Enterprise Information Security Management Framework [EISMF]

by

Dhirendra Sharma

B.E. Electrical Engineering (with First Class Honors, 1995)

Panjab University, India

Submitted to the System Design and Management Program
In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

February 2011

Signature of Author: ______________________________
System Design and Management Program
February, 2011

Certified By: ______________________________
Michael Cusumano
Sloan Management Review Distinguished Professor of Management
Thesis Supervisor

Accepted By: ______________________________
Patrick Hale
Director, System Design and Management Program

Enterprise Information Security Management Framework [EISMF]

by
Dhirendra Sharma

Submitted to the System Design and Management Program
on February, 2011, in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

ABSTRACT

There are several technological solutions available in the market to help organizations with information security breach detection and prevention such as intrusion detection and prevention systems, antivirus software, firewalls, and spam filters. There is no doubt in the fact that significant progress has been made in the technological side of information security. However, when we study causes of information security breaches, we find that a significant number are caused by non-technical reasons such as social engineering, theft of computing device or portable hard drive, human behavior, and human error. This leads us to conclude that information security should not be viewed through technology perspective only. Instead, a more holistic approach is required. This thesis provides a systems approach towards information security management and include technological, management and social aspects.

This thesis starts with introduction especially background and motivation of the author, followed by literature research. Next, Enterprise Information Security Management Framework is presented leading to estimation of an organization's information security management maturity-level. Finally, conclusion and potential future work are presented.

Thesis Supervisor: Michael Cusumano

Title: Sloan Management Review Distinguished Professor of Management

ACKNOWLEDGEMENTS

I would like to thank almighty God for giving me never ending thirst for knowledge and making me an avid learner. MIT has given me great opportunities to quench my thirst of knowledge and provided me challenges to stay in the learning mode.

I consider myself very lucky to have Professor Michael Cusumano as my thesis supervisor. I am extremely thankful to him for his constant guidance and encouragement during my thesis writing journey.

I would also take this opportunity to thank Professors Brad Morrison, Ed Crawley, Eric von Hippel, Erik Brynjolfsson, George E. Apostolakis, Michael Davies, Qi Van Eikema Hommes, Ralph Katz, Richard de Neufville, Scott Keating, Tom Allen, Shalom Saada Saar, Val Livada, and Victor Martinez-de-Albeniz. I have learned a lot from them. This thesis leverages many of their holistic thinking concepts.

I sincerely thank MIT System Design and Management program. I am extremely grateful to Pat Hale for responding to my email questions even late at night and keeping his office doors open whenever I needed his advice. Sincere thanks to Bill Foley, Dave Shultz, and Chris Bates for always helping me whenever I needed any help. I thank all my fellow classmates, from whom I learned a lot.

This great endeavor would not have been possible without the support of my family. I thank my late grandparents and my late father, whose principles and love guide me. Sincere thanks to my mother who always believes in me and constantly encourages me to accept new challenges in life. I thank my wife for her constant love, encouragement and support. I am extremely thankful to my sons for their tremendous patience and understanding throughout this journey.

Finally, I bid farewell to MIT. Thank you for everything.

God bless everyone.

DISCLAIMER

Please note that in Enterprise Information Security Maturity Level Calculations *(Tables 4 through 20)*, data shown under columns - Weight (in percentage) and Enterprise Self Estimation (percentage completion) is purely hypothetical. It was NOT obtained from any organization. Any match with any organization is purely coincidental.

Readers should not derive any organization specific information from this work. The Enterprise Information Security Management Framework (EISMF) should be used as a roadmap for taking a *systems approach towards information security management*.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

CDF	:	Code of Federal Regulations
CISO	:	Chief Information Security Officer
CIO	:	Chief Information Officer
CMMI	:	Capability Maturity Model Integration
COBIT	:	Control Objectives for Information and related Technology
COPP	:	Children's Online Privacy Protection Act
COSO	:	Committee of Sponsoring Organizations of the Treadway Commission
CTO	:	Chief Technical Officer
DoD	:	Department of Defense
DSS	:	Data Security Standard
EISMF	:	Enterprise Information Security Management Framework
FERC	:	Federal Energy Regulatory Commission
FACTA	:	Fair and Accurate Credit Transactions Act
FDA	:	Food and Drug Administration
FFIEC	:	Federal Financial Institutions Examination Council
FERPA	:	Family Educational Rights and Privacy Act

GAISP	:	Generally Accepted Information Security Principles
GISRA	:	Government Information Security Reform Act
HIPAA	:	Health Insurance Portability and Accountability Act
IBM PRM for IT	:	IBM Process Reference Model for Information Technology
IEC	:	International Electrotechnical Commission
IS	:	Information Security
ISACA	:	Information Systems Audit and Control Association
ISATRP	:	Information Security Assurance Training and Rating Program
ISECOM-SOMA	:	Institute for Security and Open Methodologies-Security Operations Maturity Architecture
ISSA	:	Information Systems Security Association
IT	:	Information Technology
ISF	:	Information Security Forum
ISM3	:	Information Security Management Maturity Model
ISMS	:	Information Security Management Standards
ISO	:	International Organization for Standardization
ITIL	:	Information Technology Infrastructure Library
ITUP	:	IBM Tivoli Unified Process
MOF	:	Microsoft Operations Framework
NERC	:	North American Electric Reliability Council
NIST	:	National Institute of Standards and Technology
OCTAVE	:	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OSSTMM	:	Open Source Security Testing Methodology Manual

OWASP	:	Open Web Application Security Project
OWASP –ASVS	:	OWASP-Application Security Verification Standard
PA-DSS	:	Payment Application Data Security Standard
PCI	:	Payment Card Industry
PII	:	Personally Identifying Information
PIN	:	Personal Identification Number
PTS	:	PIN Transaction Security
SSE-CMM	:	Systems Security Engineering Capability Maturity Model.
U.K	:	United Kingdom
U.S	:	United States of America

CHAPTER 1: Introduction

1.1 Background and Motivation

Information security and its management had been of tremendous concern to mankind since beginning of human civilization. With the advent of computers and their rapid adoption in commercial and personal domain, information has become a commodity of immense value. In this networked information age, "security" has acquired a special status in our digital life. We find that most of our personal information including financial information is stored and accessible online. Our social and business communication via email hops through various servers, telephone conversation goes through various towers and satellite, and social networking information is stored on distant servers. Hence, it is vital to manage technical, business and social aspects of information security.

In last four decades, as a result of tremendous progress in the technical side of information security, we have seen several information security related products and services. In contrast, significantly less attention has been given to comprehensive information security management. Information security is no longer just a technical challenge but it is a business and social challenge as well. Solving technical side of information security got a big push with the outbreak of virus in the public domain such as Melissa virus (March, 1999) which infected over a million[1] computers in the United States. However, information security breach is possible without involving a sophisticated technological attack such as involving virus, worm or phishing email. For example, it could happen when an employee loses his or her computer with sensitive information. Similarly, social engineering could lead a person to unknowingly give away confidential information.

