Towards evaluating security implementations using the Information Security Maturity Model (ISMM)

by

Saad Saleh Alaboodi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2007

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Saad Saleh Alaboodi

Abstract

Keywords: information security, cost of information security, IT security, security processes, maturity model, attack model, optimal security.

Information security is a common and ever-present concern for both private and public sector organizations. Information security protects information from a wide range of threats, risks, and vulnerabilities in order to ensure information availability, integrity and confidentiality, and hence business continuity.

This research seeks to use a heuristic-based investigation of the Information Security Maturity Model (ISMM), developed by the author, combined with a thorough review of existing models, to suggest considerable extensions. This shall merit various applications leading to establish a connective body of knowledge and bridge a gap in existing literature and industry regarding the information security implementation in light of use of international standards and models.

The ISMM model is neither based on a specific technology/protocol (e.g. PKI, IPSec, SSL) nor a certain system/product (e.g. Firewall, Antivirus, IDS), but rather an engineering approach towards a structured and efficient implementation of those technologies. The ISMM is a security-centric model that consists of five distinctive and ordered security layers, each of which has its own definition, scope, and characteristics. The model reflects the three key security processes (prevention, detection and recovery) and captures effects of people (visibility and sophistication) on every layer. It aims essentially to assess the maturity of any security implementation of any size and type (i.e. device, system, or environment).

New extensions of the ISMM work are put forward. Literature review is augmented by introducing a new classification of information security models. Additionally, new abstractions are introduced, first: the abstraction of security conceptual boundaries, which signifies rational priorities and captures the unavoidable interferences between information and physical security in any security context, second: the abstraction of ratios of resources utilization (i.e. computational power, energy, memory, and other costs). Further extensions include a new attack model that classifies attacks in terms of their impact. This leads to a new approach for analyzing attacks and study adversary's capabilities at different layers of both the ISMM and network models in the whole system, as one integrated entity against both single and hybrid attacks. As an example of one possible mapping and compatibility of the ISMM with other security-related models, the ISMM layers are mapped to their pertinent peers in network models (i.e. ISO/OSI and TCP/IP), which offers more information about security controls at each layer and its contribution to the actual overall security posture.

The ISMM offers a prompt and structured approach to identify the current security state of small communication devices, computing platforms, and large computing environments in a consistent manner. A cost-effective realization is achieved through the optimization of IT and security expenditure. Therefore, the model assists to minimize deficiencies in security implementation. Also, the identification of needs and goals of the following level in the ISMM hierarchy allows a strategic approach proportional to allowable resources to take place, as a result, both goals are reached and cost is reduced much faster.

This work is believed to facilitate grounds for future research endeavors such as applying these propositions on simulated examples, real life case studies, and developing a formula for the optimized distribution of security resources in a consistent manner with the best possible security level.

Acknowledgements

To begin, I would like to express my deepest thanks to my supervisor, Prof. Gordon Agnew. The freedom he gave me as a graduate student along with the valuable guidance, support and motivation was vital to achieving this degree. It made it a unique and outstanding experience, and I am really appreciative.

In addition, I would like to thank my thesis readers, Prof. Todd Veldhuizen and Prof. Pin-Han Ho, for devoting valuable time from their busy schedule and their constructive comments that have contributed to the quality and clarity of this research. I am also thankful to ECE graduate office staff for their kind cooperation and assistance. Special thank is also due to my dear friend, Abdulaziz Alkhoraidly, for his productive discussions and feedback throughout this research.

I am also grateful to the ministry of higher education in Saudi Arabia for granting me this scholarship and also for the continuous support from the Saudi Arabian Cultural Bureau in Canada throughout my study.

Thank you to my great mother, lovely brothers and sisters, and dear friends, past and present, for their continuous wit, encouragement and support during this journey. I am really thankful to each one of you and recognize that this work would not have been achievable without you. Thank you to everyone who has contributed to making my Master's experience exceptional and very enjoyable.

Thank You!

Dedication

In honor and memory of my great father, Saleh

To my beloved mother, Munirah

I owe the two of you the world

To…

Contents

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Introduction

Information and Communication Technology (ICT) has redefined work design and methodology, greatly reducing the time and effort needed to accomplish tasks, and facilitating both line performance and management decision-making process. ICT today is regarded as a vital business tool and a job-performance requirement in many organisations and at various levels within them.

The cost of information processing and acquisitions has been fundamentally altered by employing efficient information and communication systems. Information in the 21st century has become a major success factor to the organisations and states. Therefore, securing such a vital asset is a core business requirement that needs to be well planned and executed constantly in a structured manner [1]. However, information security is always characterized by three fundamental aspects: confidentiality, integrity, and availability (shortened as CIA). The application of these three aspects is broadened by including other properties such as authentications, non-repudiation, and accountability [2].

Although IT, and information security in specific, potentate a number of benefits, it also introduces special problems and concerns. Information systems do not produce benefits in their own right, but rather they are an important tool by which business processes and practices can be improved, resulting in business benefits [3]. As a result, ensuring security of information is a determinant factor for success utilization of such systems

1.2 Justification of the Study

Despite the increasing investment in information security and the strategic role played in today's organisations, understanding how to deliver information security successfully still remains one of the challenging issues facing the IT field [4,5,6,7,8,9,10]. In particular, the evaluation and delivery of reliable information systems benefits remains problematic and has attracted the attention of several researchers [11,12,13].

New risk areas that could have a significant impact on business success have uncovered the importance of information security and requirements for availability and robustness, examples may include misuse and abuse of information systems and external threats such as hackers and viruses.

Information systems however have come under severe criticism for failing to return value for the money invested. This criticism began in the early 1990s, and it continues to increase [3], failing to secure information assets is a main reason for not gaining expected return on investment on IT, which then might lead to business failure.

Several reasons leading to undertaking this research study in the area of information security are explained: First, information systems now often have a fully operational role rather than the support role of the past. Consequently, the effective work culture and reputation of the organization and its image in the eyes of its customers can be immediately influenced by any failure in its systems [14].

Second, investments in the ICT industry are large and increasing, and the technology budget is attracting more and more attention from top managers who would like to identify and clarify the benefits these investments are bringing to their business [15,16,17,7,11,10].

Third, significant barriers exist to successful implementation of these information and communication systems, many organizations have failed, in particular, in determining how to deliver IT systems successfully [4,18,5,6,19,9,12].

Fourth, security is a core requirement of organizations and states that needs to be integrated into business processes and culture [20, 1]. Hence, there is an innate need in both academia and industry for a structured and comprehensive methodology of information security process, it is required to be integrated in nature, assess progression, and provide a measure of the amount of "information security cost" in place.

Fifth, it is anticipated that the revisions and extensions of the Information Security Maturity Model (ISMM) [21] presented in this research can lead to a higher rate of success in securing computing environments.

1.3 Study Objectives

This research explores the area of information security implementation with the purpose of extending the ISMM work, which is intended for measuring and evaluating the maturity level of information security and its delivery from an integrative, inclusive, and holistic point of view.

Objectives of study presented in this research can be summarized by the following points:

- Provides a review of existing published security models and network models
- Extends the ISMM work in terms of its dimensions (layering, process, and people), propositions and dependencies
- Proposes a consistent abstraction of security boundaries, resources, amount of information security cost, and attacks
- Accordingly, suggests a new definition of optimal security notion from the ISMM model perspective
- Puts forward a new attack model that is consistent with the original ISMM model
- Shows the ISMM's compatibility with other security-related models through the use of its mapping to network models as one possible example
- Supports these propositions by an implementation snapshot of typical environment
- Offers analytical discussion of the ISMM model and its differentiated features as opposed to its peers
- Suggests possible further researches in the area

1.4 Research Questions

There are many aspects in this study that could be part of this section, however, in light of the aim and objectives of this study, the primary research questions are as follows:

- Has this subject been approached in previous studies (if any)?
- Can the ISMM model be extended to abstract and hence measure security level and amount of information security cost?
- Can this abstraction lead to sensible and coherent information when compared to the result of the actual security level on the ISMM?
- How can attacks be classified in terms of their respective impact on victim's computing device, platform, or environment instead of their origin or behaviors? Is it necessary that similar attacks should always have the same impact on different systems?
- Can layers of the ISMM be mapped to their corresponding layers in network models (i.e. ISO/OSI and TCP/IP)? At what layer(s) should security controls be implemented?
- Can this approach be used to provide consistent comparison of security level of different sizes and types of organizations/computing environments?
- How can this model be different from other maturity models in the industry? What are the added values and unique features it offers?
- Is it possible to derive relative estimates of security resource utilization (i.e. energy, processing power, and memory) and link them to their respective ISMM-specific metrics (layers, processes, quality, and ISO domains) and security control properties (parameters, risks)?
- How much is being spent on information security? On what? Are these expenditures justified?

1.5 Significance of the Study

Recent literature has confirmed that organisational investment in ICT continues to rise at an astounding rate. The literature also identifies a lack of success in achieving benefits from investment in ICT [16].

The importance of this study to practitioners and researchers is that it intends to bridge the gap between theory and practice by examining and evaluating the ISMM model and showing its compatibility with existing security-related models by linking it to standard network models as an example. The ISMM offers a new abstraction of optimal security notion and corresponding attack model. In this way, it will facilitate a new approach for measuring the amount of information security cost in any computing device, platform, or environment regardless of its size and type, leading to a more realistic estimate and correlation of security control parameters, resource utilization ratios, and the ISMM model metrics. Therefore, it facilitates more improvements in level of the maturity of security awareness and practice, as organizations seek to improve their ability to successfully compete by adopting and implementing recognized security standards and methodologies.

Researchers will find arguments made in this research are based on literature review of various information security and network models. It uses this multi-layer framework to bring heuristic evidence and evaluation of which security components and associated processes are essential to the successful

implementation and hence business survival, thus, extensions of the ISMM model provide a research vehicle of value and use to researchers. In addition, this research presents findings that will point the way to further researches in potentially rich and varied areas related to the information security delivery.

On the other side, practitioners (such as top managers, information systems executives, strategic planners, information security officers/auditors, and others) in their various firms should find this research beneficial as they move toward further implementation of information security in their organizations. This research intends to assist practitioners by providing an inclusive framework that acknowledges both aspects of defense-in-depth and attack-in-depth concepts. Therefore, it offers a reliable progressive picture of security posture.

1.6 Thesis Structure

This thesis details the reasoning, structure, core deliverables, findings and applications of the ISMM model. The thesis is divided into four chapters. Chapter one, Introduction, provides a general overview of the motivation for the research, following an explanation of the aims, objectives, and significance of the research. Chapter two begins literature review, it introduces the problem, information security key concepts, subsequently, an extended exposition of the current security standards (i.e. ISO17799), security models including the ISMM, and standard network models. Chapter three, Applications of ISMM, presents an extended explanation of the ISMM model along with a new definition of optimal security notion, followed by a newly derived attack model and one example of its compatibility with other models (the mapping to network models), supported by an implementation snapshot and discussion of the ISMM differentiated benefits as opposed to other published security models. Chapter four, Conclusion and Recommendations, provides a summary of research core deliverables, discusses the implications of the findings for practitioners and researchers, and suggests possible future research endeavours.

Chapter 2
Literature Review

2.1 Introduction

If you can't measure it, you can't manage it. [22]

This old saying is perhaps one of the most significant formulas for the information security professional. In this area, metrics are essential, be they operational or risk-based. Applying appropriate measurements that are consistent and reflect the latest security technology is a mandatory requirement for a successful security implementation. Technology never stops, continues to open more opportunities and threats, and hence cannot be controlled using outdated techniques.

Information security is safeguarding money, image, reputation and potential of the enterprise. The consequences of security incidents can be disastrous, but they are avoidable. The old physical approach to security remains important, but as businesses acquire a new virtual identity, it is not enough anymore. Technology cannot provide all answers to problems posed by people. This is because information security is not a technical issue but it is rather a business and management issue too. The answer is to adopt appropriate methodologies and controls to counter the ever-changing threats facing the organization, and to build these behaviours into day-to-day business process, operations, and culture instead of bolting it on as an optional duty or onetime project.

As mentioned in [23], technology is reshaping the economy and the relationships between businesses and consumers. The world economy is undergoing fundamental change. Billions of dollars are being exchanged at the speed of thought. Companies are now working on a 24/7 basis worldwide. Digital commerce is becoming the norm, rather than the exception. In fact, the very idea of a corporate headquarters is beginning to become a metaphysical concept, increasingly, the corridors in which managers run into each other are increasingly transforming from physical to electronic ones.

Information is an asset that, like other vital business assets, has value to the organization. It can exist in many forms, it can be printed or written on paper, stored electronically, transmitted by post or using electronic means, demonstrated in presentation, or spoken in conversation. Regardless of which form it may take, it should always be accurately identified, properly handled, and proportionally secured to its associated weight and importance of the organization.

Information security is one of the hottest issues in the current ICT industry, and will remain so into the foreseeable future. Information security to a business means having information available to it when it needs it, it means being able to trust in the integrity of information, and it is being able to trust that the information you receive has not been seen first by others.

2.2 Key Concepts

Information may be defined as the characteristics of the output of a process, these being informative about the process and the input. [24]

This discipline independent definition may be applied to all domains. To name a few, models of communication [25], perception, observation, belief, and knowledge are suggested to be consistent with this conceptual definition framework of "information" [24].

However, information is an asset which, like other important business assets, has a value to the organization and consequently needs to be suitably protected. Information comes in many forms, such as:

- Paper
- Electronic
- Video
- Audio
- Voice
- Knowledge

The ultimate goal of the information security process is to protect three unique attributes of information (sometimes refereed to as CIA triad). These are [2]:

- Confidentiality: is assurance of data privacy. Ensuring that information is accessible only to those authorized and having appropriate access, no one else should be granted that permission
- Integrity: is assurance of data non-alteration. Safeguarding the accuracy and completeness of information, so, measures must be taken to insulate information from any accidental or deliberate change to the contents
- Availability: is assurance that authorized users have reliable access to information and associated assets at the time they need it

These attributes are further augmented to include the following qualities [2]:

- Accountability is assurance in tracing all activities/actions to a responsible and authorized individual or process within a reasonable amount of time and without undue difficulty
- Non-repudiation: is assurance of delivery and identity between sender and recipient. That is the sender of data is provided with proof of delivery, and the recipient is provided with proof of sender's identity
- Authentication: is the process of verifying the identity of an individual, computer, computer program (i.e. process), or similar

There are various definitions in the literature for information security, each of which tries to bind it with certain perspective, sometimes linked to the protection of information assets themselves, others link it to Internet and sometimes it is associated with the protection of computer architecture as whole system.

Information security can be defined as:

> *The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use. [26]*

However, others attach information security to Internet communication:

> *The ideal state where all information can be communicated across the internet secure from unauthorized persons being able to read it and/or manipulate it. [27]*

Other definitions link security with computer system's security:

> *Deals with the techniques employed to maintain security within a computer system. [28]*

Over the years IT industry has witnessed an explosion of maturity models applied to different arenas and various industries. Generally, all maturity models have one thing in common: they work as a process reference model capturing the topmost view of the capability under study.

The Software Engineering Institute (SEI) at Carnegie Mellon University is a leading creator of Capability Maturity Models (CMMs) [29]. Three examples from the SEI are the Software CMM (SW-CMM), the Systems Engineering CMM (SE-CMM), and the CMM Integration (CMMI). However, a Capability Maturity Model (CMM) is generally defined as:

> *A model for judging the maturity of the…processes of an organization and for identifying the key practices that are required to increase the maturity of these processes. [29]*

However, SEI CMM is further augmented by incorporating the integrity notion to its original CMM and hence referred to as Capability Maturity Model® Integration (CMMI) which is:

> *A process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization. [29]*

Nevertheless, the Capability Maturity Model (CMM) describes an evolutionary improvement path from an ad hoc, immature process to a mature and more disciplined process and therefore captures the progression against time.

> *the idea behind a CMM is to define areas of a project that should have processes associated with them ("process areas") and then to measure the application of those processes ("capability level") in an organization. A more "mature" organization is defined as one whose processes are better defined and managed. [30]*

The researcher argues that most of these definitions reflect notions and terms captured from either software or systems engineering, or project management disciplines. These disciplines have one thing in common: their models are all established based on a clearly defined development life cycle, which has specific start and end time points, progressive stages, and the input and output of each stage is well anticipated and defined. This observation almost applies to system, software, and project management disciplines. It is worthy noting that information security on the other hand is about continuous process once started, and therefore has no established development life cycle and should never have one (i.e. open

life cycle). As a result, any maturity model that is designed for information security with such variances in mind will be more realistic and applicable in the security field.

2.3 ISO17799 Standard

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees work in partnership in fields of mutual interest. Other international organizations, governmental and non-governmental, in contact with ISO and IEC, also take part in the work.

International Standard ISO/IEC 17799 was originally prepared by the British Standards Institution under the name BS7799, and then adopted by ISO/IEC as ISO17799. ISO17799 is the most widely recognized international information security standard. The ISO17799 Standard is mainly intended for business managers and their staff to provide a model for planning and managing an effective information security management system. Therefore, the decision for adapting the model should be made at the strategic level for the organization. Also, the design and implementation of it is influenced by business needs and objectives. ISO/IEC 17799 as mentioned in [31] outlines ten distinctive information security controls (recently eleven domains, see appendix for more explanations):

1. Information security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access Control
8. System development and maintenance
9. Business continuity management
10. Compliance

2.4 Review of Maslow Work

Maslow produced the idea that a hierarchy of needs could explain behavior. His theory of individual development and motivation was originally published in 1943 [32]. His basic proposition as mentioned in [33] is that human needs are arranged in a series of levels, a hierarchy of needs. People want beings, they always seek more and more, and what they want depends on what they already have. The connection of Maslow's work and the ISMM is briefed in 3.2.5 (Model Dependencies).

Maslow identified a hierarchy shown as ranging through five main levels, they can be defined in the following way:

- Physiological needs, at lowest level:

These include a wide range of basic human needs that every human body requires in order to stay alive and function normally. It includes homeostasis such as home, satisfaction of hunger, sleep, and oxygen

- Safety needs:

These include safety and security, examples would include freedom from any physical attack or harm, and protection from danger

- Love needs:

Love or social needs include sense of belonging and social activities, it is about social support necessary to life. Examples would include friendship and sharing love with others

- Esteem needs:

These include both self-respect (desire for confidence and strength) and esteem of others (reputation, status, and recognition)

- Self-actualization need, at the highest level:

Self-actualization is about continuous development and realization of one's full potential

The degrees of satisfaction in Maslow's work are described in terms of decreasing percentages of satisfaction when moving along levels of the hierarchy. A false impression may be given that a need must be fulfilled completely before next level's needs arise.

