) is the knowledge and attitude members of an organization possess regarding the protection of the physical, especially information, assets of an organization. According to the European Network and Information Security Agency (ENISA, 2012), ISA is awareness of the risks and available safeguards as the first line of defense for the security of information systems and networks. The focus of security awareness should be to achieve a long-term shift in the attitude of employees towards security, promoting a cultural and behavioral change within an organization. Security policies should be viewed as key enablers and an integral part of a business, not as a series of rules restricting the efficient working of business processes.

Being security-aware means acknowledging that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization. Therefore, it would be prudent to support the assets of the institution (information, physical, and personal) by trying to stop that from happening. These following issues especially show the importance of ISA (Kosutic, 2012; Peltier, 2005a, 2005b):

1. The nature of sensitive material and physical assets employees may come in contact with, such as trade secrets, privacy concerns and government classified information.
2. Employee and contractor responsibilities in handling sensitive information, including review of employee nondisclosure agreements.
3. Requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction.
4. Proper methods for protecting sensitive information on ICT systems, including password policy and use of authentication.
5. Other computer security concerns, including malware, phishing, social engineering, etc.
6. Workplace security, including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.
7. Consequences of failure to properly protect information, including potential loss of employment, economic consequences to the firm, damage to individuals whose private records are divulged, and possible civil and criminal penalties.

Information security breaches within organizations were reported by Information Security Breaches Survey (ISBS) (Potter & Beard, 2012), which stated that '*incidents caused by staff*' was experienced by 82% of the sampled large organizations (Figure 1.1). No industry sector appears immune from these incidents. Telecommunications, utilities and technology companies appear to have the most reliable systems. The public sector, travel, leisure and entertainment companies are most likely to have security problems. Moreover, it was found that the average security incident within local business organizations occurred once a month, while large or international organizations would expect an incident to occur once a week (Potter & Beard, 2012).

Nowadays, to face with ISA issues, most organizations have allocated more of their budget towards security than in the previous year (2008–2011). On average, organizations spend 8% of their IT budget on information security, and those that suffered a very serious breach were found to

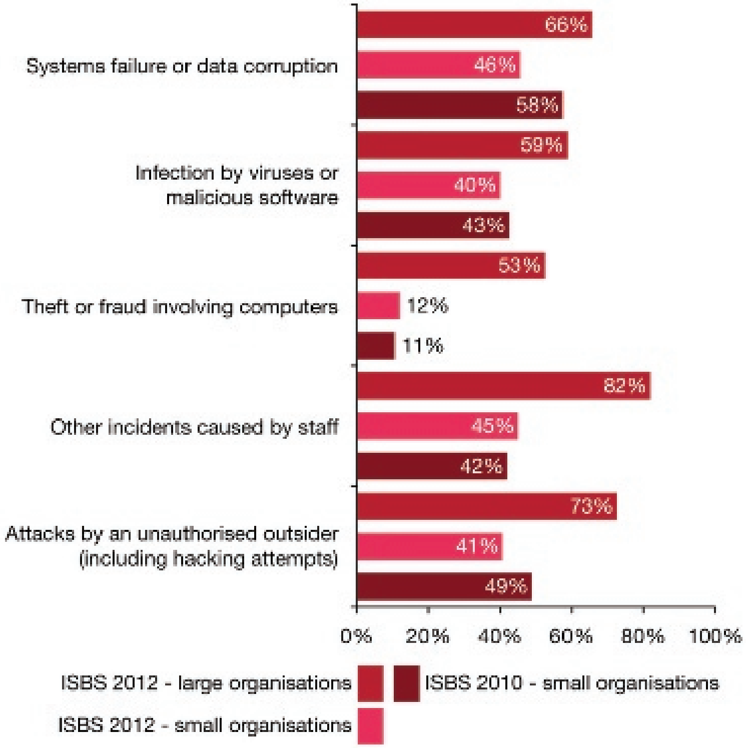

FIGURE 1.1 Type of breaches suffered by organizations (ISBS) (Potter & Beard, 2012).

have spent on average 6.5% of their IT budget on security (Potter & Beard, 2012).

As mentioned, ISA is the behavior of employees regarding protection of information assets, such as customer information and customer transactions, therefore having influence on customer trust and customer loyalty. Kottler (2002) and stated, it is obvious that business organizations are dependent on their loyal customers for business sustainability. Customer loyalty is all about attracting the right customers, winning their trust and providing convenience, getting them to buy, buy often, buy in higher quantities, and bring even more customers (Kotler, 2002). ISA implementation should be viewed as one of the corporate efforts, serving the following functions: (1) to improve corporate selling point to customers (Kottler, 1969, 2002); (2) corporate imaging and branding. Corporate branding is an economic-management and social event as well as a strategy through which customers' demands and providers' supplies are balanced (Dwyer et al., 1987); (3) to win the competitive edge within the related business area (Morrison et al., 2003); (4) as one of the marketing tools (Figure 1.2) (Kottler, 2002); (5) to increase corporate profitability (Brown et al., 2000); and (6) to increase customer trust, leading them to become loyal customers stemming from amity and customer satisfaction, sustaining the interdependency between producer and customer (Baker et al., 1996; Brown et al., 2000).