[1] United States Department of Justice, Computer Crime & Intellectual Property Section, World Wide Web, Retrieved on July 28, 2010 from http://www.justice.gov/criminal/cybercrime/ccpolicy.html

Privacy Rights Clearinghouse (PRC)[2] has created a database of data breaches within the United States starting from April, 2005 and it is updated frequently. When we analyze PRC data from July 01, 2010 through July 20, 2010, we find that breaches are *caused* due to several reasons such as loss of computer device/data drive either inadvertently or stolen carrying sensitive information, loss of computer files, employee giving out information to the public domain, dumping physical files with critical information in public waste management area, information mailed to incorrect physical address, *unauthorized access to an information database*, unattended/unprotected area containing sensitive information, email with confidential information sent to an incorrect email address, improper electronic file sharing within an organization, *virus infection*, impersonation, physical security breach, employee stealing information, incorrect display of information online, *hacking*, accidental disclosure of information, and natural disaster.

From the above data, we find that only three causes – *unauthorized access to an information database, virus infection* and *hacking* are technical in nature. Remaining causes are related to physical security (which could lead to theft or loss of computer device/hard drive), social engineering, human behavior, human error, and information storage recycling. *Therefore, majority of information security breaches are due to non technical reasons.* To further support our conclusion, we take a look at *Figure 1*. It clearly shows that in year 2009, major cause of data breach (across different industries) was theft leading to loss of a computer or an information storage medium.

Hence, we need to look at information security management in a much broader and holistic way beyond the lenses of technology which brings us to *Enterprise Information Security Management Framework.*

[2] Privacy Rights Clearinghouse, Chronology of Data Breaches, Security Breaches 2005-Present, World Wide Web, Retrieved on July 28, 2010 from http://www.privacyrights.org/data-breach

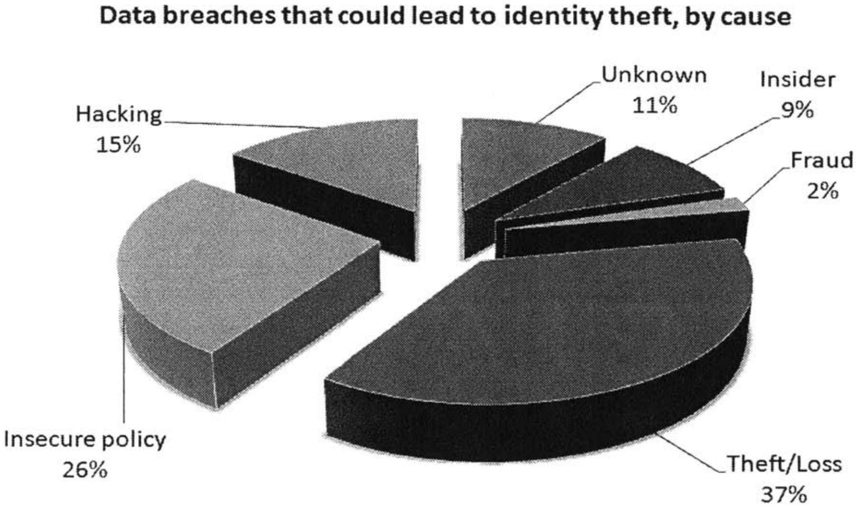


Figure 1: Data breaches that could lead to identity theft, by cause

(Source: page29, Symantec Global Internet Security Threat Report, Trends for 2009, Volume XV, Published April 2010[3]*)*

1.2 Objectives

This thesis has three objectives:

- Firstly, create an Enterprise Information Security Management Framework which would facilitate a comprehensive approach towards information security management at an enterprise level along with ability to track progress by way of estimation of enterprise information security management maturity level.
- Secondly, framework should capture role of senior management, stress alignment of information security objectives with enterprise goals, and bring out role of all of the employees in information security management.
- Finally, framework should be holistic so that technological, business, and social aspects of information security management are addressed. Framework should facilitate security of entire business rather than just the information systems.

[3] Symantec Corp. (2010), Symantec Global Internet Security Threat Report, Trends for 2009, Volume XV, Published April 2010, World Wide Web, Retrieved on July 28, 2010 from http://www.symantec.com/business/theme.jsp?themeid=threatreport

1.3 Structure of the thesis

Following steps are taken to construct this thesis:

- Chapter 1 – Introduction
  - Author's motivation, thesis objective and thesis structure are covered in this chapter.

- Chapter 2 – Literature Review
  - Current state of research in the field of comprehensive information security management is covered in this chapter. It includes some definitions which are critical for our understanding.

- Chapter 3 – Enterprise Information Security Management Framework
  - This covers the actual framework

- Chapter 4- Information Security Management Maturity Level based on EISMF
  - This chapter covers the key criterion for each point in the fourteen point EISMF
  - Using the fourteen point EISMF and key criterion, information security management maturity level is established. Sample calculation is shown as well.

- Chapter 5 – Conclusion and Future Work
  - Summary of key features of framework and information security management maturity level is captured here with regards to the stated objectives.
  - Looks at potential research opportunities.

CHAPTER 2: Literature Review

2.1 Terminology

There are two terms which need an explanation. One is *information* and the other is *security*.

First, we look into definition of *information*. Merriam Webster online dictionary has four different meanings for it. One of the four meanings close to the context of our discussion is "the communication or reception of knowledge or intelligence". However, we find that definition of information given by ISO (International Organization of Standardization) is much more relevant to our discussion here –"Information is an asset, which, like other important business assets, adds value to an organization and consequently needs to be protected."[4]

Second, we look into the definition of *security*. Merriam Webster online dictionary has four different meanings for it. One of the four meanings close to the context of our discussion is "freedom from danger". Danger to an organization could come from internal or external channels.

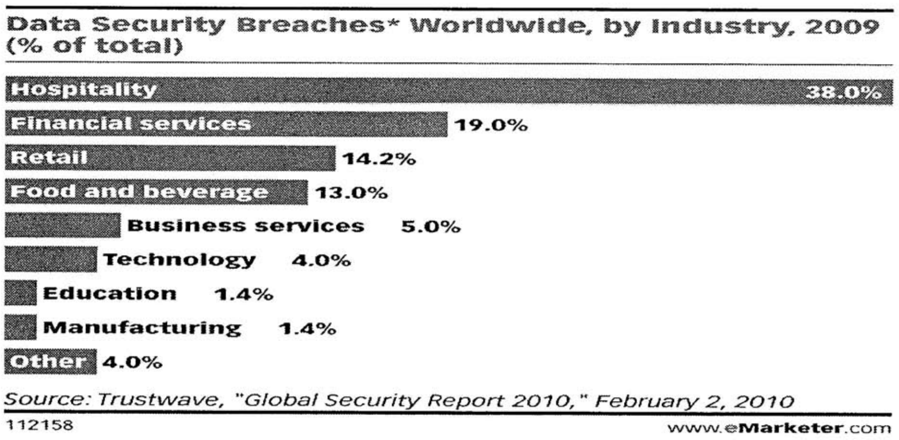
We know that information is not necessarily in electronic form only. It could be in verbal, hand written, or typed forms as well. This makes it necessary for us to look beyond securing the information systems or software security. Although securing the information systems is critical for businesses but it is not a complete solution because information breach could happen without involving any information system. Solution must involve a systems perspective and a holistic approach. All IT (Information Technology) and non-IT staff must be involved in securing an enterprise. Hence, solution must be multi-disciplinary.