> *Although Maslow suggests that most people have these basic needs in about the order indicated, he also makes it clear that the hierarchy is not necessarily a fixed order. [33]*

Maslow stated that these elements in the hierarchy are not to be considered as a rigid framework. There might be a number of exceptions to order indicated, a reversal of the hierarchy might apply on some people. Self-esteem as example may be seen as more important than love needs for some people.

However, in [34] Maslow's hierarchy shows the following properties:

- A need once satisfied is no longer a motivator, therefore, a need which is being satisfied over a period of time may be undervalued. People who have never suffered from thirst may tend to undervalue its effects on them, and regard drink as unimportant element for them
- A need cannot be effective as a motivator until satisfying those before it in the hierarchy
- If deprived of the source of satisfaction from a lower order need, it will again become a motivator
- There is an innate desire to move up the hierarchy as lower levels become satisfied to a considerable extent

- Level 5 (self actualization needs) is not like other levels: the opportunities presented cannot be exhausted or fulfilled completely

2.5 Overview of Information Security Implementation

For organizations to tackle and implement security requirements they generally either assign internal team or external expertise (outsourcing). However, outsourced management and monitoring of security systems is the fastest growing segment in the information security services market [35].

Current security dynamics show that there is a non-stop race between abusers (hackers, crackers and criminals) on one side and good guys (security bug busters and law enforcement) on the other side. It is very unfortunate that the abusers are always a step or two ahead in the game, leaving the good guys in catch-up mode.

One of the most publicized attacks on computer systems is the computer virus. However, it is becoming an increasing factor that employees, both present and former, are also posing great threats [36].

These observations and many others from various researches and surveys stress that any reliable security solution we might think of must be integrated and follow a structured approach. Attacks are increasingly becoming more sophisticated as both physical and logical attacks (i.e. breaking the physical and cyber systems together – say CCTV and communication systems respectively) are no longer separated. Therefore, the nature of information security threats has evolved into a more sophisticated dilemma which makes the job for security professional much harder. As a result of that, the framework that security solutions are being built on must respond to such new synergies and become more structured, integrated, and adoptive more than ever.

Fortunately, various security-conscious standards organizations such as the British Standards Institute, or BSI (www.bsi-global.com), and International Standards Organization, or ISO (www.iso.org), have undertaken the task of standardizing what we mean by the application of security.

The first of these standards is BS7799 developed by BSI, which was then adopted by ISO as ISO 17799. These standards define the spectrum of security controls that can be put into place. They also establish criteria for measuring those controls. However, determining the risk that the controls affect and the benefit to the organization requires experience and knowledge. There are other standards such as "Guidelines for the Management of IT Security" known as (GMITS standard). But ISO 17799 [37,38] has become the most widely accepted and recognized. Since so many security standards exist, it is often difficult to determine which best fits and applies to an organization.

A new breed of acronyms and buzzwords is finding its way to the attention of senior management as security jumps from nowhere in their attention list to become the top issue in their agendas. Obviously, the information security awareness is increasing and as a result of that the value of information is being recognized more than ever. But, still the real question is whether or not the pace of this increase is proportionate with the dynamics of current security threats and demands. However, this argument calls for a sophisticated and robust security system to protect organization assets that have significant impact on business operations and its survival.

2.6 Current Studies in Information Security Models

2.6.1 Introduction

> *Security and complexity do not usually get along. The highest security is usually accomplished with simplistic and elegant solutions to ensure that all of the entry points are clearly understood and protected…true security is based on education, knowledge, and experience. [39]*

Not all data has the same value to the organization. For the organization to govern the information assets, it should know first where the critical data resides and determine the value of different types of information before planning on appropriate measures. Because each piece of information may require different methods and levels of protection, identifying where each is located enables the organization to establish an integrated security solution balanced with its security needs, and hence, provides well-informed cost-benefits tradeoff of the organization resources.

> *The return on investment for any infrastructure is tied to the applications that use it, in commerce, government, financial and healthcare processes, the potential benefits are substantial. The return on investment from the applications it enables is the driver to use it. [40]*

However, one key issue here is the correct identification and estimation of information assets. Some information might not be perceived as crucial to the organization, but, still could become risky to the business and its reputation if it gets into the wrong hands. It is a costly mistake to underestimate the real value of information assets and the actual cost of losing it.

> *"Most organizations readily acknowledge that strategic plans are crucial to the success of a company. But do most companies really make an effort to protect these plans?" [20]*

It is instantly recognizable that much of the information that is so essential to successful business operations could be destructive if it is misused by employees, abused by outsiders, or should fall into the wrong hands. The exposure to unauthorized entities or individuals is significantly increased in networked environments, and increased drastically more when connecting to the Internet space. The protection mechanism must be done holistically and in an integrative way, thus providing the organization with the appropriate level of security at a proportionate cost.

Most models reflect three main processes of security: prevention, detection, and recovery system. Responsiveness to emerging security threats represents an innate need for any model in order to be adaptive and practical.

Nevertheless, it must be noted that

> *The presence of processes does not guarantee that the outcome of a project will be successful. But the presence of processes and the adherence to them by the organization should provide some insight into*

the ability of the organization to accurately predict the outcome and to repeat success achieved on earlier projects. [30]

However, there have been few security maturity models initiatives, most of them are developed from the industry, and unfortunately scarce literature exists in academia. The following sections elaborate on key published models.

2.6.2 SSE-CMM Model

The International Systems Security Engineering Association (ISSEA, established in 1999) is a non-profit membership organization dedicated to the advancement of Systems Security Engineering as a defined and measurable discipline [41]. The ISSEA has developed by an industry/government consortium a CMM, called the Systems Security Engineering Capability Maturity Model CMM (SSE-CMM). The SSE-CMM has been accepted by International Organization for Standardization (ISO) as ISO/IEC 21827 standard (ISSEA, Press Release) [42,43]. The SSE-CMM model provides industry best practices guidance without being specific as to how security solutions are implemented, therefore, it can be used as a vehicle to generate security requirements. It is worth noting that the SSE-CMM adopts similar context of the Systems Engineering Capability Maturity Model (SE-CMM). The SSE-CMM defines five capability levels (SSE-CMM):

Maturity Level	Description
Level 1	Base practices are performed informally
Level 2	Base practices are planned and tracked
Level 3	Base practices are well defined
Level 4	Base practices are quantitatively controlled
Level 5	Base practices are continuously improving

Table 2-1: SSE-CMM Capability Levels

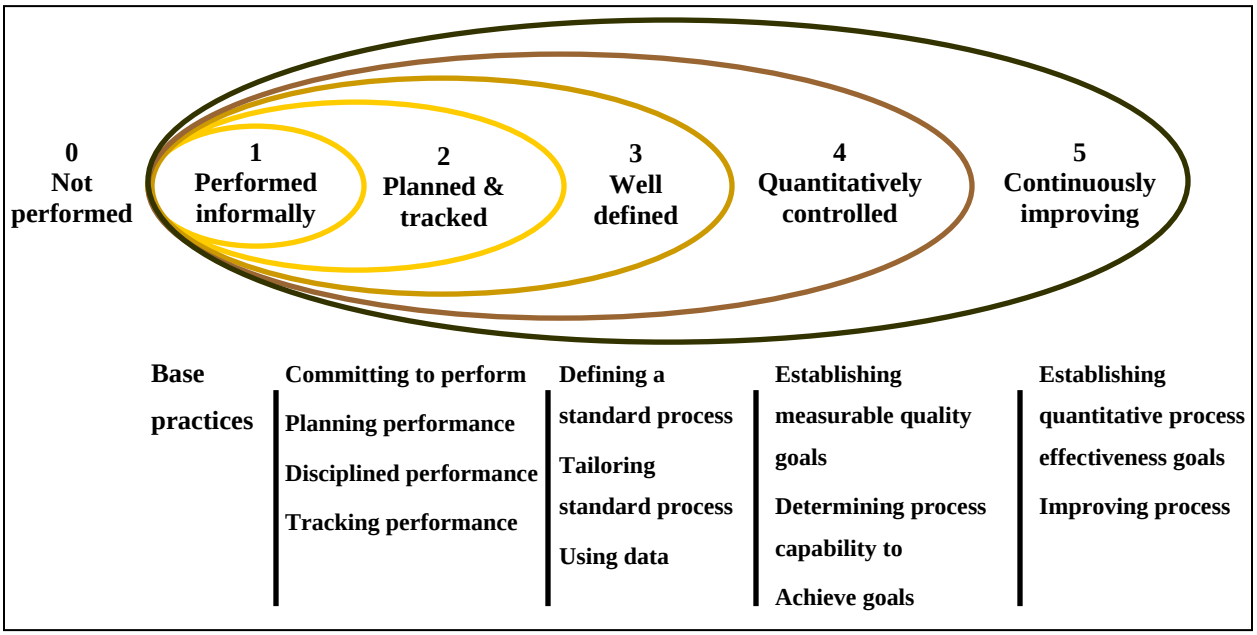

Figure 2-1: SSE-CMM Capability Levels [44]

Source: SSE-CMM Model Description Document, Version 3.0

The SSE-CMM defines eleven security-related Process Areas (PAs) and also includes another eleven process areas related to project and organizational practices (these process areas were adopted from the SE-CMM). Security-related process areas are defined in alphabetical order to avoid implications of a sequence (SSE-CMM):

PA01 – Administer Security Controls

PA02 – Assess Impact

PA03 – Assess Security Risk

PA04 – Assess Threat

PA05 – Assess Vulnerability

PA06 – Build Assurance Argument

PA07 – Coordinate Security

PA08 – Monitor Security Posture

PA09 – Provide Security Input

PA10 – Specify Security Needs

PA11 – Verify and Validate Security

Achieving capability level-1 on SSE-CMM requires 100% fulfillment of best practices predefined for this level. All other capability levels are considered achieved if 100% of the previous level and at least 80% of the current level is achieved [45].

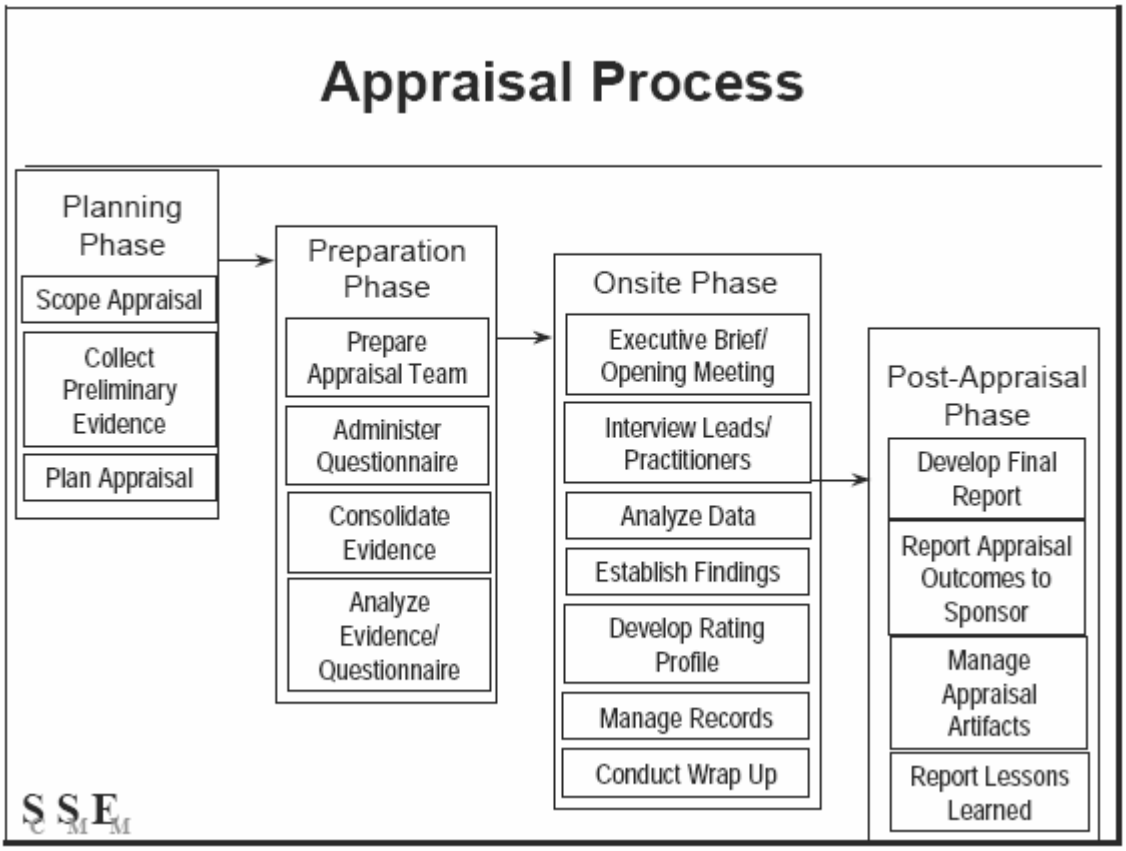

Figure 2-2: SSE-CMM Appraisal Process [45]

Source: SSE-CMM Appraisal Method (SSAM), Version 2.0

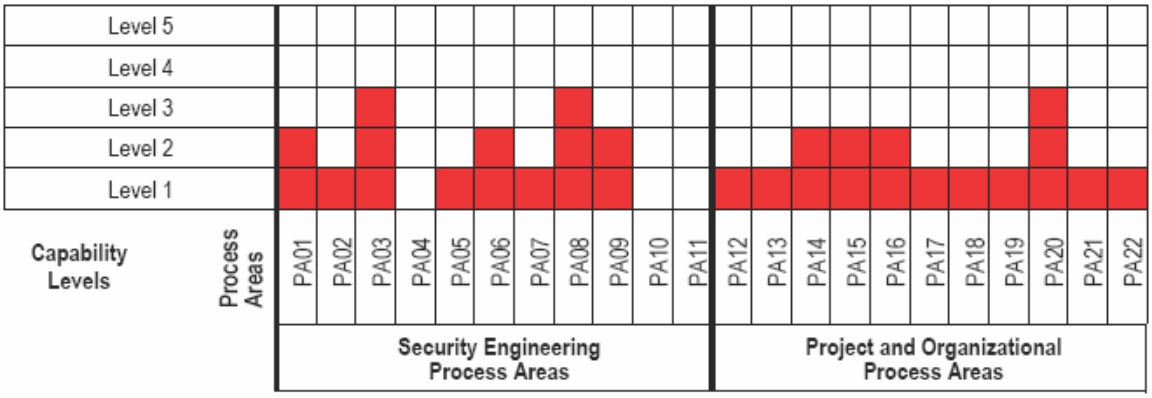

Figure 2-3: SSE-CMM Capability Levels [44]

Source: SSE-CMM Model Description Document, Version 3.0

SSE-CMM also identifies two types of metrics [43]:

Process Metrics: Metrics that could be used as a measure of the level of maturity for a specific SSE-CMM process area. Hence, they tell whether or not a mature process exists.

Security Metrics: A measure of the efficiency for a particular SSE-CMM process area. They could be quantitative or qualitative measures.

The main difference between these two process metrics is that the first type offers information about the behavior of process areas, where the second type tests the output of these process areas [41,43].

According to [44], the SSE-CMM® is a model focused on maturity of various security process areas to assess security engineering capability in linkage with the other engineering disciplines, as security spans over all of those disciplines (e.g., systems, software and hardware).

2.6.3 COBIT Model

As part of COBIT® (Control OBjectives for Information and related Technology) initiative [46], the ITGI has developed a simple information security governance maturity model, which is meant to enable an organization to establish a ranking for the way it manages information security. COBIT maturity model is derived from the maturity model that the Software Engineering Institute defined for the maturity of software development capability. Figure 2-4 and Table 2-2 depicts various maturity states and generally describes requirements at each state respectively [46].

COBIT IT processes assume application controls are governed by business process owners and hence integrated into business processes, as a result, COBIT cover general IT controls. The maturity levels are meant to describe possible states of these IT processes. They are not intended for use as a fulfillment model, where fulfilling lower level requirements is an eligibility key to promotion to higher levels. For each of the predefined 34 IT processes, COBIT helps management to identify [46]:

- The actual performance of the enterprise: the current state
- The current status of the industry: for benchmarking purposes
- The enterprise’s target for improvement: the desired state

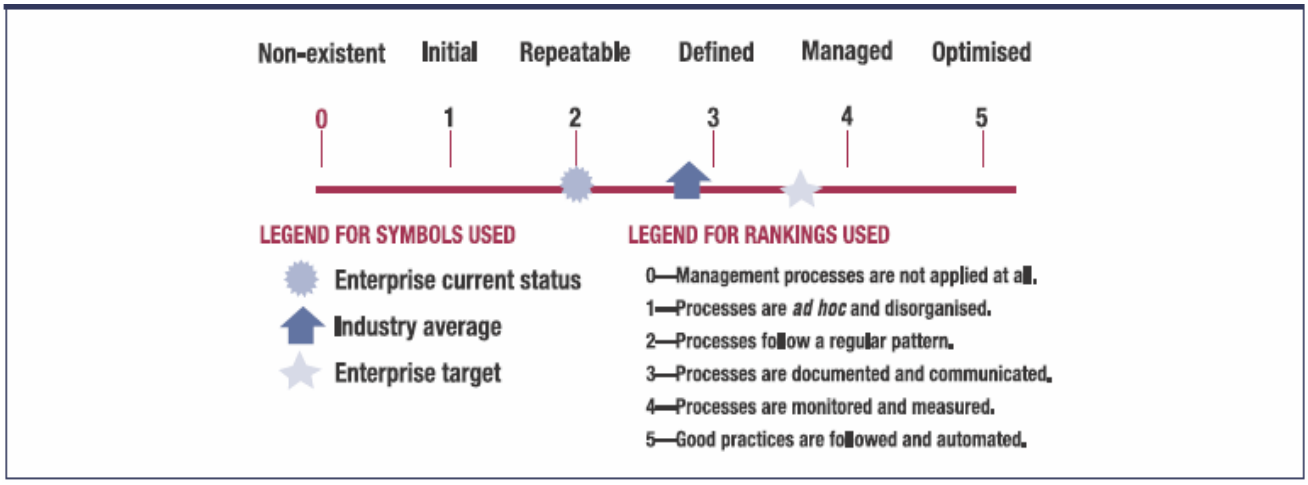

Figure 2-4: COBIT Maturity Model [46]

Source: COBIT Ver. 4, IT Governance Institute

Maturity Level	Description
Level 0 – Non-existent	The organization does not recognize the need for IT security. There is a complete lack of a recognizable system security administration process.
Level 1 – Initial / Ad hoc	The organization recognizes the need for IT security. But, the organization considers IT risks in an ad hoc manner, without following defined processes or policies.
Level 2 – Repeatable but intuitive	Responsibilities and accountabilities for IT security are assigned to an IT security coordinator. There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing.
Level 3 – Defined process	Security awareness exists and is promoted by management. An organization-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
Level 4 – Managed and measurable	Responsibilities for IT security are clearly assigned, managed and enforced. The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management.
Level 5 – Optimized	IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. Risk assessment has developed to the stage where a structured, organization-wide process is enforced, followed regularly and managed well.