1.4 RESEARCH METHOD

This research was performed through literature review, analysis, refinement of ISMS standards, proposed framework (ISF) and implementation of ISF as a software application (ISM). There were several stages conducted. The first stage was knowledge discovery and building knowledge as the first phase of the research, conducted through literature reviews on related work, comparative studies and refinement. The second stage was the construction of a new framework (ISF). The third stage was creating software architecture, constructing variables, assessment of formulae and

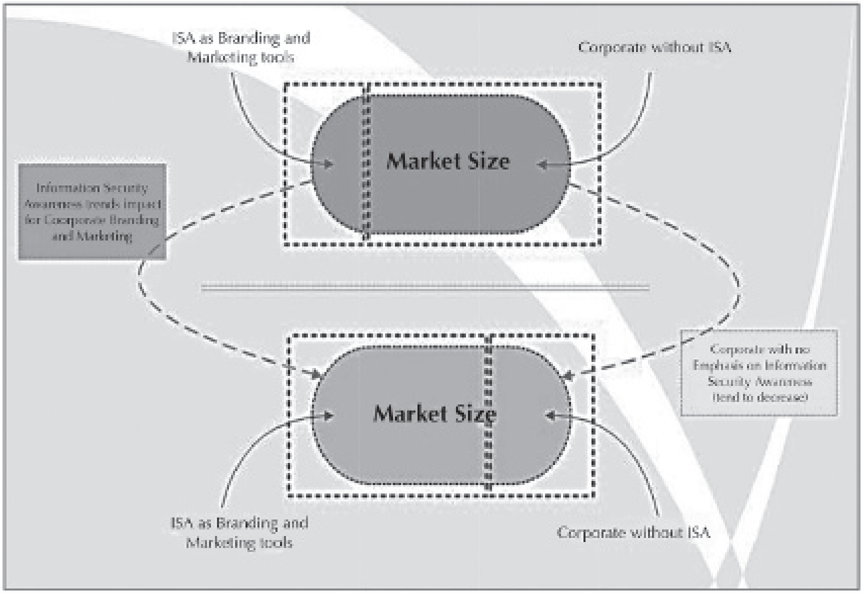
ISA as Branding and Marketing tools
Corporate without ISA
Market Size
Information Security Awareness trends impact for Corporate Branding and Marketing
Corporate with no Emphasis on Information Security Awareness (tend to decrease)
Market Size
ISA as Branding and Marketing tools
Corporate without ISA

FIGURE 1.2 ISA Impact for Branding and Marketing Tools.

software development. The last stage was comprehensive ISM evaluation; this includes testing on reliability, usability, and performance of ISM within the context of an organization.

We conducted testing on a variety of sizes of organizations; small organizations (up to 100 employees), medium sized organizations (101–250 employees) and large organizations (more than 250 employees) (Potter & Beard, 2010) as users of ISF-ISM to find out their preferences and tendencies toward ISM. The companies have businesses in the fields of telecommunications, banking and finance, airlines, and ICT consultants. These organizations were grouped in three categories:

1. Group I: ISO 27001 holders. Companies that recently received or were certified by ISO 27001 in the period of 2010–2012.
2. Group II: ISO 27001 ready. Companies currently pursuing ISO 27001 compliance, whether they were in the documents preparation stage, scenario development stage or risk management analysis stage.
3. Group III: ISO 27001 consultants. Companies in this group are ICT consultants in the security area, particularly information security and standards.

We used a selected sampling method, in which the respondents were intentionally selected from telecommunications, banking and finance, airlines, and ICT consultants. The majority of the companies are listed in the stock exchange and the companies are well recognized by their clients and the public. As listed companies, they have strategies to win competitive markets in the respective industries and they are very concerned with retaining their by clients and customers by maintaining their trust, in which information security is an important component.

The results of testing and evaluation were further analyzed using software performance parameters (SPP) (Bakry 2003a; Gan, 2006; 2003b; McCall, 1977) and release and evaluation management to find out the ISF-ISM performance, features and reliability and its efficacy as measurement tools for an organization's RISC level in ISMS standard compliance. There are eight defined parameters to measure performance and features of the framework and software, as follows: (1) how ISM functions as information security self-assessment? (2) how ISM helps organizations understand ISMS standard (ISO 27001) controls? (3) how ISM can be used to understand information security standard terms and concepts? (4) ISM features; (5) ISM graphical user interface and user friendliness; (6) analysis precision produced by ISM; (7) final result precision produced by ISM; and (8) ISM performance (Bakry, 2003a, 2003b; Gan, 2006; Von Solms, 2001).

A detailed discussion on the methodology of the study is provided in Chapter 3 of this book.

1.5 OUTCOME AND CONTRIBUTIONS

One of our research's contributions was observes the barriers facing implementation of an ISMS standard within an organization and identifying the cause of increased numbers and costs of information security breaches that are rising fast. The gaps in existing information security adoption clearly demonstrates the need for the proposed novel approach (ISF) to further appropriate information security awareness, risk management associated with information security, and ISMS compliance (further discussed in Chapter 4: Proposed Framework).

The major contribution of our research is the framework (ISF) and a new measurement approach. This enabled the binding of organizational security policies and standards to the governance and compliance requirements. This contribution changes the landscape of information security standard adoption to a more structured approach and measurement. This is a very significant contribution since it addresses the gaps of existing frameworks, as indicated by Potter & Beard (2010), Calder & Watkins (2010, 2012) Fomin et al. (2008), Susanto et al. (2012c, 2012h), that current existing frameworks do not provide a model for a formal readiness level measurement on how the ISMS standard is adopted by an organization.

ISF and ISM is an academic contribution to the scientific and practical environment. For future research, ISF could be made to accommodate and be customized to fit with other standards such as BS 7799, COBIT, ITIL, and others. ISF could possibly be implemented by other standards by following mapping stages through grouping of controls to the respective domains in each standard.

ISF is intended to introduce a novel algorithm for compliance measurement and investigation of ISMS as a bottom-up approach, designed to be implemented in high-level computer programming language, to produce a graphical user interface (GUI) that is easy to be used and powerful for ISO 27001 investigation. An innovative aspect of this approach is the development of a software (ISM) composed of two main functions: Security assessment management (SAM/e-assessment), which functions as log management and compliance reporting, and security monitoring management (SMM/e-monitoring) which functions as real-time monitoring for security-related events (further discussed in Chapter 6).