[4] International Organization of Standardization (ISO), World Wide Web, Retrieved on July 30, 2010 from http://www.iso.org/iso/iso_cafe_management_systems.htm

2.2 Overview of Recent Trends in Information Security

In the year 2009, the war between those who secure the information and those who are looking to exploit loopholes continued. The number of information data breaches which involved PII (Personally Identifying Information) that came to public knowledge in 2009 was 582[5] with approximately 221 million[5] records impacted. However, this number in 2008 was 775[5] with nearly 87 million[5] records impacted. One reason for decline could be increasing effectiveness of government agencies in catching the cyber culprits. For example, Wall Street Journal reported on August 18, 2009 that federal agents charged Albert Gonzalez who along with two other accomplices was involved in stealing information on 130 million[6] credit and debit cards from five companies. Catching Albert Gonzalez and other criminals might explain decline in reported breaches in year 2009.

Based on eMarketer –"Data Security Breaches Worldwide, by industry, 2009" report and Verizon Business's –"2010 Data Breach Investigations Report", we learn that three industries namely: *Financial Services, Hospitality* and *Retail* are leading target for information data breach [Refer Figure 2 and 3].


Data Security Breaches* Worldwide, by Industry, 2009
(% of total)

Source: Trustwave, "Global Security Report 2010," February 2, 2010

Figure 2: Data Security Breaches ***(Source: eMarketer)***

[5] Open Security Foundation, Data Loss Database, Retrieved on August 08, 2010 from http://datalossdb.org/reports

[6] Wall Street Journal, Arrest in Epic Cyber Swindle (dated August 18, 2009), Retrieved on August 08, 2010 from http://online.wsj.com/article/NA_WSJ_PUB:SB125053669921337753.html

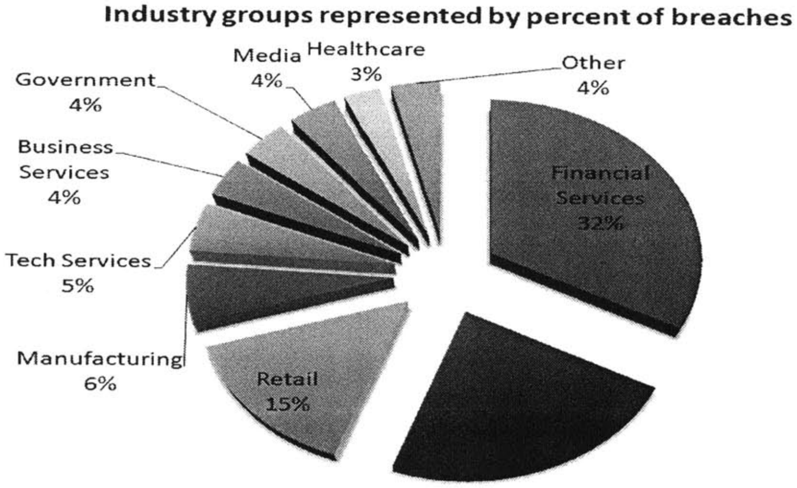


Figure 3: Data Breaches by Industry *(Source: VerizonBusiness)*

Companies make every effort to not get negative media attention due to an information security breach. As a result, management is constantly analyzing their information security infrastructure and investing in protection of information resources.

We find the following from a recent Forrester report titled-"The State Of Enterprise IT Security And Emerging Trends: 2009 To 2010" by Jonathan Penn:

- In year 2010, 42% companies are planning to increase investment in latest info security products by more than 5% from their 2009 budget values. 38% companies are planning to increase security investment by more than 5% for upgrading their existing info security infrastructure. 29% companies are considering increasing the expenditure on authorized copies of various information system hardware and software by more than 5%. 21% companies are planning to increase the number of information security employees while 19% are planning to hire outside experts on a temporary basis (Refer Figure 4). [Forrester]

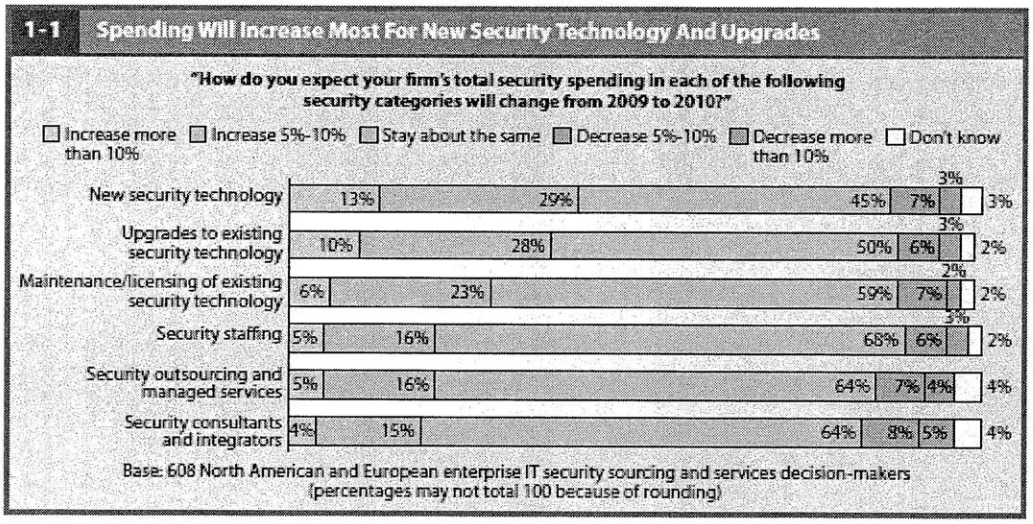


Figure 4: IT Security Spending Plans *(Source: Forrester)*

- For 89% companies "data security" [Forrester] is a top priority in year 2010. 85% companies are concerned in a major way about proactively "managing vulnerabilities and threats" [Forrester]. 81% companies are either looking for ways to reduce cost or improve performance or both (Refer Figure 5). [Forrester]