Table 2-2: Levels of COBIT Maturity Model

2.6.4 NIST Model

The Computer Security Resource Center (CSRC) under the National Institute of Standards and Technology (NIST) has developed a security maturity model based on five consecutive levels. The model links the maturity at any level with the level of documentation in place, and assumes fulfillment of previous level requirements in order to be promoted to higher level (i.e. NIST is a threshold model) [47]. The following table provides a brief description of the model details:

Maturity Level	Description
Level 1: Policies	Formal documented and updated policies are communicated to all employees. Policies establish a continuous risk assessment and implementation and cover major facilities and operations. Clearly assign roles, responsibilities, and measures.
Level 2: Procedures	Formal documented and updated policies cover all security controls. Procedures clearly identify where, how, when, when and on what the procedure to be performed. Procedures document controls implementation.
Level 3: Implementation	Procedures are communicated to respective individuals and controls are implemented in consistent manner. Initial testing is performed.
Level 4: Test	Adequate tests are routinely performed to ensure that all policies, procedures, and controls are acting as intended. Effective corrective actions, self-assessments, and independent audits are performed.
Level 5: Integration	Policies, procedures, implementations, and tests are continually reviewed and improved. IT security program is embedded into culture and an integrated practice. Continuous cost-benefit analysis is performed.

Table 2-3: Levels of NIST Maturity Model [47]

2.6.5 ISM3 Model

Canal and his coauthors have developed a maturity model for Information Security Management (ISM)[48]. The model is called Information Security Management Maturity Model (ISM3 or ISM-cubed). This model is more abstract compared to other maturity models and is intended to evaluate and implement process-oriented information security management (ISM) systems. ISM3's approach is based on the

application of ISO9001 quality management concepts to ISM systems. ISM3 defines maturity in terms of the operation of key ISM processes and requires security to be aligned with business objectives [48].

Processes are allocated to maturity levels according to a spectrum, from a basic ISM system to an advanced one with cost taken into account in order to realize return on investment at earlier maturity levels.

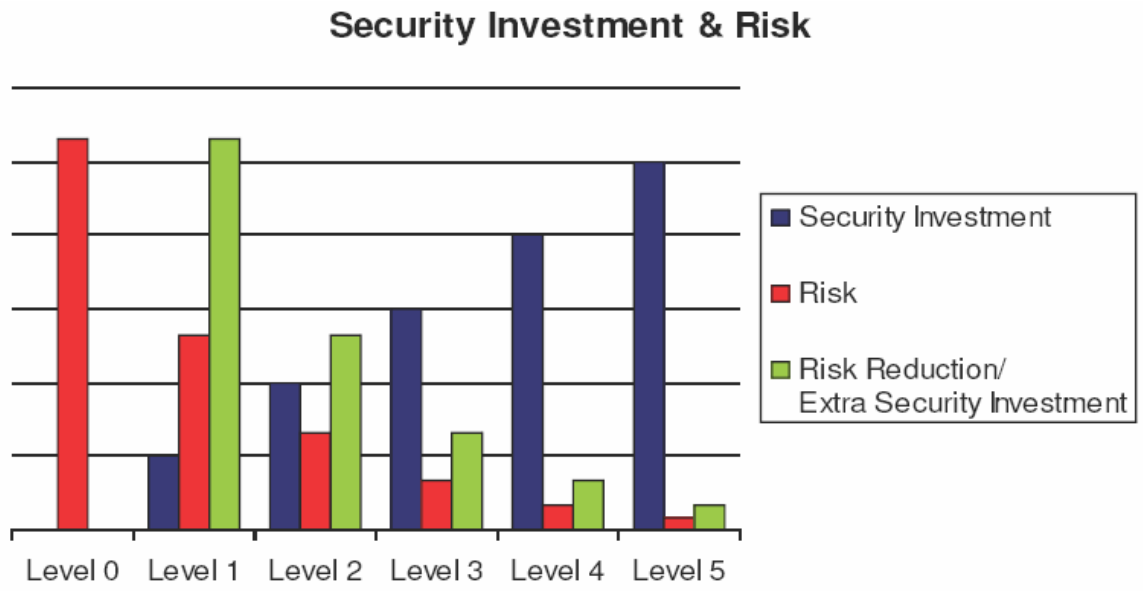

Figure 2-5: ISM3 Maturity Model [48]

Source: Canal (2006) Version 1.20

The correlation between security improvement and investment on security is supported by Mayfield's Paradox:

> *Keeping everyone out of an information system requires an infinite amount of money and getting everyone onto an information system requires an infinite amount of money, but the costs between these extremes are relatively low. [49]*

An organization may choose to implement any of the defined processes at any stage of maturity assuming its relevance to specific security objectives. However, as clarified in Table 2-4, ISM3 defines five maturity models. Security risks and associated investment represent the sliding scale at every level in ISM3.

Maturity Level	Description
ISM3 Level 1	This level should result in a significant risk reduction from technical threats, for a minimum investment in essential ISM processes.
ISM3 Level 2	This level should result in further risk reduction from technical threats, for a moderate investment in ISM processes.
ISM3 Level 3	This level should result in the highest risk reduction from technical threats, for a significant investment in Information Security processes.
ISM3 Level 4	This level should result in the highest risk reduction from technical and internal threats, for a high investment in Information Security processes.
ISM3 Level 5	This level assumes the compulsory use and continuous improvements of process metrics.

Table 2-4: Levels of ISM3 Maturity Model

The deployment of ISM3 differs depending on whether or not there is an existing ISM system. If an ISM system is in place, the initiative starts by conducting a gap analysis of the systems and processes in place against the target ISM3 maturity level followed by ensuring that quality management is aligned with the organization's security objectives and ISM3 standard. Otherwise (in case of new ISM implementation), the ISM3 is embedded into ISM formation process. However, Information Security Management consists of three management levels each of which has its own goals, practices, and processes [48]:

- Strategic (Direct and Provide), which deals with broad goals
- Tactical (Implement and Optimize), which deals with the design and implementation of the ISM system
- Operational (Execute and Report), which deals with achieving defined goals by means of technical processes

ISM3 is about process management. It suggests that, through well-defined processes, the information security is enhanced, risk is mitigated and, hence, maturity is measured.

However, the performance of a well-designed ISM system depends on the budget, the capability and the commitment of those involved in running it. The use of ISM3 is about the way security is conducted. It does not guarantee that a process will perform properly or will deliver correct results, it only guarantees that the cause of faults is not ill-structured process [48].

2.6.6 OCTAVE Model

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) is a risk-based strategic assessment and planning technique for security developed at Carnegie Mellon University. The OCTAVE approach considers both organizational and technological issues [50]. OCTAVE is self-directed, meaning

that people from an organization assume responsibility for setting the organization's security strategy [51].

OCTAVE as a process is organized into three phases [1][51]:

- Phase 1: Build Asset-Based Threat Profiles – The analysis team determines information-related asset measures. Then, it identifies threats to each critical asset, creating a threat profile
- Phase 2: Identify Infrastructure Vulnerabilities – The analysis team examines network and information technology components related to each critical asset and their resistance to network attacks
- Phase 3: Develop Security Strategy and Plans – The analysis team identifies risks to the organization's critical assets and creates a protection strategy for the organization and mitigation plans to address the predefined risks to the critical assets

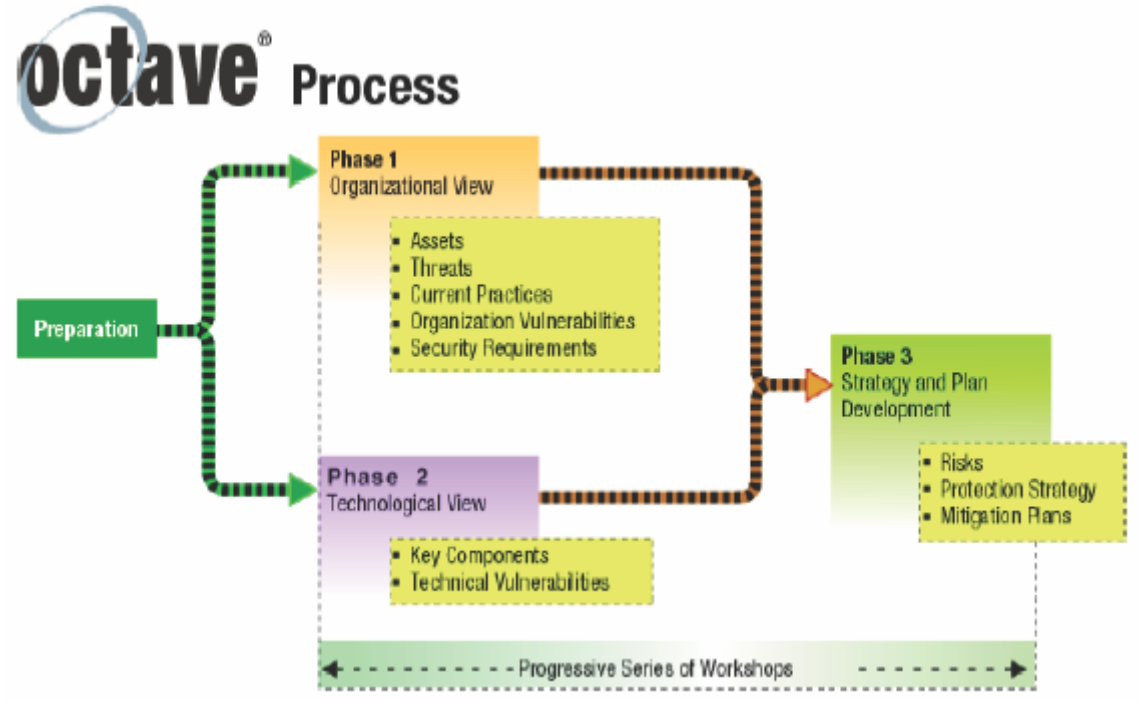

Figure 2-6: OCTAVE Process [1][51]

Source: Introduction to OCTAVE approach, Carnegie Mellon, Software Engineering Institute August 2003

[1] ©2003 Carnegie Mellon University permission is granted by the Software Engineering Institute. All rights reserved. Used by permission

2.6.7 CRAMM Model

The Central Computer and Telecommunications Agency (CCTA) was tasked by the UK Government's Cabinet Office to investigate the risk analysis and management methods currently in existence within Central Government for information security. As a result, a new framework was developed by CCTA which drew upon all of the existing best practices under the title of the CCTA Risk Analysis and Management Method (CRAMM) [52].

CRAMM is a comprehensive risk assessment tool that is compliant with BS7799 and ISO 17799. CRAMM has a database of over 3000 security controls referenced to relevant risks and ranked by effectiveness and cost. CRAMM addresses tasks such as [52]:

- Asset dependency modeling
- Business impact assessment
- Identifying and assessing threats and vulnerabilities
- Assessing levels of risk and identifying required controls

CRAMM implementation is a phased approach covering both technical (e.g. IT hardware and software) and non-technical (e.g. physical and human) aspects of security. To evaluate these components, CRAMM is divided into three stages:

- Asset identification and valuation:

  The objective is to identify the physical (e.g. IT hardware), software (e.g. application packages), data (e.g. the information held on the IT system) and location of assets that make up the information system

- Threat and vulnerability assessment:

  The objective is to determine the likelihood of deliberate and accidental occurrences of various incidents and then to calculate the level of the underlying or actual risk

- Countermeasure selection and recommendation:

  Utilizing the CRAMM countermeasure library (consists of over 3000 detailed countermeasures organized into over 70 logical groupings), appropriate countermeasures are selected proportionately to predetermined assets and risk levels

---

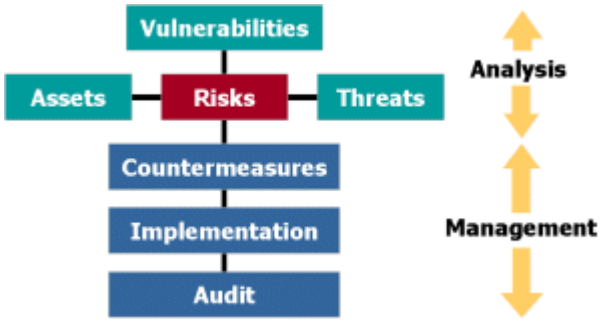

Figure 2-7: CRAMM Process [52]

Source: CRAMM, Version 5.1, http://www.cramm.com

2.6.8 SPMM Model

The Security Program Maturity Model, developed by Chapin and Akridge [53], is an approach that distinguishes between maturity and quality of any security program and offers a model that measures both aspects and presents them combined together into one picture of security posture or dashboard display. Maturity from SPMM's perspective is depicted by a simple judgment of the existence or nonexistence of large number of security elements derived from ISO17799 standard, where quality is depicted using a three-tiered quality factor: low, medium, and high, trying to transform the subjective metric (quality) into an objective one. The following table describes the ISO17799 domains covered by the model and associated elements of each domain:

ISO 17799 Categories	No. of Elements Measured	Items Covered by Elements
1. Overall security management	11	Business need, strategy, commitment, roles and responsibilities, policies and procedures
2. Asset classification and control	5	Valuation, risk assessment, business ownership, labeling and handling, inventory
3. Personnel security	8	Hiring and termination, roles and responsibilities, screening, training, reporting, review
4. Physical and environmental security	12	Perimeters, environmental hazards, risk assessment, access controls, safety, asset removal and destruction, monitoring, incident handling, awareness, cooperation
5. Access control	11	Perimeters, risk assessment, access controls, authentication, need to know, user responsibility, access updating, monitoring, mobile computing, incident handling
6. System development and maintenance	9	Standards, life cycle model, review, gap analysis, requirements planning, testing integrity and certification, code repository, release management, retirement
7. Communi-cations and operations management	16	Standards, all methods of e-communications, operations procedures, monitoring, backups, exception handling, updates and patches, help desk, change management, cryptographic systems, media handling, malicious code, system acceptance, documentation library, capacity planning
8. Organizational security	11	Security function, monitoring, advisory, auditing, forum, awareness training, segregation of duties, penetration and vulnerability testing, incident handling, cooperation
9. Business continuity management	7	Risk assessment, prioritization, backups, business continuity/ disaster recovery planning, testing, updates
10. Compliance	10	Regulatory, contractual, intellectual property, labeling and handling, record retention, auditing, sanctions

Table 2-5: SPMM: General outline of the security maturity model [53]

Source: Chapin and Akridge, How Can Security Be Measured, ISACA, Vol. 2, 2005

The following table clarifies the maturity using a sample of one domain (Asset Classification and Control) and the model suggested order for the implementation of its elements:

Order Performed	Program Maturity Elements— 2. *Asset Classification and Control*
1	2.1 **Valuation** is performed to identify and understand information assets to protect.
2	2.2 **Risk assessment** is performed to identify and quantify threats to information assets.
3	2.3 Information assets have defined **system custodians** and **business owners**.
4	2.4 Information assets **classification labeling** and **handling** procedures are developed.
5	2.5 An **asset management** inventory program is installed to handle assets on an ongoing basis.

Table 2-6: SPMM: Sample elements from security maturity model [53]

Source: Chapin and Akridge, How Can Security Be Measured, ISACA, Vol. 2, 2005

The following table depicts the quality of a specific element as a successor step of its maturity:

Program Maturity Element	*If maturity element is implemented, then…*		
	Low-quality Threshold	Medium-quality Threshold	High-quality Threshold
2.4 Information Assets **classification labeling** and **handling** procedures developed	Procedures developed but not implemented	Assets partially classified	Pervasive classification throughout entire organization

Table 2-7: SPMM: Sample of a quality measure from security maturity model [53]

Source: Chapin and Akridge, How Can Security Be Measured, ISACA, Vol. 2, 2005

2.7 Information Security Maturity Model (ISMM)

Information security is achieved by adopting and implementing the appropriate set of controls, which could be policies, procedures, practices, organizational structures or software tools and functions. If these controls are not well established, the objective of security will not be met and hence the security investments will have no or low significance to the organization benefits.

Security cannot be achieved by only technical means, it should be augmented by appropriate management and procedures [31]. As detailed in [21] and briefed in [1], the Information Security Maturity Model (ISMM) developed by the author is a five-level process-based framework. It is developed

for maturity assessment of information security and evaluation of the level of security awareness and practice (which are affected by people, process, and technology) at any ICT-enabled organization, be it public or private sector. Furthermore, it helps to better understand where and to what extent the three main processes of security (prevention, detection, and recovery) are implemented and integrated (see Figure 2-8).

In essence, the ISMM model is intended to assist organizations in maturing their information security posture in order to improve business performance and hence business continuity. It reflects both technical and social engineering aspects of information security aspects (hence the words awareness and practice), and their implementation against the three fundamental security processes.