All those study contributions could be summarized as follows:

1. **A structured approach** for determining and mapping assessment issues, controls, clause and domain settings by **the new framework (ISF)** in order to organize security management issues in an ISMS standard (ISO 27001) effectively.
2. **A systematic mechanism for ISO 27001 refinement.** The refinement is used to verify and refine ISO 27001 to determine the degree of clarity of each essential control over its parameters. Refinement is a deterministic process, and since organizations have a number of information security controls, without refinement the controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. It is obvious that essential controls are very difficult to understand, immeasurable and difficult to be implemented by organizations and stakeholders (to be explained in detail in Chapter 4).
3. **ISM (integrated solution modeling software for RISC investigation)**. The framework (ISF) has led us to develop ISM as a user interface between the stakeholder and ISF's approach to measuring information security awareness (ISA) and compliance level of the ISMS standard (ISO 27001) within an organization, such as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. ISM consists of two major subsystems of e-assessment and e-monitoring. E-assessment is to measure ISO 27001 parameters based on the proposed framework with 21 essential controls and e-monitoring is to monitor suspected

activities that may lead to security breaches and provides real-time monitoring for security-related events. The software is equipped with a user record of accomplishment, functioning to determine users' patterns of assessment (Future explanation in Chapter 5).

1.6 BOOK STRUCTURE

This book is composed of seven chapters. Chapter 1 is the introduction which contains the background, problems and motivation of the research. This chapter also highlights the methodology employed and summarizes results and contributions of the book. Chapter 2 contains the literature review of the field of information security management systems, frameworks and managing risk associated with information security. Chapter 3 is concerned with the research methodology of the book. Chapter 4 discusses the proposed framework as a new approach to map security controls within six domains. Based on the framework we developed software (ISM) as a tool to measure readiness level with ISO 27001, discussed in Chapter 5. Chapter 6 illustrates testing and comprehensive evaluation conducted by ISM in respondent organizations and discussion of the result. Finally, Chapter 7 is the conclusion.

1.7 CONCLUDING REMARKS

The main aim of this study has been to map up the terrain of information security management in organizations. Securing information resources from unauthorized access is an extremely important, since information need to be managed in a proper and systematic manner as information security is quite complex. This research contributes a new approach for RISC investigations by offering a framework for the evaluation, formation and implementation of information security, through identifying ISMS basic building blocks (assessment issues, controls, clauses, and domains).

Practitioners and stakeholders can use the research's results (ISF, refinement, and ISM) presented here as blueprints for managing information security within their organizations. They can compare and benchmark their own processes and practices against these results and come up with new critical insights to aid them in their stages to information security standard (ISO 27001) adoption. Scholars in the field of information security management can use the existing results and build further on them to form a coherent and complete body of knowledge of the area.

Finally, an innovative aspect of this research is the proposed novel framework (ISF) and development of software (ISM). ISF enables the binding of organizational security policies and standards to the governance and compliance requirements. This contribution changes the landscape of information security standard adoption to a more structured approach and measurement. ISM is a semi-automated tool to assess the readiness of an organization to comply with ISO 27001 and subsequently assess the potential threats. ISM's two main functions of Security Assessment Management (SAM/e-assessment) and Security monitoring management (SMM/e-monitoring) could help an organization to review their circumstances regarding ISMS as the preliminary adoption stage.

KEYWORDS

- **integrated solution framework**
- **integrated solution modeling**
- **security assessment management**
- **software performance parameters**

BIBLIOGRAPHY

Abu Saad, B., Saeed, F. A., Alghathbar, K., & Khan, B. (2011). Implementation of ISO 27001 in Saudi Arabia–Obstacles, motivations, outcomes, and lessons learned.

Aceituno, V. (2005). On Information Security Paradigms. *ISSA Journal, September*, *24*, 225–229.

Al Omari, L., Barnes, P. H., & Pitman, G. (2012, December). Optimising COBIT 5 for IT governance: examples from the public sector. In: *Proceedings of the ATISR 2012: 2nd International Conference on Applied and Theoretical Information Systems Research (2nd. ATISR2012)*. Academy of Taiwan Information Systems Research.

Al Osaimi, K., Alheraish, A., & Bakry, S. H. (2008). STOPE–based approach for e-readiness assessment case studies. *International Journal of Network Management*, *18*(1), 65–75.

Alfantookh, A. (2009). An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. *Computer Sciences, King Saud University*.

Aljabre, A. (2012). Cloud computing for increased business value. *International Journal of Business and Social Science*, *3*(1), 234–239.

Almunawar, M. N., Anshari, M., & Susanto, H. (2013). Crafting strategies for sustainability: how travel agents should react in facing a disintermediation. *Operational Research*, *13*(3), 317–342.

Alshitri, K. I., & Abanumy, A. N. (2014, May). Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. In: *2014 International Conference on Information Science and Applications (ICISA),* IEEE. pp. 1–4.

Amoroso, E. G. (1994). *Fundamentals of Computer Security Technology*. Prentice-Hall, Inc.

Anderson, B., & Adey, P. (2011). Affect and Security: Exercising Emergency in UK Civil Contingencies'. *Environment and Planning D: Society and Space, 29*, 1092–1109.

Anderson, E., & Weitz, B. (1989). Determinants of continuity in conventional industrial channel dyads. *Marketing Science*, *8*(4), 310–323.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308–313.

Anderson, K. (2006). IT Security Professionals Must Evolve for Changing Market. SC Magazine, 12, 2006.

Anderson, R. (2001). Why information security is hard-an economic perspective. In: *Proceedings 17th Annual Computer Security Applications Conference, 2001. ACSAC 2001*. IEEE. pp. 358–365.

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613.

Anttila, J., Kajava, J., & Varonen, R. (2004). Balanced integration of information security into business management. In: *Proceedings. 30th Euromicro Conference, 2004*. IEEE. 558–564.

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 11–33.

Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. (2007). Automated classification and analysis of internet malware. In: *Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg. pp. 178–197.