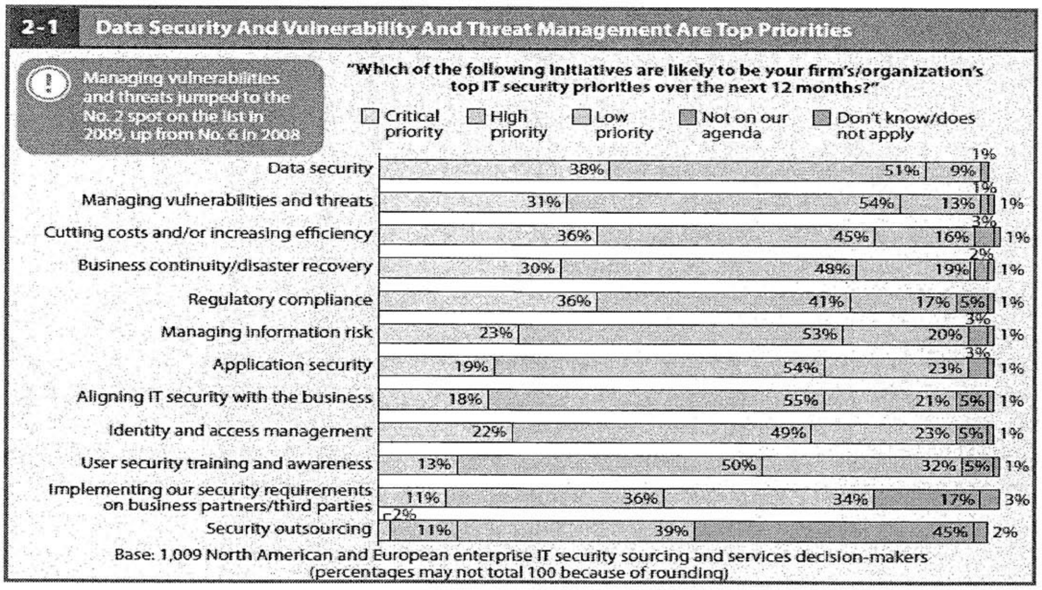


Figure 5: Priorities *(Source: Forrester)*

2.3 Recent Trends in Information Security Breaches: Phishing

Merriam-Webster online dictionary defines phishing as "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly". It usually involves users themselves giving out confidential information such as user name, password, bank account number or credit card information. This happens when user clicks on a website link received in an email and follow instructions which eventually lead a user to give out confidential information.

Sector	2009 Percentage	2008 Percentage
Financial	74%	79%
ISP	9%	8%
Retail	6%	4%
Insurance	3%	2%
Internet Community	2%	2%
Telecom	2%	2%
Computer Hardware	1%	1%
Government	1%	1%
Computer Software	<1%	<1%
Transportation	<1%	<1%

Table 1: Different phished sectors ***(Source: Symantec Corp. 2010)***

From Symantec's most recent internet security report titled "Symantec Global Internet Security Threat Report" (Symantec Corp., 2010), we find the following:

- Trade names used in phishing emails were mainly related to financial sector companies (*Refer Table 1*). [Symantec Corp., 2010]
- Financial sector was the most phished sector in year 2009 (*Figure 6*). Getting access to someone's financial accounts is definitely profitable for phishers as financial information is an easy sell in the underground economy. ISPs (Internet Service Provider) were the next

most phished sector. ISP information gained may not have direct financial benefits, however it offers other benefits. For example, getting access to an ISP account could provide email addresses of users which could be used to send spam emails. Big benefit from access to an ISP account in the underground economy comes from ability to host illegal internet web pages. [Symantec Corp., 2010]

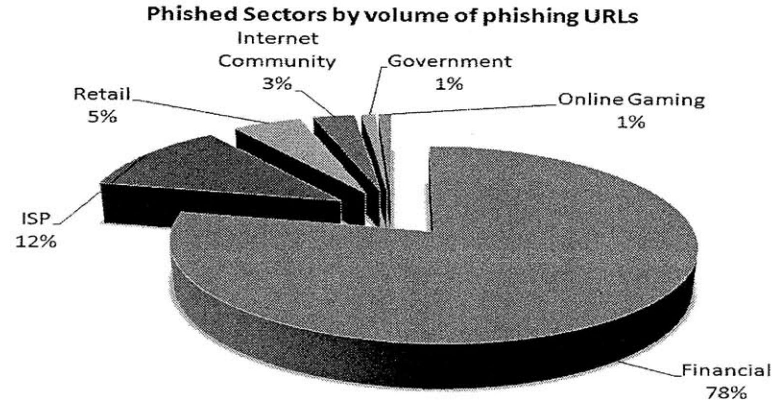


Figure 6: Phished sectors by volume of phishing URLs ***(Source: Symantec Corp. 2010)***

- Retail was the third most phished sector (Refer Figure 6). This is not a surprise because in 2009 retail sales via internet increased by more than 14%[7]. From phishing perspective, online retail is an attractive sector because buyers need to provide personal information such as user name, password and financial information such as credit or debit card information. If phishers are able to get either personal or financial or both, they can easily sell the information in the underground economy or they could use it themselves to make online purchases. [Symantec Corp., 2010]

[7] Coremetrics, Press Releases, 2009 Press Release, World Wide Web, Retrieved on August 01, 2010 from
http://www.coremetrics.com/company/2009/pr12-21-09-online_retail_sales.php

In summary, primary objective behind phishing is monetary benefit. Financial sector remains the most phished sector because probability of gaining access to an online bank account is much higher.

2.4 Recent Trends in Information Security Breaches: Spam

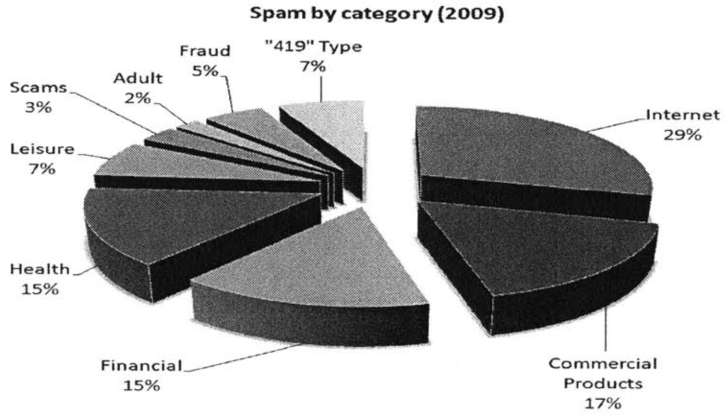


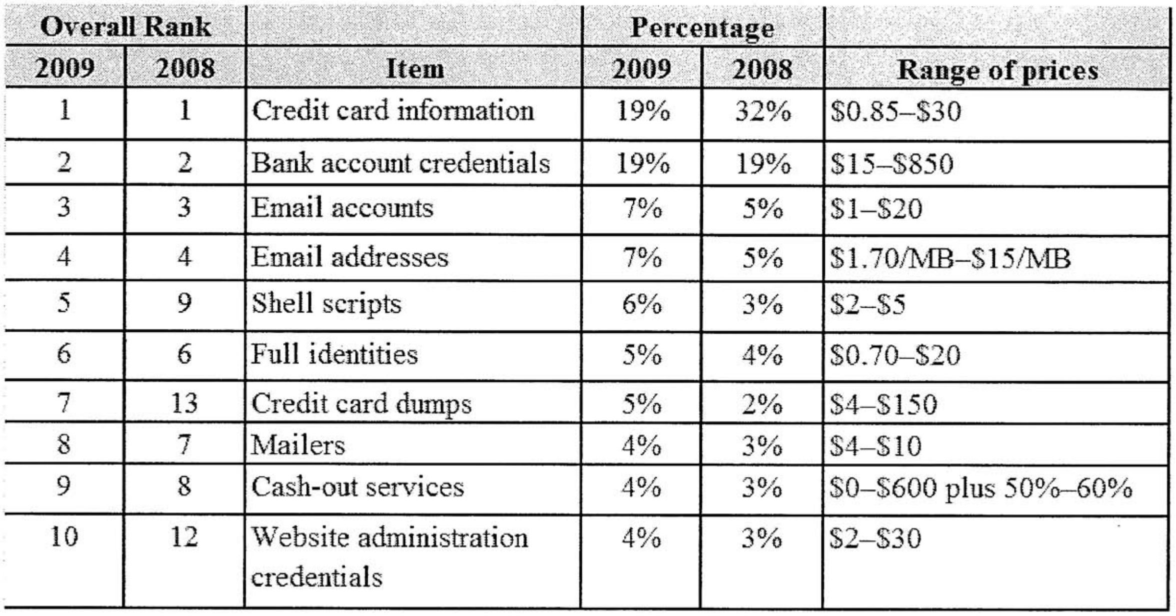
Figure 7: Spam by category - 2009 ***(Source: Symantec Corp. 2010)***