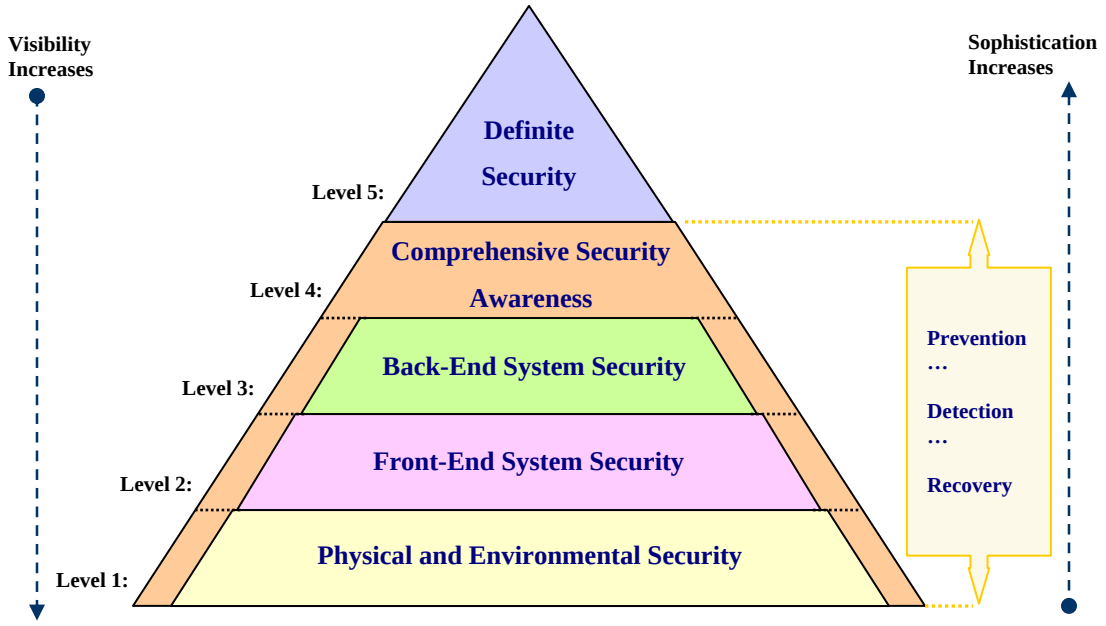

Figure 2-8: Information Security Maturity Model[1]

The ISMM model depicts three different dimensions [21,1], these are:

- **The layering dimension:** demonstrated on the model by five consecutive layers starting from physical and environmental security layer at the bottom and moving up the hierarchy to the definite security layer. This dimension captures the technology aspect of security
- **The process dimension:** represented by the three fundamental security processes: prevention, detection and recovery. This dimension captures the process aspect
- **The people dimension:** represented by two indices, sophistication and visibility indices. These indices are exhibited and exposed on the people side. Hence, this dimension captures the people's effect

Chapter 3 provides revised explanations of these three dimensions and new extensions towards the application of the whole model.

[1] ©2006 Information Systems Audit and Control Association. All rights reserved. Used by permission

2.8 Standard Network Models

2.8.1 Introduction

Networking functions are organized and described in a layered architecture. There are two main networking models: the ISO/OSI (International Standards Organization/Open Systems Interconnect) reference model and the TCP/IP (Transmission Control Protocol/Internet Protocol) reference model. These two models share the same idea behind the layering approach: the services of one layer are implemented and offered by the layer immediately below it, and different layers can be designed more or less independently for specific functions [2].

2.8.2 ISO/OSI Model

The ISO/OSI reference model was developed in 1984 by the International Standards Organization (ISO). The model is considered a conceptual framework of standards for communication in the network across different platforms and applications by different vendors and, hence, the primary architectural model for inter-computing and internetworking communications. The ISO/OSI model defines the communication process into a set of steps across seven layers. The main purpose of multiple layers is to provide clearly defined functions (a task or a group of tasks) in order to improve internetworking connectivity between different systems [2,54,55,56,57,58].

Layer	Function	Examples
Application	Interacts with operating system and applications (user access)	CMIP, FTAM, VTP, RTSE, X.400, X.500
Presentation	Converts data into standard format	ISO-PP: OSI Presentation Layer Protocol
Session	Establishes and maintains end-to-end connections	ISO-SP: OSI Session Layer Protocol
Transport	Reliable end-to-end packet transmission	ISO-TP: OSI Transport Protocols: TP0, TP1, TP2, TP3, TP4
Network	Routing, multiplexing, and addressing functions	CONP, ES-IS, IS-IS, ISO-IP, CLNP
Data link	Reliable node-to-node packet transmission	IEEE 802.2, IEEE 802.3, IEEE 802.5, FDDI, X.25
Physical	Physical characteristics of the network (bit transmission carrier)	IEEE 802.2 hardware, IEEE 802.3 hardware, FDDI hardware, X.25 hardware

Table 2-8: Functions of ISO/OSI network layers

2.8.3 TCP/IP Model

The TCP/IP reference model was developed in 1970s by the Defense Advanced Research Projects Agency (DARPA), an agency of the United States Department of Defense (DoD). The TCP/IP model is

sometimes referred to as the TCP/IP protocol stack, it is basically a layered abstract description for communications and computer network protocol design. The model does not exactly match the ISO/OSI seven layers, however, there is no universal consensus regarding a specific description of TCP/IP layers but it is generally agreed that there are fewer levels than the seven layers of the ISO/OSI model (usually described in terms from three to five layers). However, the TCP/IP model does exclude some features and combines others found under the ISO/OSI model [2,54,55,56,57,58].

Layer	Function	Examples
Application	Interacts with operating system and applications (user access). It includes functions of the ISO OSI upper three layers.	SMTP, FTP, SSH, HTTP
Transport	End-to-end message transmission. The Transmission Control Protocol (TCP) guarantees that information is received as it was sent. The User Datagram Protocol (UDP) performs no end-to-end reliability checks.	TCP, UDP, RSVP, DCCP
Network	Establish and maintain end-to-end connections (addressing and routing functions).	IP (IPv4, IPv6), ICMP, IGMP, ARP
Data Link	Reliable node-to-node packet transmission.	Ethernet, Wi-Fi, PPP, FDDI, ATM, Frame Relay, GPRS, Bluetooth
Physical	Physical characteristics of the network (bit transmission carrier).	Modems, ISDN, USB, Ethernet physical layer, Wi-Fi, GSM, Bluetooth

Table 2-9: Functions of TCP/IP network layers

The following table demonstrates the mapping between ISO/OSI and TCP/IP reference models:

	Data Unit	Layers in ISO/OSI Model	Layers in TCP/IP Model
Host Layers	Data	(7) Application	(5) Application
		(6) Presentation	
		(5) Session	
	Segments	(4) Transport	(4) Transport
Media Layers	Packets	(3) Network	(3) Network
	Frames	(2) Data link	(2) Data link
	Bits	(1) Physical	(1) Physical

Table 2-10: Layers mapping between ISO/OSI and TCP/IP network models

2.9 Summary

We live in an information age, where information technology drives our economy, pervades our culture and assists in educating our people. Understanding technology impact, its exposure and sophistication, facilitates a solid ground for adopting integrated security approach that best fits security needs and organizational culture. This is obviously fundamental to the success of our current and future digital economy.

Alan Greenspan has mentioned that the rapid growth of the economy in the past ten years has been mostly due to synergies gained via information technology, and the resultant push in capital spending as a result of technology implementation as information technology is a major influencer on economy [59].

Information security at present is in the forefront as a leading technology requirement. All organizations, whether they are commercial, nonprofit, or governmental, must face the realities of an electronic world where information security practices are not even vital to organization success but rather to its survival.

Security measurement is a very subjective issue which varies according to different people perspectives, and process and technology deployed in any ICT-enabled environment. As a maturity model, the ISMM presents an architecture model applicable at any ICT-enabled organization of any size. The ISMM model will be very useful for the governance and delivery of information security in any organization where information asset is of value.

It has become essential for organizations, both government and commercial businesses, to adopt vendor and product-neutral methodologies, to circumvent traditional risk analysis which requires constant maintenance of threat assessment, vulnerability assessment, and asset values, and to avoid over-estimating use of best practices which are not tailored to the organization applying it.

It is very common in security standards to demonstrate comprehensive domains of information security. But, organizations still need to determine and structure and scope of applicability of security controls in every domain, and to know exactly the security conceptual boundary of controls in place. Security policy as an example is mistakenly considered by many people in the IT field to be about the very basic access controls such as minimum password length, and as a result, some IT managers consider themselves as applying strict security access policies where in reality they only apply a very small portion of a prevention mechanism at a specific security boundary, the application level.

However, from the above reviews of various standards and security models, approaches to information security can be classified into five distinct types as follows:

No.	Approach/Model Type	Examples	Remarks
1	Best practices oriented	BS7799, ISO17799, ISO27001	Compiled list of best practices.
2	Process oriented	SSE-CMM, ISM3, COBIT, NIST	Use elements specified in other standards and best practices.
3	Risk oriented	CRAMM, OCTAVE	Use basic assets and risk assessment methodology.
4	Controls oriented	SPMM	Use elements specified in other standards and best practices.
5	Security oriented	ISMM	Measures security itself, which is the contribution of this research.

Table 2-11: Categorization of various security models

Table 2-12 shows a brief comparison between the ISMM model and other security models in general and maturity models in specific.

No.	ISMM	Other security models
1	Offers specific view of the security system (determined view).	Offer very high level view of the security system (topmost view).
2	Measures how good "security itself" is implemented.	Measure how good "process itself" is implemented.
3	Defines/abstracts security boundaries.	Don't define/abstract security boundaries.
4	Defines/abstracts security system resources.	Don't define/abstract security system resources.
5	Derives a relevant attack model.	Independent from attack models.
6	Captures process, people and layering dimensions.	Capture process maturity dimension only.
7	Based on the security life cycle (an open cycle).	Usually based on either project management or software engineering development life cycles.
8	Simple to understand and easy to apply.	Complex, expensive and hard to apply.
9	Can be applied to small organizations, independent machines and communication devices (scalable).	Cannot be applied to small organizations or independent machines (inflexible).

Table 2-12: Comparison between the ISMM and other Models

The ISMM model responds to the following industrial needs:

1. A relative measure of where the enterprise is in terms of security level. The model provides an efficient method to perform gap analysis against industry peers and best practices

2. An indication of security adequacy measure (i.e. evidence of organization's stance on security), to reduce the ever-growing risk interdependencies among different organizations of different sizes. Such applications may include e-government, e-commerce, partnering, outsourcing and contracting endeavors

3. An approach to efficiently decide where to go, a measure for progress, and a method to set priorities for achieving goals and further improvements

4. Security investments are still protected when the ISMM is adopted. As ISMM is compatible with the implementation and use of other security standards and maturity models such as ITIL, Cobit, ISO 27001 [60], and ISO 17799 [61]. This compatibility protects the existing investment in security systems when they are enhanced using the ISMM

Chapter 3
Applications of ISMM

3.1 Introduction

This chapter starts with an extended overview of the ISMM work, covering all of its properties: layering, processes, and people dimensions, beside model propositions and dependencies. This addition introduces a new abstraction of both information security conceptual boundaries and corresponding resources used within a computing environment. Consequently, facilitating grounds for further extensions such as measure of amount of information security cost, definition of optimal security, attack model, mapping to network models.

3.2 ISMM Extended

3.2.1 The Layering Dimension

The ISMM model depicts five different security layers, each of which has its own definition, scope of applicability, and characteristics. There is also an implicit layer at the very bottom (called ad-hoc layer or layer 0), this implied layer suggest no controls, policies, or any structured security activities are in place:

Physical and Environmental Security (level 1):

The controls at this level aim at preventing unauthorized physical access or interference with the organization or ICT equipments and information assets. Physical security of IT equipment and having restricted access control to operations room are clear examples of security controls at this level. Other mechanisms may include site design and layout, environmental components, power and fire controls, and emergency response readiness to protect people, data, systems, and the facility itself.

Obviously people with modest knowledge and common sense can identify some of the security controls at this level (e.g. having recording cameras or security gates). Typically these controls are more visible and exposed to people than other controls (e.g. platforms configuration). Therefore, the ISMM model implies that visibility index at this level is the highest compared to other higher levels. On the contrary, sophistication index (management requirement and knowledge sophistication) is the lowest as shown in the diagram.

The ISMM also shows that three main processes are applied on this level. For example, security gates could be used as a prevention mechanism, recording cameras as a detection mechanism, and while having duplicated cameras in the same area using different power sources represent a recovery mechanism for this particular control and not the whole security system.

Front-end System Security (level 2):

Front-end system security is about all application level system functions and integrity requirements between the application component itself and end-user interface. It suggests that application data should be well protected against any potential threat that might cause loss, damage, or unauthorized access by

either internal or external users. Examples of security controls are application access controls and application change management process.

The ISMM model suggests that the visibility index decreases here as compared to level-1. Clearly, the number of people who are exposed to this security boundary (e.g. application developers and users) is less than at the previous level (who could be people from outside the organization itself). On the other hand, the sophistication index is higher at this level compared to previous one. Clearly, this is due to the deeper knowledge required for both security awareness and practice of security controls at this level.

Prevention, detection, and recovery processes apply at this level, too. Restricting application access to authorized users (prevention), logging application access (detection), tracking application changes (recovery) are examples of common practices in this level.

Back-end System Security (level 3):

The back-end system security boundary includes any resource (e.g. hardware, software, process) that is beyond application level components. The underlying network infrastructure and internal and external communication devices constitute the major components at this level.

Examples may include data and communication cryptographic mechanisms, router and switch access lists, configuration of data center platforms, intrusion detection systems and firewalls.

The ISMM suggests that the visibility and exposure of such controls at this level decreases compared to lower levels as equipment is presumably placed in less accessible areas. The underlying encryption mechanism as an example is almost transparent to even application users. Additionally, the required depth and sophistication of knowledge at this level is usually more than what is required at front-end system security controls. This is further justified by looking at the available average number in the IT community of application programmers as opposed to cryptographic specialists. Therefore, the sophistication index increases at this conceptual boundary.

On the other hand, the three main processes apply here too. As a prevention control, the deployment of encryption mechanism for network traffic may be applied, deployment of an IDS system as a detection and installation of backup communication lines as a recovery mechanism.

Comprehensive Security Awareness (level 4):

Security awareness requirements are identified and affected by people. Expenditure on security awareness programs needs to be balanced against the business harm likely to result from people awareness failures. Therefore, this level implies the scope of security awareness to include the whole of the organization staff and encapsulates the practice of lower level requirements, hence the word “Comprehensive”. This layer persuades the need for the organization to operate in a security-conscious culture in all technologies deployed across all lower layers.

Although use of the latest security products and the development and implementation of information security policies, standards, procedures and guidelines are imperative to the success of the overall information security system, it will be an ineffective system if all of these products are not brought to the attention of those people who are expected to adhere to them. No amount of technology can diminish the human factor. The author stresses that the right awareness drives the right practice of security phenomenon which is the main reason for having security awareness at lower levels too (level 1, 2, and

3). The commitment of all employees, especially top level management, is a major requirement at this level. Hence, involvement is first step towards gaining real commitment.

Technology alone cannot ensure the security of a system:

> *Most advanced equipment and security safeguards are to no avail if all the users are not properly trained to be part of the security plan. [62]*

The awareness of people is an unseen element but is demonstrated by their behaviors, which explains why the ISMM suggests that the visibility index is less at this level when compared to lower levels. On the other hand, the depth and sophistication of knowledge and management requirements (sophistication index) is the highest compared to lower levels, since it is solely about people and people alone!

The three main processes of prevention, detection, and recovery are applied too. Having appropriate awareness training courses, observing people behavior, continuous improvements of security controls are examples of possible practices embedded into these processes.

Definite Security (level 5):

Security measurement is always a subjective rather than an objective issue. Accordingly, different people have different perspectives. This layer captures applied security knowledge, culture and confidence in the organization, as applied security knowledge is essentially based on critical thinking, observation, and analysis abilities. However, definite security could be a virtual feeling but in reality, it can never be fulfilled completely since security in general is a continuous process and associated with needs, leading to motivation, execution, confidence, trust and hence emotion (feeling secure). Therefore, the presence of this layer is essential to the model, first, to reflect this vital security boundary, second, to point out security is a continuous process once started (i.e. open life cycle) and third, to show that there is no such thing as a 100 percent secure computing environment or platform or communication device.

There is no denying that there is no such system that is absolutely secure since there is no foolproof "silver bullet" system or security solution. There is always a probability even very small that something wrong could happen. However, there are many systems that are rated as highly secure and designed in such a way so that they almost can detect and recover from many known incidents immediately. It is worth noting that this layer differentiates a key characteristic of this security maturity model from others which are usually based on software engineering and project management development life cycles.

3.2.2 The Process Dimension

The process dimension of the ISMM model depicts the three main processes of security, these are:

Security Prevention Process:

Information is an asset that requires protection commensurate with its value. Security measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional. During the prevention phase, quality security policies and procedures, controls and processes should be designed and implemented covering all various conceptual boundaries from the ISMM model perspective.

Security Detection Process:

Detection of a system compromise is extremely critical: detection process suggests that proper systems (e.g. Perimeter IDS and logical IDS) and legal mechanism (e.g. forensic evidence) are deployed to detect any irregular behaviors of the system at early stages. Risk management (including risk assessment) in addition to penetration testing and ethical hacking procedures are all proactive mechanisms that can be conducted to expose and detect system vulnerabilities before others.

Security Recovery Process:

For the detection process to have any value there must be a timely response. The response to an incident should be well planned and tested in advance. A Computer Security Incident Response Team (CSIRT) should be established with specific roles and responsibilities identified. CSIRT people should be formed to act upon security events in a proper timeframe. The goal of the recovery process is to restore systems to the original working conditions. The recovery plan should be clearly written and approved by appropriate levels of management, additionally, it has to be tested and reviewed frequently and should encompass all proposed layers.

3.2.3 The People Dimension

As described earlier, people dimension consists of two main indexes:

Visibility Index:

The visibility index demonstrates the scope of exposure of such security controls at people (whether organization employees or outsiders). It is obvious that this index increases when moving down the hierarchy, because visibility of controls at lower levels is more exposed than controls at higher levels as described earlier. A clear example would be visibility of physical assets and monitoring tools (such as cameras) at level-1 compared to visibility of awareness element of people behavior at level-4. Obviously, awareness is less visible which justifies such a proposition.

Sophistication Index:

The ISMM suggests that the depth of knowledge required, Total Cost of Ownership (TCO), and skills and sophistication of management increase when moving up the hierarchy along the model. An example would be comparing the knowledge required to configure back-end system controls (such as configuring firewalls and Intrusion Detection Systems) to efforts required to configure and manage physical and environmental security controls (such as recording cameras at main hallway).