Baker, L. B., & Finkle, J. (2011). Sony PlayStation suffers massive data breach. *Reuters, April*, *26*.

Baker, M., Walker, O., Mullins, J., Boyd, H., Larreche, J., & Cravens, D. (1996). Marketing strategy. *International Encyclopedia of Business and Management*, 3333–3347.

Bakers, S. (2011). Facebook statistics by country. *URL: http://www.socialbakers.com/facebook-statistics/-abgerufenam*, *17*, 2011.

Bakers, S. (2013). *Social Bakers*. Retrieved March, 14, 2013.

Bakos, J. Y. (1991). A strategic analysis of electronic marketplaces. *MIS quarterly*, 295–310.

Bakos, J. Y. (1997). Reducing buyer search costs: Implications for electronic marketplaces. *Management Science*, *43*(12), 1676–1692.

Bakry, S. H. (2003a). Toward the development of a standard e-readiness assessment policy. *International Journal of Network Management*, *13*(2), 129–137.

Bakry, S. H. (2003b). Development of security policies for private networks. *International Journal of Network Management*, *13*(3), 203–210.

Bakry, S. H. (2004). *Development of E-Government: A STOPE View. International Journal of Network Management, 14*(5), 339–350.

Bakry, S. H., & Bakry, F. H. (2001). A strategic view for the development of e-business. *International Journal of Network Management*, *11*(2), 103–112.

Baraghani, S. N. (2008). Factors influencing the adoption of internet banking. *Lulea University of Technology.*

Benjamin, R., & Wigand, R. (1995). Electronic markets and virtual value chains on the information superhighway. *Sloan Management Review (Winter, 1995)*.

Besnard, D., & Arief, B. (2003). *Computer Security Impaired by Legal Users*. University of Newcastle upon Tyne, Computing Science.

Bitazar, A. (2009). About ISO 27001 Benefits and Features. Obtained from http://www.articlesbase.com.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In: *Proceedings of the 2001 Workshop on New Security Paradigms*. ACM. 97–104.

Blessing, L. T. M., Chakrabarti, A., & Wallace, K. M. (1998). An overview of descriptive studies in relation to a general design research methodology. In: *Designers*. Springer London. pp. 42–56.

Blyth, A., & Kovacich, G. L. (2001). *What is Information Assurance?*. Springer London. pp. 3–16.

Boehm, B. W., Brown, J. R., & Lipow, M. (1976). Quantitative evaluation of software quality. In: *Proceedings of the 2nd International Conference on Software Engineering*. IEEE Computer Society Press. pp. 592–605.

Boehm, B., & Hansen, W. (2001). The spiral model as a tool for evolutionary acquisition. *CrossTalk*, *14*(5), 4–11.

Boehm, B., & Hansen, W. J. (2000). *Spiral Development: Experience, Principles, and Refinements* (No. CMU/SEI-2000-SR-008). Carnegie-Mellon University Pittsburgh, PA, Software Engineering Inst.

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *SECURWARE*, *8*, 224–231.

Bonner, E., O'Raw, J., & Curran, K. (2013). Implementing the Payment Card Industry (PCI) Data Security Standard (DSS). *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *9*(2), 365–376.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164.

Bowen, T. P., Wigle, G. B., & Tsai, J. T. (1985). *Specification of software quality attributes*. Rome Air Development Center, Air Force Systems Command.

Boyce, J. G., & Jennings, D. W. (2002). *Information Assurance: Managing Organizational IT Security Risks*. Butterworth-Heinemann.

Brand, K., & Boonen, H. (2007). *IT Governance Based on Cobit 4. 1: A Management Guide*. Van Haren Publishing.

British Standard (BS). (2012). An Overview of British Standard: BS 7799. Obtained from http://www.bsigroup.com/en/Standardsand-Publications/About-BSI-British-Standards/.

Brown, J. R., Dev, C. S., & Lee, D. J. (2000). Managing marketing channel opportunism: the efficacy of alternative governance mechanisms. *Journal of Marketing*, *64*(2), 51–65.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

BUMN.go.id. (2012). The Adoption of ISO 27001 of Telkom Indonesia: A Key Performance for Customer Trust. Obtained from: www.bumn.go.id.

Calder, A., & Watkins, S. (2012). *IT Governance: An International Guide to Data Security and ISO 27001/ISO27002*. Kogan Page Publishers.

Calder, A., & Watkins, S. G. (2010). *Information Security Risk Management for ISO 27001/ISO27002*. It Governance Ltd.

Cavano, J. P., & McCall, J. A. (1978). A framework for the measurement of software quality. *ACM SIGSOFT Software Engineering Notes*, *3*(5), 133–139.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004a). Economics of ITSecurity Management: Four Improvements to Current Security Practices. *The Communications of the Association for Information Systems*, *14*(1), 37.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004b). A model for evaluating IT security investments. *Communications of the ACM*, *47*(7), 87–92.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004c). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70–104.

Cherdantseva, Y., & Hilton, J. (2013). Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals. *Organizational, Legal, and Technological Dimensions of IS Administrator*. IGI Global Publishing.

Cherdantseva, Y., Rana, O., & Hilton, J. (2011). Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success. *ISSE Securing Electronic Business Processes*, 201–213.

Clark, D. D., & Wilson, D. R. (1987). A Comparison of Commercial and Military Computer Security Policies.

Cockburn, A., & Highsmith, J. (2001). Agile software development: The people factor. *Computer*, *34*(11), 131–133.

Combes, G. C., & Patel, J. J. (1997). Creating lifelong customer relationships: Why the race for customer acquisition on the Internet is so strategically important. *iword, 2*(4), 132–140.

Committee on National Security Systems, CNSS. (2004). 4009, "National Information Assurance Glossary," Committee on National Security Systems, May 2003. *Formerly NSTISSI, 4009*.