From "Symantec Global Internet Security Threat Report" (Symantec Corp., 2010), we learn the following about spamming activities for year 2009:

- In 2009, internet was the lead spam category (Refer Figure 7). This category includes spam such as online education. Due to downturn in the economy in 2009, spammers saw an opportunity to lead web users to a fraudulent education website which asked for payment information as part of online application form. [Symantec Corp., 2010]
- Next spammed category was commercial products which include flowers, sweets, apparel, home decoration and other personal gift items. Commercial products spam was timed according to festivals. For example, personal gift items dominated in December due to Christmas. [Symantec Corp., 2010]
- Financial and Health were the third most spammed categories. Due to the economy, financial vulnerability was high and spammers capitalized on it by sending emails that offered financial rescue to their readers. Similarly, mortgage crisis and high

unemployment were leveraged by spammers. Spammers sent emails such as work remotely from home or ways to prevent house sale by bank due to lack of mortgage payment. [Symantec Corp., 2010]

2.5 Information black market



Overall Rank			Percentage		
2009	2008	Item	2009	2008	Range of prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 2: Different items on sale in the information black market ***(Source: Symantec Corp. 2010)***

From “Symantec Global Internet Security Threat Report” (Symantec Corp., 2010), we learn the following about the information underworld activities for year 2009:

- We find that credit card information is a major item for sale in the underworld market place. [Symantec Corp., 2010]
- Credit card dump (at number 7 in Table 2) is different from credit card information. “A credit card dump is an exact copy of the encoded data contained in the magnetic stripe on a credit card. The dump data can be written to the magnetic stripes of counterfeit credit cards and then the duplicates can be used as though they were the original card.” *(page 74, Symantec Corp., 2010)*

- Bank account information is popular item for sale in the underground economy because it allows immediate monetary benefit. Once bank information is available, money could be withdrawn from the account quite easily. [Symantec Corp., 2010]
- Next on the list in Table 2 is email account. Email account facilitates spam in a more trust worthy way. More people are likely to believe in the contents of an email message from a trust worthy source (for example, email received from a known person). Address books could be used to send more spam. People store both personal and financial information in self sent emails or email drafts. [Symantec Corp., 2010]

Popularity of credit card and banking information in the underworld economy leads us to conclude that these illegal activities are primarily geared towards making quick bucks.

2.6 Recent research in Enterprise Information Security Management

Research interest has grown over the years in exploring ways for efficient information security management. We look at some of the work in this domain.

a) Pishva et al (2007), researched "information security at local governments in Japan" and finally proposed two key elements (discussed later) for improving information security management framework at local governments. They found that in year 2005 there was a significant jump from previous year in the number of organizations reporting an information breach (Refer Table 3).

Year	2002	2003	2004	2005
Total Number of Organizations Reporting	63	57	366	1032
Number of victims	418,716	1,544,592	10,435,061	8,814,735
Average Number of Victims per Incident	7,613	30,482	31,057	8,922

Table 3: Information Breach Reporting – Japan ***(Source : Pishva et al (2007))***

As part of their research, Pishva et al looked into computer virus statistics for Japan from 1990 through to 2005, security auditing methodology, different information security standards used in Japan, government issued guidelines for managing information security, and studied "Hyogo Prefectural Government" in depth. They reached an important conclusion –

"It seems that institutionalized efforts toward implementing information security have focused on protecting the systems rather than the valuable information that are stored therein." (Pishva et al , 2007).

Example is given of an information breach by an employee who can simply give out information without any traceability. Hurdles in implementing information security policy were identified. For example, work over load of IT staff, and lack of proper communication among information consumers, management and IT staff. Managers tend to off load management of information security to technical staff. Information security is mostly given to an external organization which makes technical staff to not monitor work very closely because they assume external company is doing all the contractual work.

Finally, two recommendations are made that should be the basis of an improved information security management framework.

- First recommendation is - "adoption of practical techniques" (Pishva et al , 2007). This includes focus on IT staff, their skills and their familiarity with overall organizational security objectives. Close monitoring by internal IT staff when new information systems are brought in and installed by external companies. Comprehensive emphasis on all layers of technical information security is recommended. This includes operating system layer, network layer and application layer. On the non technical side, policy should be put in place so that information is not given out by authorized people such as system administrators or other employees. Systems with proven security track record should be widely used and proven best practices should be implemented across an organization. [Pishva et al , 2007]
- Second recommendation is –"refinement of procedures" (Pishva et al , 2007). The focus here is on constant analysis of security threats and constant refinement of security methods. Managers should be made more accountable for implementation of various security methods instead of technical people such as system administrators. [Pishva et al , 2007]

Hence, from this (Pishva et al , 2007) paper, certain critical characteristics of a comprehensive information security management framework stand out. These include: Employee training, clear communication, constant information security threat analysis, and constant upgrade of security methods and policies.

b) Zulhuda (2009), explored common points between different information security standards and government legislations. In particular, Zulhuda looked into Information Security Management Standards (ISMS) - ISO 27000 series and information security laws in the U.S and the U.K.

For obvious reasons, law has a distinct advantage because not abiding by the law is a criminal offense. With the increase in information security breach in the public domain, various governments have taken initiative within their jurisdiction to come up with statutory model which lays down responsibilities for organizations storing information such as financial or health.

Standards such as ISO/IEC 27002: 2005 ("Information technology -- Security techniques -- Code of practice for information security management") necessitate abiding by applicable government laws. Laws on the other hand could be industry specific. For example, in the United States, FISMA - Federal Information Security Management Act (2002), is applicable to government organizations. Sarbanes-Oxley Act applies to publicly traded companies and their partners.

Information security standards are geared towards securing information assets of an enterprise while attempting to maximize return on information security investment. Government regulations are put in place to protect the rights of consumers. Hence, information security standards and government laws are written from different perspective while attempting to handle a common concern – information security. There is a major disconnect between lawyers and technical people. On one hand, technical people do not quite understand applicable information security laws. On the other hand, lawyers are not at ease with information security jargon.

Even though there are differences between law and industry standards as discussed above, Zulhuda (2009) came up with following three overlapping points between legal frameworks and information security standards:

- First, both highlight the need for information security with same eventual result. For example, industry information security standards as well as major laws both acknowledge that "objective of information security is to safeguard the confidentiality, integrity and availability of information assets" [Zulhuda (2009)]
- Second, both require that organization must put processes in place to ensure safety of human, financial, and other resources of a company. For example, ISO/IEC 27001:2005 requires proper record-keeping and documentation, regular review of various processes within an organization, proper handling of all material and non material resources. This is in agreement with laws such as Sarbanes Oxley Act of 2002. [Zulhuda (2009)]
- Finally, when an organization follows a standard, it fulfills certain requirements of an applicable local law. As we saw above, proper management of all resources is a step towards compliance with a local law. [Zulhuda (2009)]

We conclude that compliance is an integral part of enterprise information security management framework.

c). Solms (2000) wrote in year 2000 that development of information security could be divided into three waves as explained below.