3.2.4 Model Propositions

Sensitive ICT-enabled environments should always seek potential improvements and promotion to higher levels, and review security processes regularly in order to be proactive and avoid potential security incidents. The following propositions are important to understand the analogy and mechanism of the ISMM framework as opposed to others:

- Maturity at a given ISMM layer is reached by implementing quality prevention, detection and recovery security controls on that layer and its preceding layers

- There is an implicit layer at the bottom of the hierarchy, called ad-hoc security (could be also called level 0). Being at this level means complete lack of recognition of security issues. It suggests that the organization has no security controls, plans, policies or any security requirement in place. In other words, the organization has to have structured security practice in place in order to be eligible to have a position on the proposed security framework
- Risk Management, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), and other security practices are all embedded in security processes and intended to be reflected on different levels across the ISMM Model. Therefore, Risk Management process, as an example, is not a single function of level-1 only, it is rather required to be deployed at other levels in the hierarchy. Such a proposition helps to identify exactly the relevance and scope of applicability of each requirement and hence, avoid the false impression of its completeness while it is only implemented on limited scope from the ISMM perspective
- The provided logical order doesn't necessarily mean a certain level requirement must be met fully before a subsequent level requirement arises. A more realistic description is in terms of decreasing percentages of meeting requirements along levels of the ISMM hierarchy. For example, arbitrary and logical figures for an organization may be: 85 percent in meeting physical and environmental requirements (level 1), 70 percent in front-end system security (level 2), 50 percent in back-end system security, 25 percent in comprehensive security awareness, and 10 percent in definite security. In essence, it is logical practice that there is a gradual emergence of meeting higher-level requirements as lower-level requirements become more satisfied. But, again it is not always the case as some environments, due to lack of knowledge, focus more on network security (level-3) while leaving application security wide open (level-2) which has more exposure!
- Being qualified at level-n means the current system has fulfilled, to an acceptable and relevant ratio, all security controls and requirements of level-n and subsequent lower levels too. In other words, logically, lower level security requirements need to be taken care of first, or at least to a considerable extent before promotion
- If a lower level security violation occurs for a given organization, its security measurement (score) decreases to that level immediately. A more realistic example: if a removable storage is stolen in level-3 qualified organization, then that organization will be level-1 qualified instead until the recovery process completes and appropriate countermeasure are implemented successfully. This proposition coincides with the famous saying that security chain is measured by its weakest link
- Definite security can never be fulfilled completely since security is a continuous process. Therefore, the level of security is rather identified and measured by subjective metrics more than objective ones

3.2.5 Model Dependencies

The ISMM was the end result of an extensive study of relevant literature, the industry, and a thorough review of various international frameworks and quality standards such as ISO17799/BS7799, ISO27001, Systems Security Engineering Capability Maturity Model CMM (SSE-CMM), Capability Maturity Model

Integration (CMMI), Control Objectives for Information and Related Technology (CobiT), Six Sigma, and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). However, the main body of the ISMM model is developed based on two main dependencies, context and content dependencies:

Context Dependency:

The context dependency of the ISMM model is based on the intervention with the work of Maslow who put a theoretical framework of individual personality development and motivation based on a hierarchy of human needs. Human motivation doesn't have a complete development life cycle that ends at a certain level but it has a start point. Maslow's work may still have broad applicability in the business world. It consists of five distinctive levels as follows:

- The physiological needs
- The safety and security needs
- The love and belonging needs
- The esteem needs
- Self-actualization

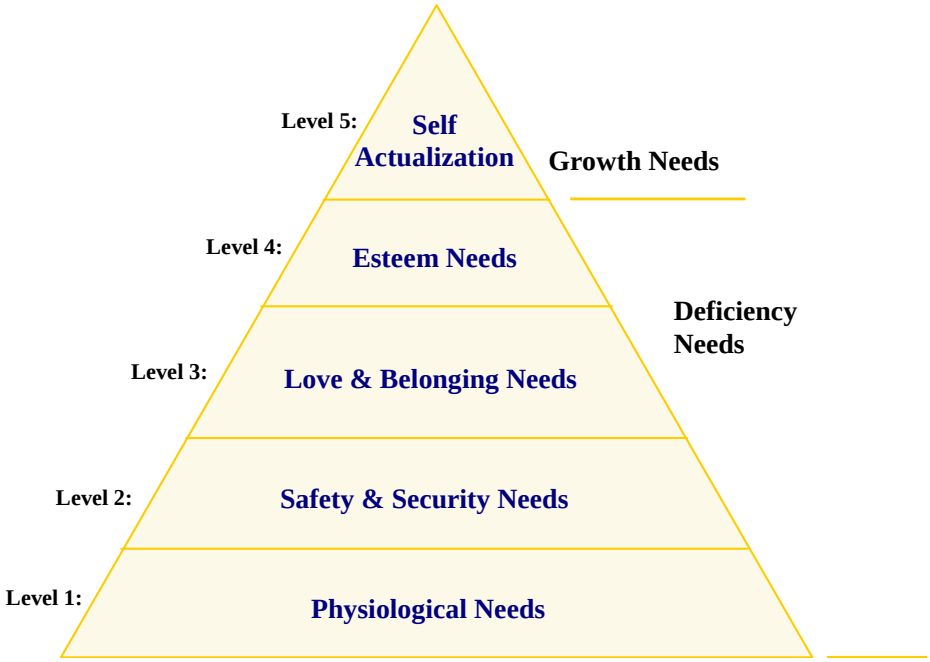

Figure 3-1: Maslow Hierarchy Theory, 1943 [32]

The ISMM model inherits some context features of Maslow theory. Particularly, the following points:

- The ISMM model inherits the layering feature of Maslow, and the incremental growth of the requirements along the hierarchy
- The ISMM model inherits the feature of probability of undervaluing implemented security controls over a period of time:

> *A need once satisfied is no longer a motivator, therefore, a need which is being satisfied over a period of time may be undervalued, people who have never suffered from thirst may tend to undervalue its effects on them, and regard drink as unimportant element for them. [34]*

- In keeping with Maslow theory up to this point, if self-actualizing level is wanted, then lower level needs are to be taken care of first, or at least to a considerable extent [33]. Therefore Maslow's top level involves the continuous desire to fulfill potentials, to

  > *Becoming everything that one is capable of becoming. [32]*

  In comparison to the ISMM, organizations logically should continuously seek fulfilling lower levels requirements first in order to promote to higher levels. It is irrational to invest more on back-end system security (e.g. encryption) if computer room (where critical servers reside) placed in an open area!

- According to Maslow, motivation for people varies since they have different needs based on their level on the hierarchy. In comparison, the ISMM model suggests that motivation for implementing security controls for an organization varies based on its security needs and its current position on the ISMM hierarchy

- These elements in Maslow hierarchy are not to be considered as a rigid framework, there might be a number of exceptions to order indicated, a reversal of the hierarchy might apply to some people:

  > *Although Maslow suggests that most people have these basic needs in about the order indicated, he also makes it clear that the hierarchy is not necessarily a fixed order. [33]*

- The ISMM model suggests that a number of exceptions might exist where some organizations do not meet logical order when deploying overall security controls. Lack of expertise on particular area (e.g. application security) might affect deployed security controls at respective layer (i.e. improper application architecture or change tracking controls)

- According to Maslow, if deprived of the source of satisfaction from a lower order need, it will again become a motivator, which is again seeking for fulfillment of lower level needs. For example, if an esteem-level employee is given notice of job termination, natural reaction would be to start looking for a new job, which is again seeking for fulfillment of needs of lower levels [34]

  In comparison, the ISMM model suggests that if a security breach occurs at lower level for a given organization, then its security level drops immediately to that level where breach took place

- The degrees of satisfaction are described in terms of decreasing percentages of satisfaction when moving along levels of the hierarchy. A false impression may be given that a need must be fulfilled completely before next level's needs arise. As clarified earlier, the ISMM inherits this feature too

- The ISMM model inherits the feature of Level 5 (self actualization needs) as it is not like other levels, where the opportunities presented cannot be exhausted or fulfilled completely [34]
- The ISMM model inherits the feature of Maslow's work of not considering human motivation a complete life cycle with a clear start and end as opposed to other knowledge disciplines (such as software development or project management life cycles). The ISMM considers security a continuous process once started (i.e. open life cycle) in a similar analogy to Maslow's
- The ISMM model inherits Maslow's context of need, which leads to motivation, and hence, feeling and confidence factors

Content Dependency:

It is apparent that contents of the ISMM layers and associated security controls can be easily made compatible with requirements of major domains of any information security standards. However, contents are mainly derived from ISO 17799 standard domains as being the most widely accepted standard. The questionnaire attached (see Appendix) was used in earlier work as part of research methodology during the development of this model [21], it however highlights some attributes of the information security requirements associated with each level.

ISO/IEC 17799 lists ten distinctive controls for information security management systems (currently modified to eleven controls) [31,37,38,61]:

1. Security Policy
2. Information Security Infrastructure
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. System Development and Maintenance
9. Business Continuity Management
10. Compliance

The strength of the ISMM model comes from the structured thinking about information security level which is a very subjective and sophisticated process. The practice of each requirement of ISO17799 is reflected on the model according to its scope of applicability across all levels including the natural synergistic relationship between physical and cyber security (or IT security). ISO17799 as example provides a clear description of security policy and its importance (domain 1), but the ISMM additionally focuses on the applicability and scope of practice of that security policy (spoken, written, and deployed) in the organization according to hierarchy suggested. It stresses that security policy should not give false impression of security, be misunderstood or undervalued by applying it only to limited scope in the organization and then misguidedly considered as complete. The scope of practice of such requirement should be further identified, bounded and reflected on all relevant levels (e.g. level 1, 2, 3…up the hierarchy) [21]. However, some ISO17799 requirements such as physical and environmental security apply the most on level-1 of the ISMM model.

Nevertheless, the ISMM model helps to better understand the application of information security controls outlined in ISO17799. Table 3-1 shows contents matrix that maps the scope of applicability between various security controls mentioned in ISO17799 ten domains and the corresponding scope on the ISMM model [21].

ISO17799 Standard			ISMM Model (Scope of applicability)				
Domain Number	**Domain Name**	**Domain Sub-name**	**Layer 1**	**Layer 2**	**Layer 3**	**Layer 4**	**Layer 5**
1	Security policy	n/a	✓	✓	✓	✓	
2	Organizational security	Information security infrastructure	✓	✓	✓		
		Security of third-part access	✓	✓	✓	✓	
		Outsourcing	✓	✓	✓	✓	
3	Asset classification and control	Accountability for assets	✓	✓	✓		
		Information classification	✓	✓	✓		
4	Personnel security	Security in job definition and resourcing	✓				
		User training				✓	
		Responding to security incidents/malfunctions	✓	✓	✓	✓	
5	Physical and environmental security	Secure areas	✓				
		Equipment security	✓				
		General controls	✓				
6	Communications and operations management	Operational procedures and responsibilities		✓	✓		
		System planning and acceptance		✓	✓		
		Protection against malicious software		✓			
		Housekeeping		✓	✓		
		Network management			✓		
		Media handling and security	✓				
		Exchange of information and software		✓			
7	Access control	Business requirement for access control	✓	✓	✓		
		User access management		✓			
		User responsibilities		✓			
		Network access control			✓		
		Operating system access control			✓		
		Application access control		✓			
		Monitoring system access and use		✓	✓		
		Mobile computing and teleworking		✓	✓		
8	System development and maintenance	Security requirement of systems		✓	✓		
		Security in application systems		✓			
		Cryptographic controls		✓	✓		
		Security of system files		✓	✓		
		Security in development and support processes		✓	✓		
9	Business continuity	n/a				✓	✓
10	Compliance	Compliance with legal requirements				✓	
		Review of security policy and compliance				✓	
		System audit considerations				✓	

Table 3-1: Mapping matrix of ISO17799 domains and the ISMM model [21,1]

3.3 Optimal Security

The literature is vague on finding a precise and abstract definition of optimal security. Two versions of an optimal security definition are suggested as part of this research effort. The first one is considered to be a detailed one and meant to capture the main characteristics of the optimal security level of any computing environment. The second definition on the other side is meant to be concise and abstracted to reflect the main approach for achieving optimal security, which in turn implies meeting all key requirements covered in the first definition.

Optimal security can be defined as continuous fulfillment of security requirements of all the relevant ISMM conceptual boundaries in accordance with the need of the environment under study.

Or

Fulfillment of security requirements of all the relevant ISMM conceptual boundaries continuously and proportionately with the need of the environment under study.

This detailed definition is thought to capture key principles of information security process from the ISMM perspective, these are: 1) continuous fulfillment, 2) deployment of relevant security controls, and 3) reflection of conceptual security layers.

Moreover, optimal security can be defined in an abstract way as continuously and proportionately seeking to fulfill level 5 requirements.

Or

Continuously and proportionately seeking to fulfill level 5 security needs.

This is a short definition that summarizes the key aspect behind those principles of first definition into one main objective, which is seeking development and maintenance of relevant security controls in a continuous fashion.

3.4 ISMM Attack Model

The ISMM model characterizes a new perspective on the concept and attributes of attack techniques and models in information security. The new paradigm classifies various attack approaches in terms of their resultant impact. Attacks, both passive (i.e. intercepting information only) and active (i.e. changing information), are classified in terms of their impact and breaches left in the victim's system. Moreover, attacks are linked with their corresponding ISMM layers, such linkage leads to capture and discover the "weakness in depth" as opposed to the "defense in depth" concept when using the original ISMM model as a defense/protection model. Such classification offers a useful tool to better realize and hence improve the organization's security posture, estimate encountered impact, specify required recovery procedures, and allocate appropriate investment to fix breaches found.

The following diagram (Figure 3-2) depicts the suggested ISMM attack model. It defines five levels of attacks, each of which is mapped to its corresponding layer in the ISMM model. Layer 1 to 4 denotes single attacks where layer 5 denotes hybrid attacks, which means any combination of two or more attacks occurred in different layers (i.e. in lower layers from 1 to 4).

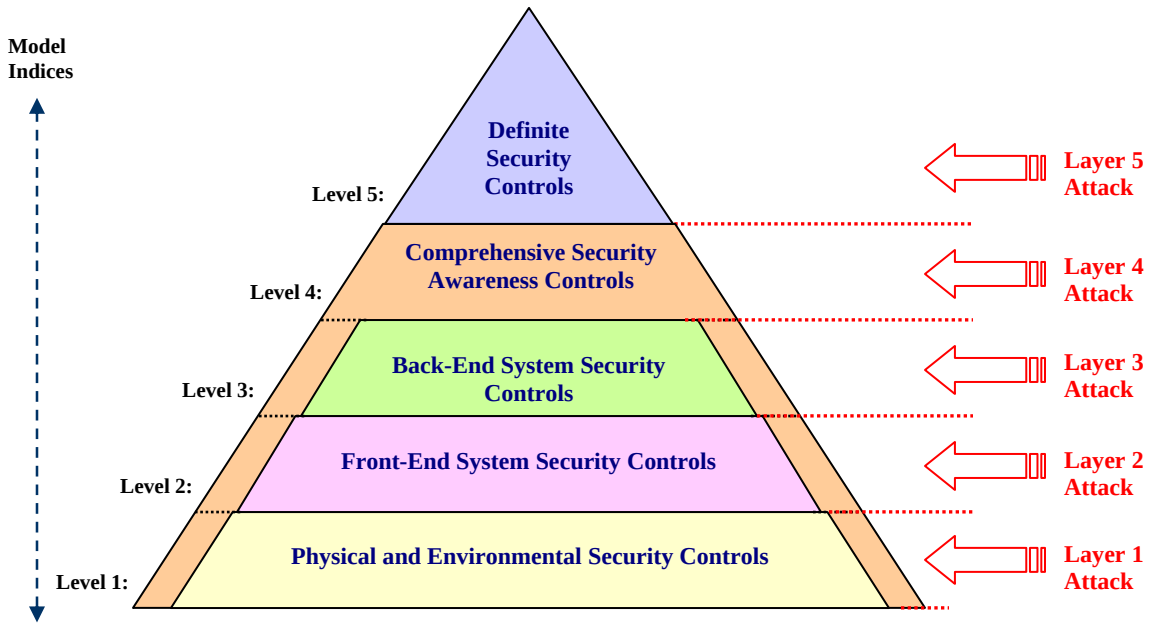

Figure 3-2: ISMM Attack Model

Layer 1 Attack as example means the organization has encountered an attack which targeted controls in layer 1 (physical and environmental security controls) such as breaking the secret key for CCTV system. Man-in-the middle and chosen-ciphertext attacks against public-key encryption in IPSec implementation are considered Layer 2 attacks, while same type of attacks on SSL implementation are considered Layer 3 attacks, and the same analogy applies to other layers in the ISMM. Therefore, attacks are classified based on their origin and impact from the ISMM attack model's perspective. This attack model offers a useful tool in order to:

- Analyze and study various attacks (attack in depth)
- Analyze and track down the main origin of security breaches (weakness in depth)
- Locate incidents and their impacts accurately and hence speed up recovery procedures
- Guide to the right and necessary system fixes
- Plan and optimize efforts and investments in the maintenance and development of security controls
- Associate attacks to their relevant breaches for every organizational context, as similar attacks might cause different impact to different organizations
- Assist to better estimate cost of security, its return, and its failures

3.5 Mapping ISMM to Network Models

As mentioned earlier, networking functions are organized and described in a layered architecture (both ISO/OSI and TCP/IP reference models). Many services and protocols are implemented as part of the distinct functions embedded into layers of these models. However, many security breaches are created too

as both needs and respective technologies continuously evolve and change. Security experts and houses however are always trying to catch up and develop various products and services in trying to control these exploits and reduce caused risks. Nevertheless, this section suggests a mapping between the ISMM and Network models.

The key questions to ask in order to understand potential benefits behind the mapping between the ISMM and network reference models and the adaptation of the ISMM model in this dilemma are:

- Is the organization/environment under study implementing appropriate measures and controls on all networking layers of the model in use (whether ISO/OSI or TCP/IP)?
- Will the implementation of appropriate security measures and controls on all these layers of the network model guarantee a secure communication environment?
- What is the optimized distribution or formula for resources usage ratios, including computational power, energy, and memory beside other investments, among these controls across all networking layers? And, what are their actual weights on the ISMM? In other words, where does the balance lie?

Figure 3-3 depicts the proposed mapping between the ISMM and network models. The mapping shows how the order and priority of implementation of functions and services among networking models are not necessary the exact match to security models and the ISMM in specific.