Cooper, H. (1998). Synthesizing Research: A Guide for Literature Reviews Common Criteria (CC) for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1. Revision 3. July 2009.

Costa, L., & D'Amico, R. (2011). Malware Detection and Prevention Platform: Telecom Italia Case Study. In: *ISSE 2010 Securing Electronic Business Processes,* pp. 203–213. Vieweg + Teubner.

Cusumano, M. A., & Smith, S. A. (1995). Beyond the Waterfall: Software Development at Microsoft.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98.

D'Arcy, S. P., & Brogan, J. C. (2001). Enterprise risk management. *Journal of Risk Management of Korea*, *12*(1), 207–228.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207.

Dark, M. J., Ekstrom, J. J., & Lunt, B. M. (2005). Integration of information assurance and security into the IT2005 model curriculum. In: *Proceedings of the 6th Conference on Information Technology Education*. ACM, pp. 7–14.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307–324.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307–324.

Dellinger, A. (2005). Validity and the review of literature. *Research in the Schools*, *12*(2), pp. 41–54.

Dellinger, A. B., & Leech, N. L. (2007). Toward a unified validation framework in mixed methods research. *Journal of Mixed Methods Research*, *1*(4), 309–332.

Detik.com. (2013). Indonesia – Australia in Wiretapped issues (www.detik.com).

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases*. New York: Wiley. 97–129.

Dick, A. S., & Basu, K. (1994). Customer loyalty: Toward an integrated conceptual framework. *Journal of the Academy of Marketing Science*, *22*(2), 99–113.

Dictionary, O. E. (2013). Oxford English Dictionary.

Diefenbach, T. (2009). Are case studies more than sophisticated storytelling?: Methodological problems of qualitative empirical research mainly based on semi-structured interviews. *Quality & Quantity*, *43*(6), 875–894.

Dietrich, C. J., Rossow, C., & Pohlmann, N. (2013). CoCoSpot: Clustering and recognizing botnet command and control channels using traffic analysis. *Computer Networks*, *57*(2), 475–486.

Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3), 189–198.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, *25*(1), 55–63.

Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). *A Systematic Approach to Define the Domain of Information System Security Risk Management.* In Intentional Perspectives on Information Systems Engineering (pp. 289–306). Springer Berlin Heidelberg.

Dwyer, F. R., Schurr, P. H., & Oh, S. (1987). Developing buyer-seller relationships. *The Journal of Marketing*, 11–27.

Easttom, W. C. (2012). *Computer Security Fundamentals*. Pearson Education India.

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*, *2005*(11), 10–16.

Eloff, M. M., & Solms, S. H. (2000). Information security management: A hierarchical framework for various approaches. *Computers & Security, 19*(3) 243–256. doi: 10.1016/S0167-4048(00)88613-7. Elsevier.

FinanceToday.com. (2013). Indonesian's ICT consumer behavior. Obtained from www.financetoday.com.

Fink, D. (1994). A Security Framework for Information Systems Outsourcing. *Information Management and Computer Security, 2*(4), 3–8. doi: 10.1108/09685229410068235. Emerald.

Fomin, V. V., Vries, H., & Barlette, Y. (2008). ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. In: *EUROMOT 2008 Conference, Nice, France*.

Fomin, V. V., Vries, H., & Barlette, Y. (2008). ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. In: *Proceedings of The Third European Conference on Management of Technology (EUROMOT)*.

Fordyce, S. (1982). Computer security: A current assessment. *Computers & Security*, *1*(1), 9–16.

Furnell, S. (2005). Why users cannot use security. *Computers & Security*, *24*(4), 274–279.

Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research*, *9*(5), 372–382.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27–35.

Furnell, S. M., Onions, P. D., Knahl, M., Sanders, P. W., Bleimann, U., Gojny, U., & Röder, H. F. (1998). A security framework for online distance learning and training. *Internet Research*, *8*(3), 236–242.

Galvan, J. L. (2006). *A Guide for Students of the Social and Behavioral Sciences*. Pyrczak Publishing.

Gan, X. (2006). Software Performance Testing. In: *Seminar Paper, University of Helsinki*. pp. 26–29.

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, *23*(4), 367–376.

Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, *2*(5), 544–554.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457.

Green, B. F., & Hall, J. A. (1984). Quantitative methods for literature reviews. *Annual Review of Psychology*, *35*(1), 37–54.

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., & Calandrino, J. A. (2009). Lest we remember: cold-boot attacks on encryption keys. *Communications of the ACM*, *52*(5), 91–98.

Hart, T. B. (2008). Visual Methodologies: Rose, Gillian. Visual Methodologies: An Introduction to the Interpretation of Visual Materials. London: Sage, 2007, 301 pp.

Hentea, M. (2005). A perspective on achieving information security awareness. *Informing Science: International Journal of an Emerging Transdiscipline*, *2*, 169–178.

Herbsleb, J., Zubrow, D., Goldenson, D., Hayes, W., & Paulk, M. (1997). Software quality and the capability maturity model. *Communications of the ACM*, *40*(6), 30–40.

Highsmith, J., & Cockburn, A. (2001). Agile software development: The business of innovation. *Computer*, *34*(9), 120–127.

Hoo, K. J. S. (2000). *How Much is Enough? A Risk Management Approach to Computer Security*. Stanford University.

Humphreys, E. J., Moses, R. H., & Plate, A. E. (1998). *Guide to Risk Assessment and Risk Management*. British Standards Institution.

Huo, M., Verner, J., Zhu, L., & Babar, M. A. (2004, September). Software quality and agile methods. In: *Computer Software and Applications Conference, 2004. COMPSAC 2004. Proceedings of the 28th Annual International*. IEEE. pp. 520–525.

Information Assurance Advisory Council (IAAC) in association with Microsoft. Benchmarking Information Assurance. (2002).

Information Assurance Collaboration Group (IACG). (2007). Industry Response To The HMG Information Assurance Strategy and Delivery Plan. A report by the IACG Working Group On The Role Of Industry In Delivering The National IA Strategy (IWI009).