From the early days of computing to beginning years of 1980s could be thought of as "First Wave" [Solms (2000)] or "Technical Wave" [Solms (2000)]. This was the time of large computing machines called the mainframes. Purely technical solutions were created for ensuring information security. Users were given user names and allowed to choose their passwords. Some authorization scheme was put in the mainframe which limited the user access to information depending on the identity of the user based on user name used for log in. Management was not involved. Users were not educated on the strength of their passwords or other critical aspects of information security. People on the technology side working on information security began to think that management should work closely with them. Overall, information security remained purely a technical challenge during this period.

From early years of 1980s to mid 1990s, is the "Second Wave" [Solms (2000)] or "Management Wave" [Solms (2000)]. During this time frame, management got more and more involved with information security. Wide spread adoption of client server model during the 1980s, introduction of the worldwide web, and development of internet based business led to information security getting attention from top management. Management started putting procedures in place for ensuring information security. Staff was hired for dedicated information security work. However, after some time, management wanted to know what return on information security investment they were getting. They also wanted to know what other companies were doing and where they stand as far as information security was concerned. Note that first wave continued during this time.

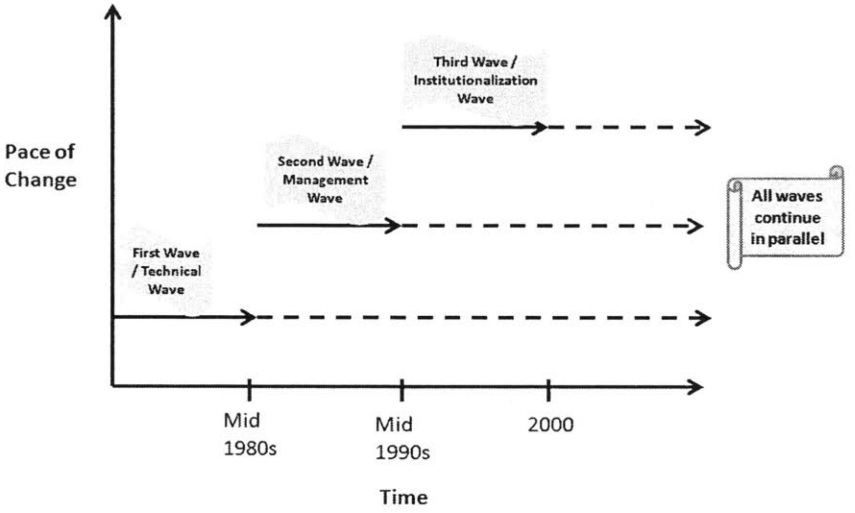

Pace of Change
Third Wave / Institutionalization Wave
Second Wave / Management Wave
First Wave / Technical Wave
All waves continue in parallel
Mid 1980s
Mid 1990s
2000
Time

Figure 8: Information Security — The Third Wave?

(Source: Solms (2000) and Helokunnas et al (2003))

"Third Wave" [Solms (2000)] or "Institutionalization" [Solms (2000)] started in the mid 1990s. Key features include the following:

- Emergence of various IS standards. For example, British Standards Institute published BS 7799 – an IS Management standard in February, 1995[8].[Solms (2000)]
- To establish trust among companies sharing electronic information, certifications/accreditations came along. They were a way to show business partners that company is serious about information security. [Solms (2000)]
- It was felt that employees may pose greatest information security threat mostly due to lack of awareness. Therefore, organizations started educating their employees on the importance and ways of information security. [Solms (2000)]
- Methods were developed to measure information security effectiveness. [Solms (2000)]

Solms (2000) talks about possibility of a "Fourth Wave" called "Commodity Wave". Solms (2000) says the following:

"This wave may be characterized by information security having become such a commodity that it is not an issue anymore — it totally disappears from the radar screen. Personally I doubt such a wave, precisely because of the absolute impact of the human dimension of information security." [Solms (2000)]

In summary, from Solms (2000) paper we learn that for an efficient information security management, an applicable standard should be followed at an enterprise level coupled with regular measurements on effectiveness of information security efforts. For employees information security must be part of their daily work and organization should look for appropriate certification.

d). Sowa et al (2008) thought that information security management lacks alignment with overall enterprise objectives. Hence, they came up with – "Business ORiented management of Information Security" or "BORIS" [Sowa et al (2008)]. Their framework had following six requirements:

[8] British Standards Institute, BS 7799: Part 1: 1995, World Wide Web, Retrieved from http://shop.bsigroup.com/en/ProductDetail/?pid=000000000001324657 on August 05, 2010

- Linkage between enterprise and information security objectives [Sowa et al (2008)].
- Ability to provide metrics on information security along with capability to make key aspects better [Sowa et al (2008)].
- Support for precise and discernible information security measures [Sowa et al (2008)]
- Allow management to evaluate monetary side of information security [Sowa et al (2008)].
- Assessment approach for improving financial and tactical aspects of enterprise information security [Sowa et al (2008)].
- A methodology which could be used on a long term basis and geared towards overall enterprise goals [Sowa et al (2008)].

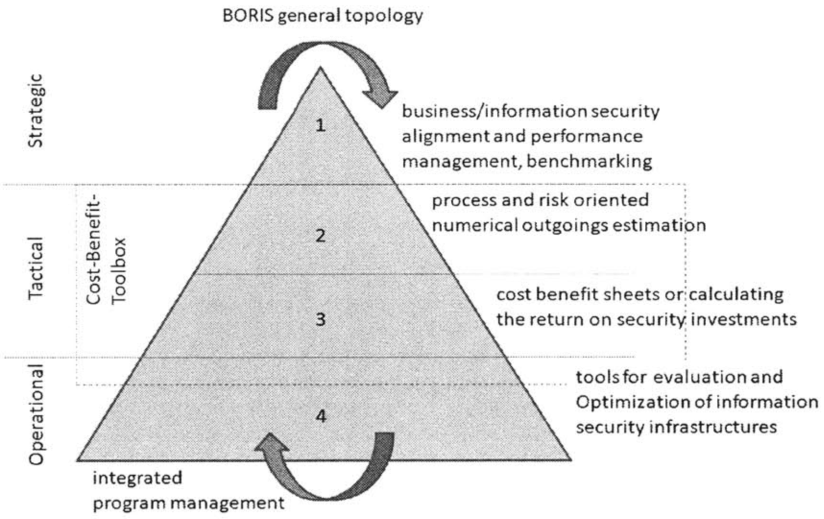

BORIS general topology
Strategic
Tactical
Operational
Cost-Benefit-Toolbox
1
2
3
4
business/information security alignment and performance management, benchmarking
process and risk oriented numerical outgoings estimation
cost benefit sheets or calculating the return on security investments
tools for evaluation and Optimization of information security infrastructures
integrated program management

Figure 9: BORIS General Topology ***(Source: Sowa et al (2008))***

The framework has four broad components as shown in Figure 9. Top component deals with overall enterprise strategy and its overlap with information security management. Second component is based on work done as part of top component. Clear information security goals are established with conformance to overall enterprise goals. Third component is about financial analysis of various information security investment options. Fourth component consists of various methods for evaluating information security investments. Component two, three and four are grouped together in a "Cost-Benefit-Toolbox" [Sowa et al (2008)]. Comprehensive "integrated program management" [Sowa et al (2008)] concludes the framework. Sowa et al (2008) goes on to explain each of the above components in detail.