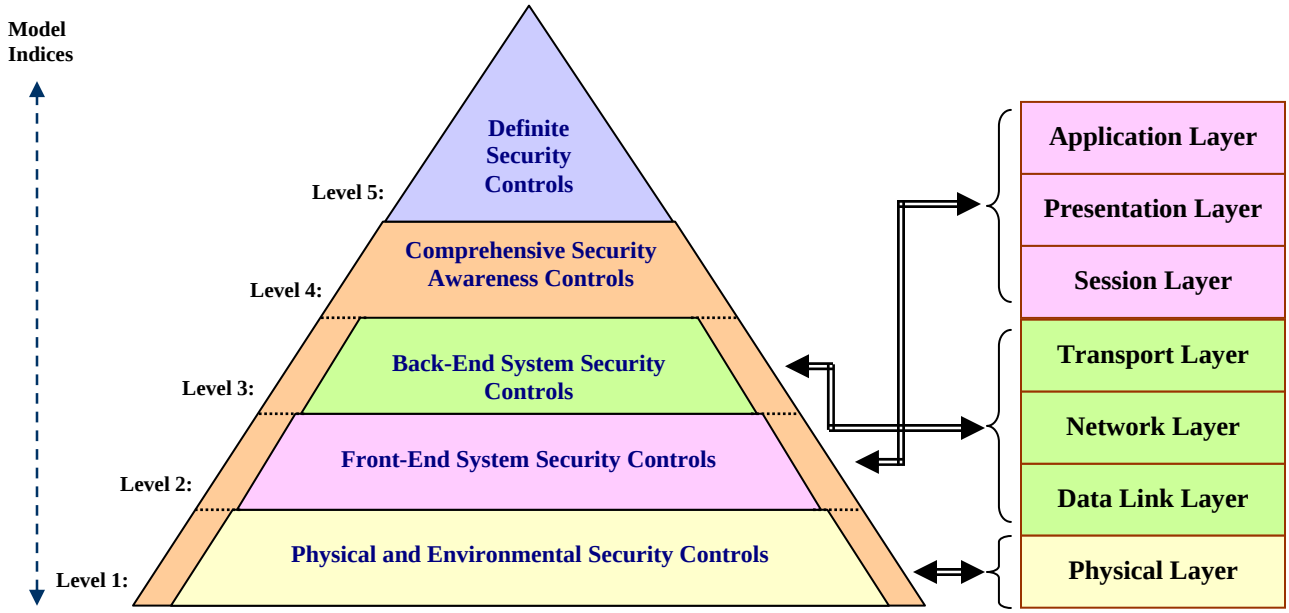

Figure 3-3: Mapping ISMM to Network Models

There are many security implementations in various layers of networking models. Some protocols are implemented with built-in security functions while in many others security functions were added later on in the design. General examples of security functions may include SSH and HTTPS in the application layer, SSL and TLS in Presentation and Session layers, IPSec in network layer, Error and Flow Control in Data Link Layer.

Each one of these implementations has its own design details and various configuration parameters. TLS and SSL as an example are cryptographic protocols which provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers. TLS uses some cryptographic primitives to offer endpoints with authentication and communications privacy, and is designed to prevent eavesdropping, tampering, and message forgery [2].

One method of TLS implementation is to only allow the server side to be authenticated (identity is ensured) while the client remains unauthenticated. The other way is called mutual authentication where both sides, client and server, are authenticated and this implementation requires PKI deployments to both sides, this approach requires the following key phases in general:

- Peer negotiation for algorithms and associated crypto parameters
- Public key encryption for authentication and key exchange
- Symmetric cipher for traffic encryption

The following schemas and algorithms may be used [2]:

- Public-key cryptography: RSA, Diffie-Hellman, DSA, ECC
- Symmetric ciphers: RC4, IDEA, Triple DES, AES
- One-way hash functions: MD5 or SHA

Regardless of which combination is used, it is worth noting that any implementation of these options requires certain processing power, memory, and energy resources of the computing platform or environment, this is of course besides the required policies, procedures, and various other costs (i.e. development and maintenance) associated with human factors. Theoretically, summing up the totals of these resources and other costs yields total investment cost for that particular security control (i.e. TLS/SSL implementation). Obviously, all these resources and costs have lower and upper bounds, they are finite quantities! Moreover, these figures convey useful and yet sensitive information when mapped to the ISMM and network models as they tell the actual amount of investment and return per layer on both models (i.e. the ISMM and Network models).

Obviously, TLS example mentioned above tells more information about security level when reflected on the ISMM model. With this mapping, for any environment, it can easily derive the information about all security controls and measures in place at every layer in both models, the ISMM and Network. Implementing TLS/SSL is only one measure that fills up a requirement gap in level 2 in the ISMM model (Front-end system security) even though it is implemented in higher layers in ISO/OSI and TCP/IP network models.

The example does not state that this control (i.e. TLS/SSL) is enough for that particular environment or even that layer. Moreover, having security controls in other layers in network model does not mean reaching sufficiency level of security! This is the reason that makes the ISMM model offers richer information about integrity and security level, network models fill up only some gaps in different levels in the ISMM and still leave others untouched. Nevertheless, network models do not tell logical order of priority of implementation, as it was not originally meant to be, in terms of security posture.

Following practical example shall clarify these arguments, assume an organization that implements a reliable IPSec encryption using PKI infrastructure (layer 3 in network models: network layer) which is

considered level 3 control in the ISMM. Assume 256-bits cryptographic strength is used with the following setting as recommended by NSA Suite B [63] and in NIST SP-800 Crypto Specifications [64]:

Crypto function	Algorithm
Encryption	AES-256 bits
Hashing	SHA-512 bits
Key Exchange	ECDH-512 bits
Digital Signature	ECDSA-512 bits (equivalent to RSA-15360 bits)

Table 3-2: Example of 256-bits cryptographic strength

Now, if the application authentication mechanism is not strong enough, then the security level cannot exceed ISMM level 2 regardless of the reliability of IPSec implementation and complexity of its encryption used, as Front-End system security comes before Back-End, also if some of the physical assets such as network cards or hard disks are not physically protected enough, then it can not even pass ISMM level 1 (Physical and Environmental Security Level) which is worse than what it might seems to be. In this case it is possible that appropriate security measures (cryptographic controls on all networking levels) are taken and the organization still does not qualify for more than level 1 security in the ISMM model, again when the physical aspects are missing! This concern is significant and currently getting more attention by security professionals than ever as physical security is extraordinary rising due to the rapid advances in wireless computing.

The previous example shows how the adaptation of the ISMM model can tell richer information about what security controls are in place in network models, where do they match on the ISMM model? What gaps are missing? What resources are being used and at what ratios? And hence helps to covey a more realistic picture about actual security and avoid the illusion of security!

3.6 Implementation Snapshot

To further clarify the resulted benefits of adopting the ISMM and its mapping to existing network models for any computing/communication system, two scenarios are presented. Similar security controls at various layers in both the ISMM and Network models are assumed in both examples. The first scenario depicts a typical computing environment with different computing and communication systems. The second scenario shows same environment mapped to the ISMM model where security controls are compiled and reflected.

Scenario 1: Typical environment

The following diagram (Figure 3-4) depicts a typical computing environment with multiple computing and communication systems and devices, say personal computers, servers, handheld devices, routers, firewalls, electronic locks, and the TCP/IP network model is used.

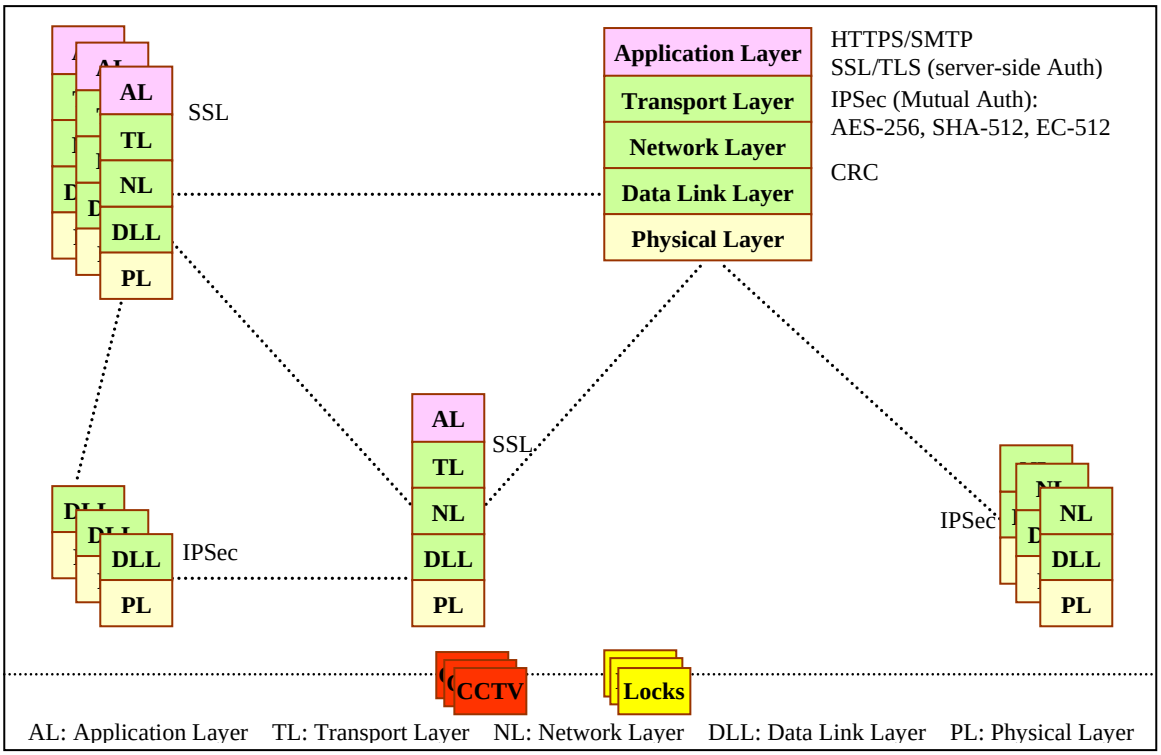

Figure 3-4: Typical computing environment

Scenario 2: The ISMM adopted

In this scenario, the same computing systems and devices are used but all relevant information about existing security controls are compiled and reflected in the ISMM model. It is worth noting that the ISMM model is meant to be mainly mapped to the organization under study or computing environment as a whole. However, it can be further mapped to smaller blocks like different sites, department, operation rooms, and even down to a single computing/communication platform/system. Such scalability offers more information about actual security implementation at both the macro and micro level of the organization. Figure 3-5 shows a simple way of reflecting all security controls in place in the ISMM model. Security controls are simply aggregated in their respective layer.

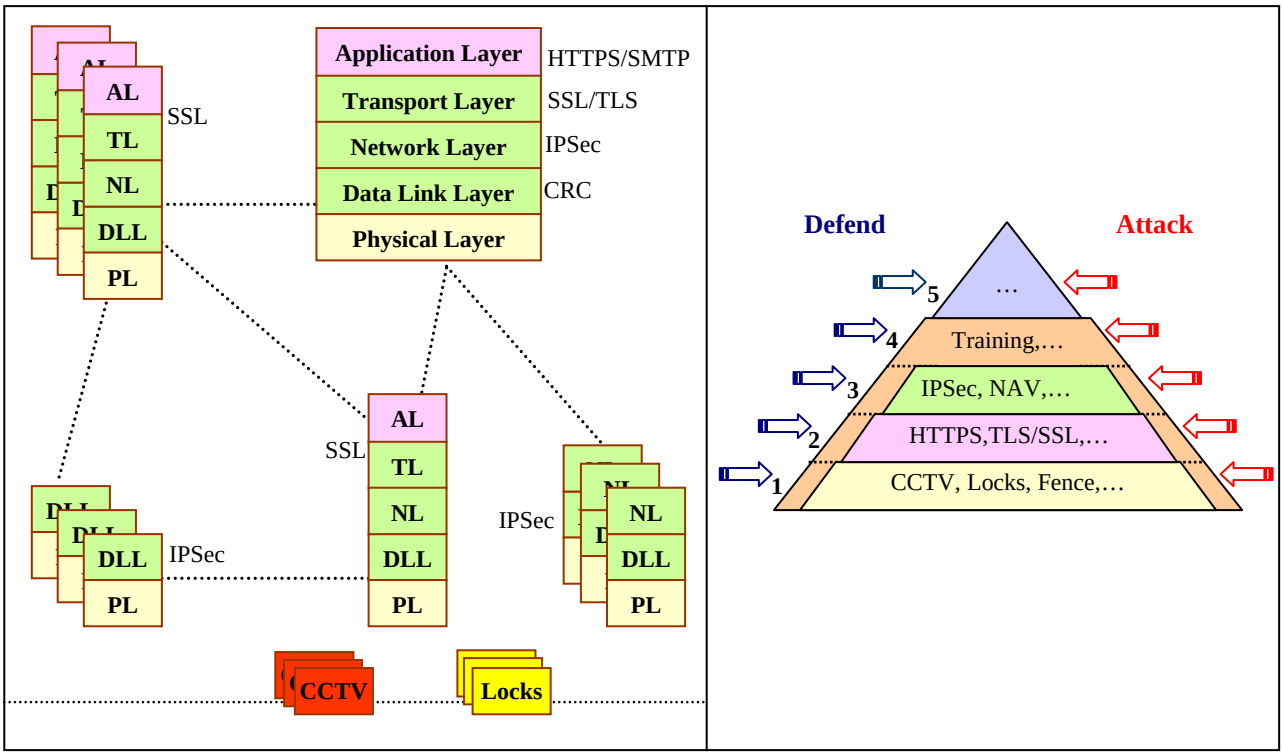

Figure 3-5: Typical computing environment mapped to the ISMM Model

Maturity at a given ISMM layer is reached by implementing quality prevention, detection, and recovery security controls on that layer and its preceding layers. Therefore, quality can be achieved at control level while maturity is achieved at various layers of the model. Table 3-3 provides different representations (say dashboards) of the information that details every control, its ISMM model properties, and resource usage. Similar types of these representations are used in other models explained earlier such as Security Program Maturity Model [53].

Controls-specific			ISMM-specific				Resources-specific				
Control	Parameters	Risks	Layer (1-5)	Process (P,D,R)	Quality (0-3)	ISO Domain (1-10)	Memory (0-100%)	Processing Power (0-100%)	Energy (0-100%)	Effort (0-100%)	Cost (0-100%)

Table 3-3: Simulated example showing controls-specific, ISMM-specific, and resource-specific parameters

Table 3-4 and Table 3-5 depict the analysis of the organizational information security and maps it to security processes and quality respectively. Table 3-6 shows security posture in a more modular representation, say by site or department level. Maturity and quality are reflected separately as they

should always be. Note that these different tables and other diagrams may be taken at different times in order to measure progress against certain time. Resources (such as memory, processing power, and power energy) are always limited and hence are integrated into the whole evaluation process. The ISMM model is simply repeatable, its measures are suggested and judged against their logical order, moreover, integrated and mapped to network models.

Processes	**Layers**					
	1	**2**	**3**	**4**	**5**	**Total**
Prevention						
Detection						
Recovery						
Total						

Table 3-4: Dashboard of the ISMM layers and corresponding processes

Quality	**Layers**					
	1	**2**	**3**	**4**	**5**	**Total**
None						
Low						
Med						
High						
Total						

Table 3-5: Dashboard of the ISMM layers and corresponding quality measures

Site/Branch/Department	**Layers**						**Maturity**	**Average Quality**
	1	**2**	**3**	**4**	**5**	**Total**		
A								
B								
…								
Total								

Table 3-6: Management dashboard of an aggregation of the ISMM layers, maturity levels, and quality

3.7 ISMM Differentiating Features

According to [65], enterprises that expressed confidence in their security practices were in fact more secure, this was referred to as "confidence correlation". Such confidence results in a virtuous cycle that spreads into the enterprise and leads to continuous support and improvements. The ISMM model acknowledges such correlation resulted from synergies of its three dimensions (people, process, and layering) where confidence is manifested in people, as security needs starting at lower levels lead to motivation, practices, then confidence and trust as a resultant and accumulated feeling of being more secure as we go up the hierarchy.

The results of the Global Information Security Survey in 2004 suggest that most of the organizations are not well structured in terms of their security investment or practices:

> *Quite a few organizations aren't 'doing security right'. It is a combination of a failure to invest and a failure to enforce…many organizations should not feel comfortable and secure, since they neither know themselves nor their enemies very well. [66]*

This survey observation is based on the linkage with the work of Sun Tzu, The Art of War, which was written during the 6th century BC. Sun Tzu work is relevant and still has an influence on an organization effort to effectively protect itself against security threats [66].

> *Know the enemy and know yourself, in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril. [67]*

The ISMM is neither derived from the perspective of security as a closed lifecycle, nor from only the attacker's or defender's (security professional) point of view, it is actually rather derived from the battlefield between both parties (i.e. attacker and defender at same time). Hence, it reflects conceptual and yet logical security boundaries, signifies rational security priorities, and captures commonsensical synergies between logical and physical security. Therefore, it offers unambiguous realization of the organization's security level, and a better vehicle to study enemy's capabilities at separate layers and in whole system as one integrated entity against both single and hybrid attacks.

The ISMM model is deemed compatible and consistent with other security-related models and systems architecture. To mention some examples, it can be mapped to operating system security models, trust models, and mobile and wireless computing architectures, as the issues of physical security and resource scarceness that constitute major concerns for these models are already captured by the ISMM model.

Regardless of the size or type of the environment or computing system under study, the ISMM provides a logical abstract of two sides of information security, these are:

First: It abstracts the conceptual boundaries of information security into five specific, ordered, and related layers. These layers capture both technical and social aspects of any security implementation and also reflect the unavoidable interdependencies between physical and cyber security. Furthermore, Security controls are always classified in terms of their main functions as prevention, detection, or recovery controls.

Second: It also abstracts the totals of resources used for security controls (i.e. memory, processing power, energy, effort, and cost), such resources are further bonded to their respective ISMM-specific properties (security level, process, quality, and ISO17799) and control-specific properties (parameters and risks). These figures offer a richer picture of total investment on information security and progress against time, leading to a more justified estimate and guidance towards Return On Information (ROI).

Such abstraction opens several new extensions of the model. It can be used as a solid ground for deriving following several major aspects in information security:

First: A new definition of the notion optimally secure environment or system is suggested, which is tied to these conceptual layers and resource ratios.

Second: An introduction towards developing an optimization formula for finding the best utilization ratio of various resources (i.e. memory, CPU, energy) in order to reach the desired (or maximum achievable) security level from the perspective of the ISMM abstracted layers. The formula shall capture both the original (i.e. existing) and optimized distribution of these resources and therefore shall have both lower and upper bounds of such usage.

Third, a new attack model is proposed that is consistent with the original ISMM defense model and categorizes different attacks in such away that facilitates a new structured approach towards the analysis of their impacts.

Additionally, the mapping of the ISMM model to network models (TCP/IP or ISO/OSI) suggests that security parameters and functions implemented into these networking layers can be further studied and analyzed in terms of their contribution to the security posture (on various layers of the ISMM) and consumptions of available resources.

3.8 Summary

As mentioned in [65], there are six secrets of highly secure organizations as a result of a review of the 2004 Global Information Security Survey (more than 8,000 respondents from 62 countries), organizations were advised to:

1. Spend more
2. Separate information security from IT
3. Conduct a penetration test
4. Create a comprehensive risk assessment process
5. Define overall security architecture
6. Establish a quarterly review process

Obviously, these advices are facilitated and made a lot clearer from the ISMM model perspective. The ISMM model abstracts security controls, resources and security boundaries from other elements including IT. The model captures the logical integration between physical and cyber security into one approach leading to richer view of the overall security architecture in place and, hence, facilitates more efficient risk assessment, auditing and penetration tests over information security. The model can also provide a

variety of security posture snapshots at different times, leading to a more structured realization of progress and spending against time for the quarterly review process.