International Standard Organization (ISO). 2004. Information Security Management System. Obtained from http://www.isms-guide.blogspot.com/2007/11/key-components-ofstandard-iso-27001-iso.html and www.ISO 27001security.com.

ISACA. (2008). Glossary of Terms. Available online at http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf [accessed on 10.07.2011].

ISACA. (2009). *An Introduction to the Business Model for Information Security*.

ISO. (2004). ISO/IEC 13335–1: Information technology – Security techniques – Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management.

ISO. (2009). (E) ISO/IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary.

ISO. (2009). ISO/IEC 15408–1: Information technology – Security techniques – Evaluation criteria for IT security. Part 1: Introduction and general model.

ISO/IEC 27000:2009 (E) Information technology - Security techniques – Information security management systems - Overview and vocabulary.

IT Governance Institute (ITGI). (2007). COBIT 4.1 Excerpts. Rolling Meadows, IL 60008 USA.

IT Governance Institute (ITGI). (2007). COBIT 4.1 Executive Overview. ITGI Rolling Meadows, USA.

IT Governance Institute (ITGI). (2008). Aligning CobiT® 4. 1, ITIL® V3 and ISO/IEC 27002 for Business Benefit A Management Briefing From ITGI and OGC. ITGI Rolling Meadows, USA.

IT Governance Institute (ITGI). (2008). COBIT Mapping. ITGI Rolling Meadows, USA.

IT Governance Institute (ITGI). (2008). Mapping of ITIL v3 with COBIT 4.1. Rolling Meadows, IL 60008 USA.

Jackson, M. (2001). *Problem Frames: Analyzing and Structuring Software Development Problems*. Addison-Wesley.

Jung, H. W., Kim, S. G., & Chung, C. S. (2004). Measuring software product quality: A survey of ISO/IEC 9126. *IEEE Software*, *21*(5), 88–92.

Kan, S. H. (2002). *Metrics and Models in Software Quality Engineering*. Addison-Wesley Longman Publishing Co., Inc.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154.

Kawakoya, Y., Iwamura, M., & Itoh, M. (2010, October). Memory behavior-based automatic malware unpacking in stealth debugging environment. In: *2010 5th International Conference on Malicious and Unwanted Software (MALWARE),* IEEE. pp. 39–46.

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, *6*(14), 4982–4989.

Kelleher, Z., & Hall, H. (2005). Response to risk Experts and end-user perspectives on email security, and the role of the business information professional in policy development. *Business Information Review*, *22*(1), 46–52.

Khosroshahy, M., Mehmet Ali, M. K., & Qiu, D. (2013). The SIC botnet lifecycle model: A step beyond traditional epidemiological models. *Computer Networks*, *57*(2), 404–421.

Kompas.com. (2013). Diplomatic Tensions Indonesia – Australia in Wiretapped issues. Obtained from: www.kompas.com.

Kosutic, D. (2010). ISO 27001 and BS 25999. Obtained from http://blog.ISO 27001standard.com.

Kosutic, D. (2013). *Risk Assessment of ISO 27001*. Retrieved November, 2013, from http://blog.ISO 27001standard.com/.

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International.

Kotler, P. (2002). Marketing Management. Prentice Hall.

Kotler, P., & Levy, S. J. (1969). Broadening the concept of marketing. *Journal of Marketing*, *33*(1).

Kruse II, W. G., & Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials*. Pearson Education.

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4–13.

Lacey, D. (2011). *Managing the Human Factor in Information Security: How to Win Over Staff and Influence Business Managers*. John Wiley & Sons.

Lambo, T. (2006). ISO/IEC 27001: The future of infosec certification. *ISSA Journal, Information Systems Security Organization (http://www.issa.org)*.

Laredo, V. G. (2008). PCI DSS compliance: A matter of strategy. *Card Technology Today*, *20*(4), 9.

Leder, F., Steinbock, B., & Martini, P. (2009). Classification and detection of metamorphic malware using value set analysis. In: *2009 4th International Conference on Malicious and Unwanted Software (MALWARE),* IEEE. pp. 39–46.

Lee, Y. W., Strong, D. M., Kahn, B. K., & Wang, R. Y. (2002). AIMQ: A methodology for information quality assessment. *Information & Management*, *40*(2), 133–146.

Lichtenstein, S., & Williamson, K. (2006). Understanding consumer adoption of internet banking: An interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, *7*(2), 50–66.

MacCormack, A., & Verganti, R. (2003). Managing the sources of uncertainty: Matching process and context in software development. *Journal of Product Innovation Management*, *20*(3), 217–232.

Madu, C. N., & Kuei, C. H. (1993). Introducing strategic quality management. *Long Range Planning*, *26*(6), 121–131.

Mataracioglu, T., & Ozkan, S. (2011). Analysis of the User Acceptance for Implementing ISO/IEC 27001: 2005 in Turkish Public Organizations. *arXiv preprint arXiv:1103.0405*.

McCall, J. A., Richards, P. K., & Walters, G. F. (1977a). *Factors in Software Quality. Volume-I. Concepts and Definitions of Software Quality*. General Electric Co., Sunnyvale, CA.

McCall, J. A., Richards, P. K., & Walters, G. F. (1977b). *Factors in Software Quality. Volume-III. Preliminary Handbook on Software Quality for an Acquisition Manager*. General Electric Co., Sunnyvale CA.

McCumber, J. (1991). Information systems security: A comprehensive model. In: *Proceedings of the 14th National Computer Security Conference*.

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, *20*(4), 248–263.

Morrison, M., Sweeney, A., & Heffernan, T. (2003). Learning styles of on-campus and off-campus marketing students: The challenge for marketing educators. *Journal of Marketing Education*, *25*(3), 208–217.

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review*, *24*(6), 540–554.