In summary, BORIS brings information security management in alignment with overall enterprise objectives. It starts with enterprise objectives, followed by defining specific information security goals. Financial analysis is considered before an information security investment decision is taken.

This framework brings two characteristics that an enterprise information security management framework should have. These are: 1). Alignment with corporate goals and 2).Financial Analysis.

e). Tsoumas et al (2006) worked on an information security management framework which leveraged "security ontology (SO)" [Tsoumas et al (2006)] . This is a technological framework. They found that when information security goals are considered independent of technology side, it results in smooth information security management. Overall strategic goals were connected to implementable information security measures.

Tsoumas et al (2006) built upon DMTF Common Information Model (CIM)[9] and added security ontology -"an ontology that elaborates on the security aspects of an information system" [Tsoumas et al (2006)]. CIM was chosen because it can leverage Web Ontology Language - OWL. For building ontological relationships, standards such as "ISO-/IEC 17799, British Standard 7799 Part 2, Australian Standard Handbook of Information Security Risk Management (AS/NZS 4360), and CCTA Risk Analysis and Management Method (CRAMM) "[Tsoumas et al (2006)] were utilized.

Conceptual model of security ontology is explained next followed by explanation of the ontology based information security management framework. Figure 10 shows the conceptual model of security ontology. Tsoumas et al (2006) explains the diagram (i.e. Figure 10) as below:

- Key elements are: Asset, Stakeholder, Vulnerability, Countermeasure, and Threat [Tsoumas et al (2006)].

[9] Distributed Management Task Force, Inc.(DMTF), Common Information Model (CIM) Standards, Retrieved on August 06,2010 from http://www.dmtf.org/standards/cim/

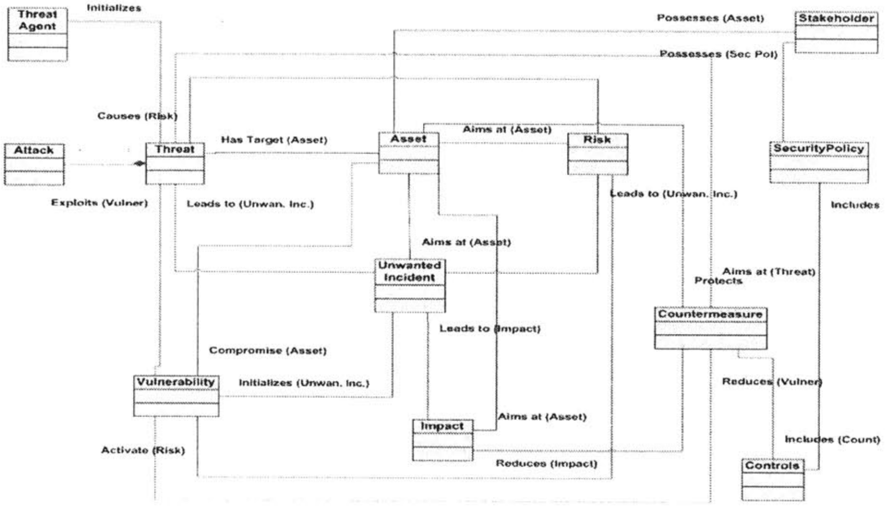


Figure 10: Conceptual model of Security Ontology *(Source: Tsoumas et al (2006))*

- Stakeholder is in some way responsible for Asset which could be harmed by a Threat which looks for Vulnerability in the asset [Tsoumas et al (2006)].
- Unwanted Incident i.e. information security breach occurs when an attacker succeeds in utilizing vulnerability to his/her advantage [Tsoumas et al (2006)].
- Unwanted Incident causes Impact on the organization [Tsoumas et al (2006)].
- Countermeasures help mitigate the Threat by employing Controls [Tsoumas et al (2006)].
- Controls are based on Security Policy developed by the Stakeholder [Tsoumas et al (2006)].

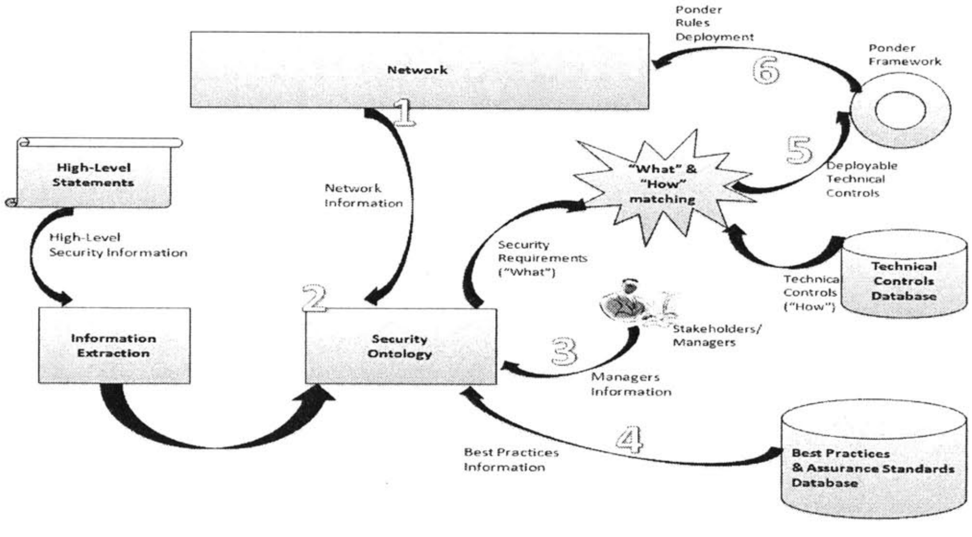

Ponder Rules Deployment
Ponder Framework
Network
6
1
5
High-Level Statements
Deployable Technical Controls
"What" & "How" matching
Network Information
High-Level Security Information
Security Requirements ("What")
Technical Controls ("How")
Technical Controls Database
2
Stakeholders/ Managers
Information Extraction
Security Ontology
3
Managers Information
4
Best Practices Information
Best Practices & Assurance Standards Database

Figure 11: An ontology-centric architecture for IS security management *(Source: Tsoumas et al (2006))*

Per Tsoumas et al (2006), their ontology based information security management framework consists of four different "phases" involving six "steps" as described below:-

- First phase comprising of first step is called –"Building of Security Ontology". This is information gathering phase which involves technological information regarding the existing IS infrastructure including anatomy of network, ports used by various servers, details of servers (for example: IP addresses, name, port etc.) , operational services, and network accessibility through VPN or wireless. In summary, a complete picture of existing information infrastructure is built from a technological standpoint. Next, enterprise goals are considered by involving management people. Finally, utilizing the technological information, "ontology concepts' instances" are created. Management input is implemented using programming interfaces. First step is shown in Figure 11 as "Network Information" [Tsoumas et al (2006)].