The suggested new definition of optimal security is derived from the abstraction of the ISMM at both conceptual security boundaries and resources. This bound provides a delimiter of various security levels. It puts optimal security into a new context that is measurable, auditable, repeatable, and yet simple. Furthermore, the suggested new ISMM Attack Model offers another tool for classifying attacks in terms of their breaches and impact caused. Such approach leads to a consistent view of weaknesses from sides: defense-in-depth and attack-in-depth.

The ISMM model can be applied to different types of organizations while producing consistent results. Having or losing security will always be a comprised figure on something else, it must have a cost, the real art then is to optimize that cost for maximum return. In other words, it is an optimization problem that aims to find the right tradeoff between security needs, controls, and investment. Such approach shall lead to better realize the security into perspective and avoid the illusion of security.

Chapter 4
Conclusions and Recommendations

4.1 Introduction

Organizations are globalizing and expanding their business operations, hence, facing the ever-growing risk interdependencies:

> *Today's huge opportunity can quickly become tomorrow's nightmare - particularly if the nightmare involves loss or corruption of company information, theft of trade secrets, exposure of customer information, or infiltration of systems. [68]*

Almost 80% of participants in Global Information Security Survey in 2006 agreed that efforts and activities to achieve regulatory compliance have improved their companies' information security and think of it as a vehicle to address security issues including controls and processes proactively.

The results of Global Information Security Survey, utilizing ISO17799-besd questionnaire and participants from nearly 1,200 organizations in 48 countries from around the world, have identified five global priorities for information security that will have a significant impact on organizations' capacity to manage their risks and, eventually, on their success [68]. These five priorities are:

- Integrating information security with the organization culture and overall risk management
- Extending the impact of compliance as it promotes teaming with other business functions and hence improves information security
- Managing the risks of third party relationships due to the impact of globalized business environments and resulted risk interdependencies
- Formalizing privacy and personal data protection practices
- Building and standardizing information security architecture and alignment with business goals

The importance of these trends is increasing due to current globalized environments and extended business operations. The ISMM coincides with this orientation and can be used as a vehicle toward achieving such trends. Especially the integration of information security functions with other functions, compliance requirements, and managing organizational risk interdependencies. This is achieved because the ISMM measures security itself (actual delivery) regardless of the size or type of the organization under study, and hence, its certification mechanism goes beyond measuring the way security is governed (its process), and yet the ISMM is simple so that it can be understood and communicated easily at various organizational levels.

4.2 Research Conclusions

While successful delivery of information security systems offers many advantages, including enhanced efficiency and effectiveness of operations, failure to successfully deliver information security is costly in monetary terms and also in personnel and organisational terms. In spite of all the investment in ICT and the increasingly important strategic role of ICT in the organisation, how to deliver information security successfully remains a challenge.

Obviously, current information security industry has witnessed several auditing and monitoring models and tools. However, due to the evolving dynamics and complexity of current attacks and associated risks, there is a vital need for an adaptive maturity model that captures the convergence of both physical and cyber security into one multi-layer framework, that is neither tied up to a specific technology/protocol (e.g. PKI, IPSec, SSL) nor a certain system/product (e.g. Firewall, Antivirus, IDS). The ISMM, as a complement contribution to existing models and technologies, offers a methodology that guides toward an evolution path from an ad-hoc information security delivery approach into a more structured, flexible, scalable, repeatable, and yet simple one.

This research used a heuristics-based investigation of security-related models in general and the ISMM model in specific including all its properties: the three dimensions, propositions and dependencies. Consequently, introduces new extensions that are believed to facilitate various applications such as a method to abstract the amount of information security cost in a given communication device or computing environment, provides a measure of relative resources utilization against respective security controls and the ISMM layers, and abstracts optimal security notion and attacks in terms of their associated impact. Furthermore, a possible mapping of the ISMM to network models (ISO/OSI and TCP/IP) is demonstrated as an example of its consistency with other security-related models.

These enhancements are believed to fill a gap in existing literature and industry practices regarding information security implementation. It can be concluded that this model presents a framework to assess and evaluate the quality of the deployed information security system, measures amount of information security cost, guides to the right layers and resource amounts of implementing security. Hence, assists to structure thoughts and realize actual information security posture progressively.

4.3 Contribution to Knowledge

In an attempt to provide tools for both practitioners and researchers by which they might devise schemes to increase the likelihood of information security implementation success, the researcher undertook a holistic approach in enhancing and extending the multi-layer, process-based Information Security Maturity Model, ISMM, in order to facilitate a vehicle that merit further applications and research endeavours.

The researcher anticipates that the deployment of the ISMM model will enhance understanding the information security awareness and practice and thereby create an environment of a higher rate of success in ICT implementation.

This research meets an identified research need into the information security engineering discipline, mainly the maturity models of information security. Contributions to the existing body of knowledge include enhancements and extensions of the Information Security Maturity Model (ISMM) as described

in the literature and a bridge between the literary and theory to the identification and use of the model in real-world situations. Significant contributions include the following points:

- Literature review and discussion of existing security models in light of internationally recognized standards (i.e. ISO17799). This review is supported by introducing a new categorization of these models as follows:
    - Best practices oriented (such as BS7799, ISO17799, ISO27001)
    - Process oriented (such as SSE-CMM, ISM3, COBIT, NIST)
    - Risk oriented (such as CRAMM, OCTAVE)
    - Controls oriented (such as SPMM)
    - Security oriented (such as ISMM)
- Abstracts information security cost and its conceptual boundaries into five specific, ordered, and still related layers, and captures both technical and social aspects of any security implementation. Additionally, acknowledges the unavoidable interdependencies between physical and cyber security
- Abstracts totals of resources utilization for security controls (i.e. memory, processing power, energy, effort, and cost), and links them to model properties (i.e. security level, process, quality, and ISO17799) and control properties (i.e. parameters and risks). These figures offer additional information about security posture, and lead to a justified guidance towards information security direction and realization of Return On Information (ROI)
- Suggests a definition of what an optimal security notion might mean, besides a new consistent attack model that is independent from any attack and size or type of the victim's computing device or environment
- Depicts an example of one possible mapping of the ISMM to other security-related models (through the use of network models)
- Offers a useful and comprehensive tool to measure security level of any computing environment in a consistent way, facilitates various applications such as comparing security levels of different organizations for various business endeavors (such as certification, partnership, e-commerce, and networking)
- Presents a convenient approach to measure investment on information security

4.4 Further Research Questions

Many questions were raised during this study that merit further investigation. The research has highlighted the lack of comprehensive maturity models that benefit both researchers and practitioners toward proper and structured understanding and implementation of such an important issue, the information security, as it is being recognised and paid attention more than ever. It is recommended that future work on this model could tackle the following issues:

- How to apply this model in real life examples? Will it be possible to be implemented on some case studies?

- What is the optimized distribution or formula of the usage of various resources, including computational power, energy, and memory, beside other investments, for a given computing device or environment? Can this formula be further analyzed as an optimization problem from the ISMM abstraction of both conceptual boundaries and amount of information security cost? In the other words, where does the balance lie?
- Can this formula be generalized to be applied on networking models (ISO/OSI and TCP/IP)?
- Can these abstractions of security boundaries, costs, and attacks lead to formulate a measure of the "amount of information security" in place?
- Can the ISMM research components be further extended to evaluate not only who deploys security controls, but who develops them and who drives them? As the behavioural characteristics of the organisations and the groups within them are necessary to the results and right use of these security models

4.5 Summary

Security is a costly element but the cost of losing it is much more. Besides saving informational assets, structured security implementation adds a unique and competitive advantage to the computing environment. As a result, the enhancement of such a holistic and integrative framework was a necessary step for both researchers and practitioners.

The ISMM model along with its extensions described in this research meets that need. It provides a workable and reliable way to gather, map, and analyse data regarding the whole of the information security implementation/delivery landscape. The ISMM model can be applied at both the macro and micro level of any computing element, it can be applied on the computing environment under study as a whole and also can be brought down to the detailed level of security controls and associated parameters in every layer of the ISMM and networking models.

The extended definitions of the ISMM components along with the abstraction provided of security conceptual boundaries and amount of information security cost, suggested optimal security definition, attack model, and mapping to network models are meant to be consistent in nature, integrated, and logical contributions to the mosaic of information security.

Further research into any of the areas mentioned above will also be facilitated by these extensions. It is hoped that the next few years will produce other research endeavours showing the efficacy of this new framework.

Appendix A

ISO17799 Standard

ISO and IEC form the specialized system for worldwide standardization. International Standard ISO/IEC 17799 was originally prepared by the British Standards Institution under the name BS7799, and then adopted by ISO/IEC as ISO17799. ISO/IEC 17799 outlines ten (recently eleven domains) distinctive information security controls [31, 61]:

1. Information security policy:

The objective of this control is to have a documented information security policy, which is approved by the management and communicated to all intended employees. The policy should be reviewed regularly, and should always reflect all changes to ensure its consistency.

2. Organizational security:

This domain consists of three parts which are:

a. *Information security infrastructure:*

The objective of this control is to manage information security within the organization. There should be a management information security forum to ensure the availability and visibility of clear management commitment and support for security initiatives.

b. *Security of third-party access:*

The objective of this control is to maintain the security of organizational information processing facilities and information assets accessed by third parties. The associated risks shall be assessed and appropriate security controls implemented.

c. *Outsourcing:*

The objective of this control is to maintain the security of information when the responsibility for information processing has been outsourced to another organization.

3. Asset classification and control:

This domain consists of two parts which are:

a. *Accountability for assets:*

The objective of this control is to maintain appropriate protection of organizational assets. An inventory of all important assets associated with each information system shall be drawn up and maintained.

b. *Information classification:*

The objective of this control is to ensure that information assets receive an appropriate level of protection. Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs.

4. Personnel security:

This domain consists of three parts which are:

a. *Security in job definition and resourcing:*

The objective of this control is to reduce the risks of human error, theft, fraud or misuse of facilities. Security roles and responsibilities, as laid down in the organization's information security policy, shall be documented in job definitions.

b. *User training:*

The objective of this control is to ensure that users (could be employees or third-party) are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

c. *Responding to security incidents and malfunctions:*

The objective of this control is to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents. Security incidents shall be reported through appropriate management channels as quickly as possible.

5. Physical and environmental security:

This domain consists of three parts which are:

a. Secure areas:

The objective of this control is to prevent unauthorized physical access, damage and interference to business premises and information.

b. *Equipment security:*

The objective of this control is to prevent loss, damage or compromise of assets and interruption to business activities. Equipment shall be sited or protected to reduce the risks from environmental threats and hazards.

c. *General controls:*

The objective of this control is to prevent compromise or theft of information and information processing facilities. Organizations shall have a clear desk and a clear screen policy aimed at reducing the risks of unauthorized access, loss of, and damage to information.

6. Communications and operations management:

This domain consists of seven parts which are:

a. *Operational procedures and responsibilities:*

The objective is to ensure the correct and secure operation of information processing facilities.

b. *System planning and acceptance:*

The objective is to minimize the risk of systems failure. Capacity demands shall be monitored and projections of future capacity requirements made to enable adequate processing power and storage to be made available.

c. *Protection against malicious software:*

The objective of this control is to protect the integrity of software and information from damage by malicious software (detection and prevention controls).

d. *Housekeeping:*

The objective of this control is to maintain the integrity and availability of information processing and communication services (back-up copies).

e. *Network management:*

The control objective is to ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

f. *Media handling and security:*

The objective is to prevent damage to assets and interruptions to business activities. The management and disposal of media (i.e. tapes, disks) when no longer required.

g. *Exchanges of information and software:*

The control objective is to prevent loss, modification or misuse of information exchanged between organizations.

7. Access Control:

This domain consists of eight parts which are:

a. *Business requirement for access control:*

The objective is to control access to information. Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.

b. *User access management:*

The objective is to ensure that access rights to information systems are appropriately authorized, allocated and maintained.

c. User responsibilities:

The objective of this control is to prevent unauthorized user access.

d. *Network access control:*

The objective of this control is protection of networked services. Users shall only have direct access to the services that they have been specifically authorized to use.

e. *Operating system access control:*

The objective of this control is to prevent unauthorized computer access.

f. *Application access control:*

The objective of this control is to prevent unauthorized access to information held in information systems.

g. *Monitoring system access and use:*

The objective of this control is to detect unauthorized activities (i.e. audit logs).

h. *Mobile computing and teleworking:*

The objective of this control is to ensure information security when using mobile computing and teleworking facilities.

8. System development and maintenance:

This domain consists of five parts which are:

a. *Security requirements of systems :*

The objective of this control is to ensure that security is built into information systems.

b. *Security in application systems:*

The objective of this control is to prevent loss, modification or misuse of user data in application systems.

c. *Cryptographic controls:*

The objective of this control is to protect the confidentiality, authenticity and integrity of information. Encryption shall be applied to protect the confidentiality of sensitive or critical information. Digital signatures shall be applied to protect the authenticity and integrity of electronic information. Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event or action. A key management system based on an agreed set of standards, procedures and methods shall be used.

d. *Security of system files:*

The objective of this control is to ensure that IT projects and support activities are conducted in a secure manner.

e. *Security in development and support processes:*

The objective is to maintain the security of application system software and information. The implementation of changes shall be strictly controlled by the use of formal change control procedures.

9. Business continuity management:

The objective of this control is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

10. Compliance:

This domain consists of three parts which are:

a. *Compliance with legal requirements:*

The objective of this control is to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

b. *Reviews of security policy and technical compliance:*

The objective of this control is to ensure compliance of systems with organizational security policies and standards.

c. *System audit considerations:*

Aims to maximize the effectiveness of and to minimize interference to/from the system audit process.

Appendix B

ISMM Questionnaire

Part I: General Information

- *Check appropriate number*
- *When using Microsoft Word, Double click the Checkbox field and select Checked in order to be set*

1. Your name and location (optional):

2. What best describes the size of your company in term of number of employees:

☐ Less than 50 employees ☐ between 50 and 100 employees

☐ Between 100 and 500 employees ☐ between 500 and 1000 employees

☐ Between 1000 and 5000 employees ☐ more than 5000 employees

3. Date of organization establishment:

☐ Before 1980 ☐ between 1980 and 1990 ☐ After 1990

4. Nature of business (check each one that applies):

☐ Industrial ☐ Services ☐ Diversified ☐ Trading

☐ Banking ☐ Contracting ☐ Government ☐ Others (specify):

5. Organization overall annual budget (in Saudi Riyals):

☐ Less than 5 million ☐ between 5 and 10 million

☐ Between 10 and 20 million ☐ between 20 and 50 million

☐ Between 50 and 100 million ☐ Above 100 million

6. IT department budget in relation to overall annual budget:

☐ Less than 5% ☐ Between 5% and 10%

☐ Between 10% and 20% ☐ More than 20%

7. Information security budget in relation to overall IT department budget:

☐ Less than 5% ☐ Between 5% and 10%

☐ Between 10% and 20% ☐ More than 20%

8. Organization profit in relation to overall organization budget:

☐ Less than 5% ☐ Between 5% and 10%

☐ Between 10% and 20% ☐ Between 20% and 30%

☐ Between 30% and 40% ☐ More than 40% ☐ N/A or Non-profit

9. Number of computers (either PCs or Workstations) in your organization:

☐ Less than 100 ☐ between 100 and 500

☐ Between 500 and 1000 ☐ more than 1000

Part II: Physical and Environmental Security

- *Check appropriate number*
- *Use following key:*

5= Rigorous and complete

4= Complete

3= In part

2= Patchy

1= Poor

0= None, not known, or not applicable

Definition: The control at this level aims at preventing unauthorized physical access or interference to IT environment or computer equipments and information assets. Physical security of IT department and having restricted access control to operation room are clear examples at this level.

10. Are there a current, documented security policies and procedures which define all security physical access requirements to the facility including vendors and support personnel?

5☐ 4☐ 3☐ 2☐ 1☐ 0☐

11. Are all IT equipments and information processing facilities in areas protected from unauthorized physical access?

5☐ 4☐ 3☐ 2☐ 1☐ 0☐

12. Is there a legally approved scheme to detect any access violation to secure areas (e.g. using 24/7 recording cameras and other monitoring systems)?

5☐ 4☐ 3☐ 2☐ 1☐ 0☐

13. How do you rate the overall classification and control of business assets?

5☐ 4☐ 3☐ 2☐ 1☐ 0☐

14. Is there a current, documented, and tested recovery plan in case of physical security counter measures fail?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

15. Is there a current, documented, and tested emergency plan (evacuation) in case of environmental disaster occurs (e.g. fire)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

16. Is preventive maintenance of all hardware equipments (mainframes, if applicable, PC's, Routers, LAN's, etc.) performed according to published schedules?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

17. Among following list, check tool(s) or mechanism(s) used for prevention and detection of any incident/violation to physical assets:

☐Recording cameras

☐Biometrics

☐Locks

☐Guards

☐Smart Cards

☐Others (please specify):

Part III: Front-end System Security

- *Check appropriate number*
- *Use same previous key*

Definition: Front-end system security is about all application level system functions and integrity requirements between the application itself and end-user interface, it suggests that application data should be protected against any potential threat that might cause loss, damage, or unauthorized access by either internal or external users. Application change management process and application authorization controls are just examples of what could fall in this section.

18. Is a structured change management process for all application related development cycle issues in place?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

19. Is there a clear, updated user's manual that details proper usage of application?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

20. Are appropriate policies and procedures relating to software licensing, development, selection, specification, acquisition, testing, introduction, migration & disposal in place?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

21. Is application designed in such away that grants access permissions to only authorised users on the need basis for particular application functions?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

22. Are appropriate measures and controls that prevent users installing and using unauthorized software in place?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

23. If you have an externally accessible Web Server, are access controls implemented for the files and directories that are stored on the Web server?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

24. Are backup and recovery policies and procedures documented, tested, and updated regularly for all application level data?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

25. Do authorized individuals use their privileged accounts only for the tasks for which they are needed and use their unprivileged accounts for all other normal business activities?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

26. Are appropriate procedures in place to ensure that the passwords and privileges of terminated employees and contractors are immediately revoked?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

27. How well application level security issues are monitored and investigated regularly by security officer(s)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

28. Is removable media containing sensitive information properly labelled and protected against unauthorized access at all times?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

29. Are software audit tools in place to detect any unauthorized access, change, or removal of data, which will assist in post analysis and system corrections?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

Part IV: Back-end System Security

- *Check appropriate number*
- *Use same previous key*

Definition: Back-end system security includes any resource (e.g. hardware, software, etc.) that are beyond application level components. Underlying network infrastructure and internal and external communication constitute the major components at this level. Examples are configuration of back-end platforms, intrusions detection systems, firewalls, and deployed cryptographic mechanism.