Morse, E. A., & Raval, V. (2011). Private ordering in light of the law: Achieving consumer protection through payment card security measures. *DePaul Bus. & Comm. LJ*, *10*, 213.

Müller, D., Herbst, J., Hammori, M., & Reichert, M. (2006). *IT Support for Release Management Processes in the Automotive Industry.* Springer Berlin Heidelberg. pp. 368–377.

Neumann, P. G. (1999). *Practical Architectures for Survivable Systems and Networks: Phase-One Final Report*. Sri International Menlo Park, CA, Computer Science Lab.

Nicolett, M., & Kavanagh, K. M. (2011). Magic quadrant for security information and event management. *Gartner RAS Core Research Note (May 2009)*.

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaua, T. (2009). Information security governance framework. *Proceedings of the First ACM Workshop on Information Security Governance.*

Oliver, D., & Lainhart, J. (2012). COBIT 5: Adding Value Through Effective Geit. *EDPACS*, *46*(3), 1–12.

Onwubiko, C. (2009). A security audit framework for security management in the enterprise. In: *Global Security, Safety, and Sustainability*. Springer Berlin Heidelberg. pp. 9–17.

Othman, M. F. I., Chan, T., Foo, E., Nelson, K. J., & Timbrell, G. T. (2011, August). Barriers to information technology governance adoption: a preliminary empirical investigation. In: *Proceedings of 15th International Business Information Management Association Conference*. pp. 1771–1787.

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information* (pp. I–XV). New York: Wiley.

Patton, M. Q. (1980). *Qualitative Evaluation Methods*.

Patton, M. Q. (2005). *Qualitative Research*. John Wiley & Sons, Ltd.

Peltier, T. R. (2005a). *Information Security Risk Analysis*. CRC press.

Peltier, T. R. (2005b). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49.

Peters, J. F., & Pedrycz, W. (1998). *Software Engineering: An Engineering Approach*. John Wiley & Sons, Inc.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR.

Pipkin, D. L. (2000). *Information Security: Protecting the Global Enterprise*. Upper Saddle River, NJ: Prentice Hall PTR.

Pollitt, D. (2005). Energies trains employees and customers in IT security: only one company in ten has staff with the necessary qualifications. *Human Resource Management International Digest*, *13*(2), 25–28.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646.

Potter, C., & Beard, A. (2010). Information security breaches survey 2010. *Price Water House Coopers. Earl's Court, London*.

Potter, C., & Beard, A. (2012). Information security breaches survey 2012. *Price Water House Coopers*. Earl's Court, London.

Prince Muqrin Chair (PMC). (2010). Area and Trends of Computer Security Issues.

Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness.

Queensland Government Information Security Policy Framework (QGISPF). (2009). *Shaping Government ICT to Support Business Outcomes: Queensland Government Information Security Policy Framework.* Queensland Government.

Rahim, A., & Bin Muhaya, F. T. (2010). Discovering the Botnet Detection Techniques. In *Security Technology, Disaster Recovery and Business Continuity*. Springer Berlin Heidelberg. pp. 231–235.

Ralph, P., & Wand, Y. (2009). A proposal for a formal definition of the design concept. In: *Design Requirements Engineering: A Ten-Year Perspective*. Springer Berlin Heidelberg. pp. 103–136.

Ramayah, T., Jantan, M., Mohd Noor, M. N., Razak, R. C., & Koay, P. L. (2003). Receptiveness of internet banking by Malaysian consumers: The case of Penang. *Asian Academy of Management Journal*, *8*(2), 1–29.

Ridley, G., Young, J., & Carroll, P. (2004, January). COBIT and its Utilization: A framework from the literature. In: *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004*. IEEE. 8 pp.

Rowlingson, R., & Winsborrow, R. (2006). A comparison of the Payment Card Industry data security standard with ISO17799. *Computer Fraud & Security*, *3*, 16–19.

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60–66.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, *9*(2), 107–118.

Saleh, M. S., Alrabiah, A., & Bakry, S. H. (2007a). A STOPE model for the investigation of compliance with ISO 17799–2005. *Information Management & Computer Security*, *15*(4), 283–294.

Saleh, M. S., Alrabiah, A., & Bakry, S. H. (2007b). Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach. *International Journal of Network Management*, *17*(1), 85–97.

Scandura, T. A., & Williams, E. A. (2000). Research methodology in management: Current practices, trends, and implications for future research. *Academy of Management Journal*, *43*(6), 1248–1264.

Schneier, B. (1999). Attack trees. *Dr. Dobb's Journal*, *24*(12), 21–29.

Schneier, B. (2001). Secrets & Lies: Digital Security in a Networked World. *International Hydrographic Review*, *2*(1), 103–104.

Schneier, B. (2008). The psychology of security. In: *Progress in Cryptology–AFRICACRYPT 2008*. Springer Berlin Heidelberg. pp. 50–79.

Schneier, B. (2009). *Schneier on Security*. John Wiley & Sons.

Schwalbe, K. (2010). *Information Technology Project Management, Revised*. Cengage Learning.

Schweitzer, J. A. (1982). *Managing Information Security: A Program for the Electronic Information Age*. Butterworth Publishers.

Shahsavarani, N., & Ji, S. (2014). Research in Information Technology Service Management (ITSM) (2000–2010): An Overview. *International Journal of Information Systems in the Service Sector (IJISSS)*, *6*(4), 73–91.

Shaw, A. (2009). Data breach: From notification to prevention using PCI DSS. *Colum. JL & Soc. Probs.*, *43*, 517.

Shaw, M. L. N. M. J., & Strader, T. J. (2010). Sustainable e-Business Management.

Sherwood, J., Clark, A., & Lynas, D. (2005). Enterprise security architecture. *Computer Security Journal*, *21*(4), 24.

Shieh, S. P., & Gligor, V. D. (1997). On a pattern-oriented model for intrusion detection. *IEEE Transactions on Knowledge and Data Engineering, 9*(4), 661–667.

Shoemaker, D., Bawol, J., Drommi, A., & Schymik, G. (2004). A delivery model for an Information Security curriculum. In: *Proceedings of the Third Security Conference*.

Sipior, J. C., & Ward, B. T. (2008). *A Framework for Information Security Management Based on Guiding Standards: A United States Perspective*. Issues in Informing Science & Information Technology, p. 5.

Siponen, M. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems*, *7*(1), 19.

Siponen, M., & Willison, R. (2007). A critical assessment of IS security research between 1990–2004.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270.

Standish Group. (2013). ICT Project Report. The CHAOS Manifesto.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *Mis Quarterly*, 441–469.

Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management*, *33*(1), 1–11.

Straub, Jr., D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276.

Susanto, H., & Almunawar, M. N., (2012d). Information Security Awareness Within Business Environment: An IT Review. ASEAN FBEPS-AGBEP PhD Colloquium. UBD, Brunei Darussalam.

Susanto, H., & Muhaya, F. B. (2010a). Multimedia Information Security Architecture Framework. In: *2010 5th International Conference on Future Information Technology (FutureTech),* IEEE. pp. 1–6.

Susanto, H., Almunawar, M. N., & Kang, C. C. (2012e). Toward Cloud Computing Evolution: Efficiency vs. Trendy vs. Security. *International Journal of Engineering and Technology – UK. 2*(9). Available at SSRN 2039739.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011a). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*, *11*(5).

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011b). I-SolFramework View on ISO 27001. Information Security Management System: Refinement Integrated Solution's Six Domains. *Journal of Computer, Asian Transaction*.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012b). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*, *2*(1).

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012c). A novel method on ISO 27001 reviews: ISMS compliance readiness level measurement. *arXiv preprint arXiv:1203.6622*.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012f). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*, *2*(1). *Preprint arXiv:1203.6622*.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012h). Information security challenge and breaches: novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*, *2*(1).

Susanto, H., Almunawar, M. N., Tuan, Y. C., & Aksoy, M. S. (2012g). I-SolFramework: An Integrated Solution Framework Six Layers Assessment on Multimedia Information Security Architecture Policy Compliance. *International Journal of Electrical & Computer Sciences*, *12*(1).

Susanto, H., Almunawar, M. N., Tuan, Y. C., Aksoy, M. S., & Syam, W. P. (2012a). Integrated solution modeling software: A new paradigm on information security review and assessment. *arXiv preprint arXiv:1203.6214*.

Susanto, H., Muhaya,F., & Almunawar, M. N. (2010b). Refinement of Strategy and Technology Domains STOPE View on ISO 27001. Accepted paper, International Conference on Intelligent Computing and Control – Future Technology (ICOICC 2010). Archived *preprint arXiv:1204.1385*.

The European Union Agency for Network and Information Security (ENISA). Information Security Awareness. Obtained from www.enisa.europa.eu. November 2012.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472–484.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173.

Tiller, J. S. (2010). *Adaptive Security Management Architecture*. CRC Press.

Toleman, M., Cater-Steel, A., Kissell, B., Chown, R., & Thompson, M. (2009). Improving ICT governance: A radical restructure using CobiT and ITIL. *Information Technology Governance and Service Management: Frameworks and Adaptations, Information Science Reference, Hershey*, 178–189.

Trend Micro. (2011). In: *Internet Content Security Software and Cloud Computing Security.* Obtained from: www.trendmicro.com

TribunNews.com. (2013). Indonesian ICT Markets. Obtained from www.tribunnews.com.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security*, *24*(2), 105–108.

Ungoed-Thomas, J. (2003). The e-mail timebomb. *Sunday Times*, p. 19.

Van Vliet, H., Van Vliet, H., & Van Vliet, J. C. (1993). *Software Engineering: Principles and Practice* (Vol. 3). Wiley.

Von Solms, B. (2001). Information security–a multidimensional discipline. *Computers & Security*, *20*(6), 504–508.

Von Solms, B. (2005). *Information Security Governance: COBIT or ISO 17799 or Both?*. Computers & Security, 24(2), 99–104. Elsevier.

Von Solms, B. (2005b). Information Security governance: COBIT or ISO 17799 or both?. *Computers & Security*, *24*(2), 99–104.

Von Solms, B., & von Solms, R. (2005). From information security to business security?. *Computers & Security*, *24*(4), 271–273.

Von Solms, S. H. (2005a). Information security governance–compliance management vs. operational management. *Computers & Security*, *24*(6), 443–447.

Wahono, R. S. (2006). *Software Quality Measurement Techniques*. Obtained from: www.ilmukomputer.com

Walenstein, A., Hefner, D. J., & Wichers, J. (2010, October). Header information in malware families and impact on automated classifiers. In: *2010 5th International Conference on Malicious and Unwanted Software (MALWARE),* IEEE. pp. 15–22

Whitman, M., & Mattord, H. (2011). *Principles of Information Security*. Cengage Learning.

Whitten, J. L., Barlow, V. M., & Bentley, L. (1997). *Systems Analysis and Design Methods*. McGraw-Hill Professional.

Wolfgang, P. (1994). *Design Patterns for Object-Oriented Software Development*. Reading, Mass: Addison-Wesley.

Woon, I. M., & Kankanhalli, A. (2007). Investigation of IS professionals' intention to practice secure development of applications. *International Journal of Human-Computer Studies*, *65*(1), 29–41.

Wu, D. D., & Olson, D. L. (2009). Introduction to the special section on "optimizing risk management: methods and tools". *Human and Ecological Risk Assessment*, *15*(2), 220–226.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy Magazine*, *1*(4), 15–23.

Zeltser, L., Skoudis, E., Stratton, W., & Teall, H. (2003). Malware: Fighting Malicious Code.