30. Are there documented operating procedures for security requirements and access control of all networks, mission critical systems and their components that control access (e.g. firewalls, routers, web servers, application servers, etc.)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

31. Are appropriate multi-layer defense controls used to prevent unauthorized access on all connections between internal networks and systems and external networks, such as vendor's systems or the internet?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

32. Is there an enforced separation of duties in all critical process steps for all security sensitive operations?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

33. Is all sensitive information encrypted properly whenever it is stored or transmitted over all networks (either internally or externally)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

34. How well are prevention and detection systems (e.g. Antivirus, Firewalls, IDS) are deployed and monitored?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

35. How well do you feel the encryption keys are always safe from any accidental or intentional key compromise?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

36. Are backup and recovery policies and procedures documented, tested, and updated regularly for all back-end mission critical systems?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

37. How reliable is deployed security system monitors and responds to any networks intrusions, vulnerabilities, hacking or any irregularities behaviors on 24/7 basis?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

38. Are there fault tolerant or redundant components that control access to the company's trusted systems to and from all external networks (e.g. redundant firewalls, routers, web servers, application servers, etc.)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

Part V: Comprehensive Security Awareness

- *Check appropriate number*
- *Use same previous key*

Definition: Security awareness requirements are identified and affected by people. Expenditure on security awareness programs needs to be balanced against the business harm likely to result from people awareness failures, therefore, this level suggests that the scope of security awareness includes the whole of the organisation staff and encapsulates the practice of deployed security controls.

39. Has the organization developed and communicated, as appropriate, to all employees a written information technology security policy that complies with international standards such as ISO/IEC 17799?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

40. Is security awareness training program (formal or informal) conducted prior to users receiving access to an application?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

41. Are employees, consultants and contract personnel informed about the importance of security and the proper process for reporting suspected security incidents?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

42. If you had a security breach today, are you likely know or be made aware immediately?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

43. To what extent do you rate that employees have a clear understanding of their roles and responsibilities relating to information security?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

44. Are information security policies and procedures cover all lower levels requirements mentioned earlier (physical and environmental, front-end system, and back-end system)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

45. How well do you feel that your business data is always safe from accidental or malicious corruption, copying, theft or tampering?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

46. Do you have documented, tested, and updated regularly contingency plans for all lower levels systems' failure (physical and environmental, front-end system, and back-end system requirements)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

47. Are all security relevant actions on all lower levels systems requirements (physical and environmental, front-end system, and back-end system) controlled and logged?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

48. As part of the hiring/contracting process, are applicants for system administration, security administration, sensitive programming, and other positions requiring high level access to mission critical systems subject to background checks with law enforcement authorities (and government agencies if warranted)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

49. Are all sensitive security logs reviewed at least daily for suspicious activities?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

50. Are the employees, designated to respond to suspected intrusions, trained in the handling of forensic evidence, law enforcement involvement and press relations?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

51. Are there comprehensive penetration tests conducted regularly to verify the security of the whole company's perimeter which covers all lower levels requirements (physical and environmental, front-end, and back-end)?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

52. Are all resource procurements coordinated and approved by a centralized authority to ensure compliance with existing standards, including IT security standards/requirements?

5☐ 4☐ 3☐ 2☐ 1☐ 0☐

53. Is a documented organization-wide approach for risk assessment and management in place?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

54. Does a security policy review take place in response to any changes affecting the basis of the original risk assessment e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

55. Are IT assets, their ownership and agreed security classification (such as paper, expertise, electronic, etc.) clearly identified and regularly reviewed?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

56. To avoid breaches of any criminal and civil law, are all relevant statutory, regulatory and contractual requirements being explicitly defined and documented for each information system?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

57. Does your company have formal privacy policy that has been approved by legal counsel and communicated to all employees?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

Part VI: Definite Security:

- *Check appropriate number*
- *Use same previous key*

Definition: Security measurement is always a subjective rather than objective issue. Definite security could be a virtual feeling but in reality, it can never been fulfilled completely (i.e. reaches one hundred percent) since security in general is a continuous process and associated with emotions. There is no denying that there is no such system that is absolutely secured since there is no full proof "silver bullet" security solution. However, there are many systems that are rated as highly secured ones, and designed in such a way so that they almost can detect, and recover from incidents immediately.

58. To what extent do you feel physical and environmental security requirements are ultimate and totally complete?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

59. To what extent do you feel front-end system security requirements are ultimate and totally complete?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

60. To what extent do you feel back-end system security requirements are ultimate and totally complete?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

61. To what extent do you feel security awareness requirements are ultimate and totally complete?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

62. Would your company resume business and recover immediately from any major disaster such as earthquake or big fire?
5☐ 4☐ 3☐ 2☐ 1☐ 0☐

63. From the list of factors which might prevent a rigorous and complete implementation of overall controls, please select the main factor(s) causing the default:

☐Culture

☐Time

☐Budget

☐Environment (e.g. potential disaster)

☐Technology

☐Risk

☐Knowledge

☐Others (please specify):

Final comments/suggestions:

Acronyms

CMIP: Common Management Information Protocol

FTAM: File Transfer Access and Management

VTP: ISO Virtual Terminal Protocol

RTSE: Reliable Transfer Service Element Protocol

X.400: Message Handling Service (ISO email transmission service) Protocols

X.500: Directory Access Service Protocol (DAP)

CONP: Connection-Oriented Network Protocol

ES-IS: End System to Intermediate System Routing Exchange protocol

IS-IS: Intermediate System to Intermediate System

ISO-IP: CLNP: Connectionless Network Protocol

IEEE 802.2: IEEE standard definition for Logical Link Control (LLC)

IEEE 802.3: IEEE standards definition for physical layer and the media access control (MAC) sublayer of the data link layer of wired Ethernet

IEEE 802.5: IBM Token Ring standard

FDDI: Fiber-Distributed Data Interface standard

X.25: an ITU-T standard protocol suite for wide area networks using the phone or ISDN system as the networking hardware. It defines standard physical layer, data link layer and network layers (layers 1 through 3) of the OSI model

IEEE: The Institute of Electrical and Electronics Engineers

SMTP: Simple Mail Transfer Protocol

FTP: File Transfer Protocol

SSH: Secure Shell

HTTP: Hypertext Transfer Protocol

SSL: Secure Sockets Layer

TLS: Transport Layer Security

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

RSVP: Resource reservation protocol

DCCP: Datagram Congestion Control Protocol

IP (IPv4, IPv6): Internet Protocol (version 4, version 6)

ICMP: Internet Control Message Protocol

IGMP: Internet Group Management Protocol

ARP: Address Resolution Protocol

PPP: Point-to-Point Protocol

ATM: Asynchronous Transfer Mode

GPRS: General Packet Radio Services

ISDN: Integrated Services Digital Network

USB: Universal Serial Bus

GSM: Global System for Mobile Communications

PKI: Public Key Infrastructure

RSA: an algorithm named after Ron Rivest, Adi Shamir and Len Adleman

Diffie-Hellman: a key exchange cryptographic protocol

DSA: Digital Signature Algorithm

RC4: Ron's Code or Rivest Cipher 4, is a software-based stream cipher

IDEA: International Data Encryption Algorithm , a block cipher

Triple DES: formed from the Data Encryption Standard (DES) cipher by using it three times, a block cipher

AES: Advanced Encryption Standard, a block cipher

MD5: Message-Digest algorithm 5, a 128-bit cryptographic hash function

SHA: Secure Hash Algorithm, denoted SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512, are cryptographic hash functions

ECC: Elliptic Curve Cryptography

ECDH: Elliptic Curve Diffie-Hellman

ECDSA: Elliptic Curve Digital Signature Algorithm

CCTV: Closed-Circuit Television

Bibliography

[1]Alaboodi, Saad (2006), *A New Approach for Assessing the Maturity of Information Security*, Journal of the Information Systems Audit and Control Association (ISACA), Vol. 3.

[2] Wikipedia Foundation Inc. (2007), (online) *Available: http://wikipedia.org/wiki/Main_Page* (April 15, 2007).

[3] Remenyi, D. (1999), *IT Investment Making a Business Case*, Butterworth-Heinemann, Oxford.

[4] Swanson, E. (1988), *Information Systems Implementation*, Homewood, Irwin.

[5] Brancheau, J. and Wetherbe, J. (1990), *The Adoption of Spreadsheet Software: Testing Innovation Diffusion in the Context of End-user Computing*, *Information Systems Research*, 1(2), pp. 115-143.

[6] Lucas, H. Jr., Ginzberg, M. and Schultz, R. (1990), *Information Systems Implementation: Testing a Structural Model*, Ablex Publishing Corporation, Norwood, NJ.

[7] Remenyi, D. (1996), *Ten Common Information Systems Mistakes*, Journal of General Managemen., 21(4), pp. 78-91.

[8] Booty, F. (1998), *Network Management: The Bottom Line*, Manufacturing Computer Solutions, 4(5), pp. 37-40.

[9] Garrity, E. and Sanders, G. (1998), *Information Systems Success Measurement*, Hershey, Idea Group Publishing, USA.

[10] Ishman, M., Pegels, C. and Sanders, G. (2001), *Managerial Information System Success Factors within the Cultural Context of North America and a Former Soviet Republic*, The Journal of Strategic Information Systems 10(4), pp. 291-312.

[11] Farbey, B., Land, F. and Targett, D. (1999), *Moving IS Evaluation Forward: Learning Themes and Research Issues*, The Journal of Strategic Information Systems, 8(2), pp. 189-207.

[12] Remenyi, D. and Sherwood-Smith, M. (1999), *Maximize Information Systems Value by Continuous Participative Evaluation*, Logistics Information Management, 12(1/2), pp. 14-31.

[13] Keil, M., Wallace, L., Turk, D., Dixon-Randall, G. and Nulden, U. (2000), *An Investigation of Risk Perception and Risk Propensity on the Decision to Continue a Software Development Project*. Journal of Systems and Software 53(2), pp. 145-157.

[14] Macmillan, H. (1997), *Managing Information Systems: Three Key Principles for General Managers*, Journal of General Management 22(3), pp. 12-23.

[15] Broadbent, M., Butler, C. and Hansell, A. (1994), *Business and Technology Agenda for Information Systems Executives*. International Journal of Information Management, 14(6), pp. 411-426.

[16] McKeen, J., Smith, H. and Parent, M. (1996), *An Integrative Research Approach to Assess the Business Value of Information Technology*, Proceedings of the Third European Conference on the Evaluation of Information Technology, Bath, November, United Kingdom.

[17] Pumo, J. (1996), *Delivering IT Value in Three Easy Steps*, Planning Review, 24(1), pp. 42-43.

[18] Earl, M. (1989), *Management Strategies for Information Technology*, London, Prentice Hall.

[19] Barne, S. (June, 1997), *A Cause Map Approach to Assessing IS Implementation and Evaluation in the UK Health Sector*, Proceedings. Fifth European Conference on Information Systems. Cork, United Kingdom.

[20] Symantec (2007), *Managing Enterprise Security*, (online) Available: http://www.symantec.com/index.jsp (Jan 10, 2007).

[21] Alaboodi, Saad (May, 2003), *Proposal of New Approach for Assessing the Maturity of Information Security*, Master's Thesis, Hull University, UK.

[22] Browne, J.A. (1997), *You Can't Manage What You Can't Measure*, Information Technologies for Utilities, Prentice Hall, New York.

[23] Gates, Bill (May, 2001), *Business @ the Speed of Thought: Succeeding in the Digital Economy*, Warner Books.

[24] Losee, Robert M. (March, 1997), *A Discipline Independent Definition of Information*, Journal of the American Society for Information Science, Vol. 48, Issue 3, 254-269, John Wiley & Sons Inc., New York, NY, USA.

[25] Shannon, Claude (1949), *Communication Theory of Secrecy Systems, Bell System Technical Journal*, vol.28(4), page 656–715.

[26] McDaniel, George, ed. (1994), *IBM Dictionary of Computing*, New York, NY: McGraw-Hill, Inc.

[27] Essinger, J. (2001), *Internet Trust and Security*, Britain: Addison –Wesley.

[28] Gollmann, Dieter (1999), *Computer Security*, John Wiley & Sons. Inc., 605 Third Avenue, New York, NY 10158-0012.

[29] Carnegie Mellon Software Engineering Institute (2006), *Capability Maturity Model Integration (CMMI)*, (online) Available: http://www.sei.cmu.edu/cmmi (November 03, 2006).

[30] Phillips, Mike (March 2003), *Using a Capability Maturity Model to Derive Security Requirements*,

SANS Institute.

[31] ISO (2000), International Organization for Standardization, *ISO/IEC 17799, The International Standard Code of Practice for Information Security Management*.

[32] Maslow, A. (1970), *Motivation and Personality*, 2nd ed., Harper & Row.

[33] Mullins, L. J. (1999), *Management and Organizational Behavior*, 5th Edition, Financial Times Prentice Hall, London, (originally published in 1985).

[34] Martin, J. (2001), *Organizational Behaviour (2nd edn.)*, Thomson Learning, London.

[35] Gartner Dataquest (2001, June 1), *The U.S. Security Services Market Forecast*, 2000–2005.

[36] CBI The Voice of Business (2001), *Cybercrime Survey 2001, Making the information superhighway safe for business*, Waterside Press.

[37] British Standards Institution (2000), *BS 7799-1, Code of Practice for Information Security Management*, British Standards Publishing Limited BSPL, London.

[38] British Standards Institution (2002), BS 7799-2, *Information Security Management Systems – Specification with guidance for use*, British Standards Publishing Limited BSPL, London.

[39] Harris, Shon (September, 2005), *CISSP All-in-One Exam Guide*, 3rd Edition, McGraw-Hill Osborne Media.

[40] Brink, D. and RSA Security (2002), *PKI and Financial Return on Investment: white paper*, PKI Forum Inc.

[41] ISSEA (2007), International Systems Security Engineering Association, (online) Available: http://www.issea.org (Feb 5, 2007).

[42] ISO (2002), International Organization for Standardization, ISO/IEC 21827, *Information technology-Systems Security Engineering - Capability Maturity Model (SSE-CMM®)*.

[43] SSE-CMM (2007), Systems Security Engineering – Capability Maturity Model, (online) Available: http://www.sse-cmm.org/index.html (March 9, 2007).

[44] Systems Security Engineering Capability Maturity Model (June 15, 2003), *SSE-CMM Model Description Document*, Version 3.0.

[45] Systems Security Engineering Capability Maturity Model (April 16, 1999), *SSE-CMM Appraisal Method (SSAM)*, Version 2.0.

[46] ITGI (2005), IT Governance Institute, *Control Objectives for Information and related Technology (COBIT)*, Version. 4, USA, (online) Available: www.itgi.org, (Feb 7, 2007).

[47] NIST (2005), National Institute of Standards and Technology, *Computer Security Resource Center (CSRC), Program Review for Information Security Management Assistance (PRISMA)*, (online) Available: http://prisma.nist.gov/index.html (March 12, 2007).

[48] Canal, Vicente Aceituno (2006), *ISM3, Information Security Management Maturity Model*, Version1.20. Creative Commons.

[49] The University of New Haven Center for Cybercrime and Forensic Computer Investigation and The University of Southern California Department of Mathematics (2001), *Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security*, Information Systems Control Journal (ISACA), Volume 2.

[50] OCTAVE (2007), *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework*, Version 1.0, (online) Available:http://www.cert.org/octave/ (April 5, 2007).

[51] Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (August, 2003), *Introduction to OCTAVE approach*, Carnegie Mellon, Software Engineering Institute, Pittsburgh.

[52] CRAMM (2005), *CCTA Risk Analysis and Management Method CRAMM*, Version 5.1, (online) Available: http://www.cramm.com (Jan 20, 2007).

[53] Chapin, D. A., Akridge, S. (2005), *How Can Security Be Measured?*, Journal of the Information Systems Audit and Control Association (ISACA), Volume 2.

[54] IETF (2007), The Internet Engineering Task Force, (online) Available: http://www.ietf.org/ (Feb 2, 2007).

[55] RFC (2007), The Request for Comments, (online) Available: http://www.rfc-editor.org/ (March 5, 2007).

[56] ITU (2007), International telecommunication Union, (online) Available: http://www.itu.int (Jan 10, 2007).

[57] IEEE (2007), The Institute of Electrical and Electronics Engineers, (online) Available: http://www.ieee.org (April 22, 2007).

[58] Network Dictionary (2007), (online) Available: http://www.networkdictionary.com/ (March 8, 2007).

[59] Greenspan, A. (February 13, 2001), *Federal Reserve Board's semiannual monetary policy report to the Congress, Before the Committee on Banking, Housing, and Urban Affairs*, U.S. Senate.

[60] ISO (2005), International Organization for Standardization, *ISO/IEC 27001, Specification for an Information Security Management System.*

[61] ISO (2005), International Organization for Standardization, *ISO/IEC 17799, Information technology - Security techniques - Code of practice for information security management.*

[62] SANS Institute (2001), *The Weakest Link: The Human Factor Lessons Learned from the German WWII Enigma Cryptosystem*, (online) Available: http://www.sans.org (Feb 22, 2007).

[63] National Security Agency (2007), *Central Security Service, NSA Suite B Cryptography*, (online) Available: http://www.nsa.gov/ia/industry/crypto_suite_b.cfm (March 9, 2007).

[64] NIST (2007), National Institute of Standards and Technology, *Computer Security Resource Center (CSRC)*, NIST Special Publications – 800 Series, (online) Available: http://csrc.nist.gov/publications/nistpubs/ (Feb 15, 2007).

[65] Berinato, Scott, and Ware Lorraine C. (Sep 15, 2004), *Six Secrets of Highly Secure Organizations*, CIO Magazine.

[66] ERNST & YOUNG (2004), *Global Information Security Survey*, (online) Available: www.ey.com (Jan 20, 2007).

[67] Mark R. McNeilly (2001), *Sun Tzu and the Art of Modern Warfare*, Oxford University Press, USA.

[68] ERNST & YOUNG (2006), *Achieving Success in a Globalized World: Is Your Way Secure? Global Information Security Survey*, (online) Available: www.ey.com (Jan 20, 2007).