- Second phase-"Security Requirements Collection" consists of second, third and fourth steps. This involves going through information security documents such as "IS Policy document" and drawing out Information Security related information. This is shown in Figure 11 as "Information Extraction". Using the information gathered from various documents, complete the input gained from management in step one so that now we have complete –"Managers Information" as shown in Figure 11. Various information security needs gathered so far should be reviewed by technical and management personnel. Leverage the various information security standards and best practices. This is shown in Figure 11 as "Best Practices Information" [Tsoumas et al (2006)].

- Third phase –"Security Actions Definition" consists of a single step (step #5). This is essentially a mapping of what needs to be done to how things should get done. Security objectives developed so far are mapped to specific implementation methods. Methods are changed to "Ponder-compatible input" [Tsoumas et al (2006)]. [Note: *Refer Damianou N., et al (2001) for 'The Ponder Policy Specification Language"*]

- Fourth phase –"Security Actions Deployment and Monitoring" comprise of step #6. It involves implementing the "Ponder rules over the IS infrastructure". Finally, repeat all of the above on regular intervals. [Tsoumas et al (2006)]

In summary, this is a technological solution for enterprise information security management and it involves input from both technical and management people. However, it leaves out possibility of information breach without involving any technological failure.

Based on literature research in Enterprise Information Security Management domain, the author found below characteristics that are essential elements of a comprehensive Enterprise Information Security Management Framework:

- Employee training, clear communication, constant information security threat analysis, constant upgrade of security methods and policies.(Pishva et al , 2007)
- Compliance should be an integral part of enterprise information security management framework. (Zulhuda, 2009)
- An applicable standard should be followed at an enterprise level coupled with regular measurements on effectiveness of information security efforts. (Solms, 2000)
- Alignment with corporate goals and Financial Analysis are essential. (Sowa et al, 2008)

In the next chapter, the author presents an enterprise information security management framework based on literature research, numerous searches on the internet (i.e. the World Wide Web) and personal IT experience.

CHAPTER 3: Enterprise Information Security Management Framework

Modern businesses are catering to customers around the world 24 hours a day and 7 days a week via the internet. Companies heavily rely on their information systems for smooth business operations. Businesses are always looking for ways to minimize threats, protect intellectual property and maintain privacy of customers. Information security is an integral part of business activities and must be considered from a business as well as technical perspective. It is a key component of business processes. Enterprise Information Security Management Framework is based upon *information security driven business process development*. The idea is that information security should be forethought rather than an afterthought. Enterprise Information Security Management Framework is shown below.

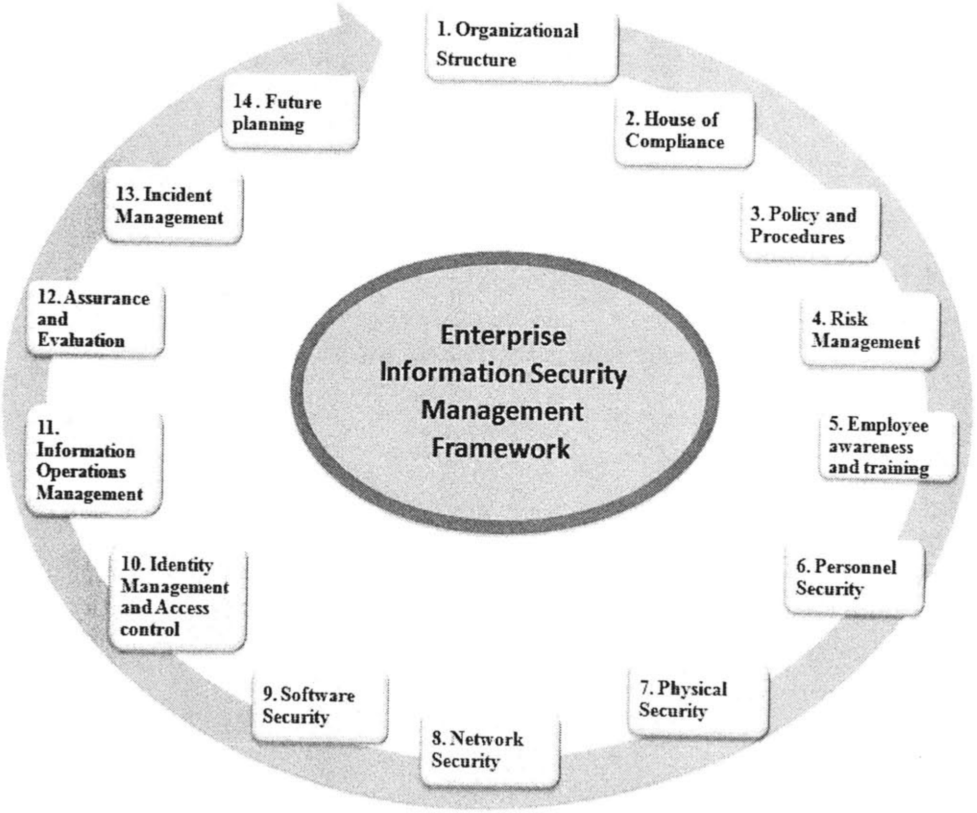

Enterprise Information Security Management Framework
1. Organizational Structure
2. House of Compliance
3. Policy and Procedures
4. Risk Management
5. Employee awareness and training
6. Personnel Security
7. Physical Security
8. Network Security
9. Software Security
10. Identity Management and Access control
11. Information Operations Management
12. Assurance and Evaluation
13. Incident Management
14. Future planning

Figure 12: Enterprise Information Security Management Framework [EISMF]

3.1 Organizational Structure

In constantly changing information threat landscape, it is important for an organization to have a dedicated high level person responsible for overall information security strategy, pro-active planning, and implementation of information security processes, training and tools. Depending on type of business and organization revenues, a company may choose between a full time or part time resource for overall information security management. With a top level (for example, C-level) person responsible for information security, management understands that information is a strategic challenge as well as a tactical challenge. Single person leadership for information security facilitates alignment of information security processes and tools across departments with overall objectives of an organization. Single dedicated person with a responsibility for the entire organization is more likely to think holistically i.e. at an enterprise level instead of approaching information security at a department level. It also helps different departments to leverage common resources instead of various departments taking a different approach to information security and therefore requiring unrelated tools/processes. In other words, we have economies of scale with single top leadership.

In year 2006, based on a survey involving 227[10] information security personnel from different companies located in North America with more than 1,000 employees, Enterprise Strategy Group (ESG)[10] found the following:

- 63%[10] of these companies had CISO (Chief Information Security Officer)[10].
- CISO generally reported to Chief Information Officer (CIO) [10].
- CISO have a broad understanding on all aspects of information security including both technology and managements aspects[10].
- Companies with CISO tend to allocate more funds towards information security. Of the companies who had a CISO, 23%[10] were planning to raise their information security budget in coming year. Whereas, companies with no CISO, only 8%[10] were considering increasing information security budget in the coming year[10].

[10] SC Magazine, Roundup 2006: Do CISOs matter?, Dated December 14, 2006, Retrieved on August 11,2010 from http://www.scmagazineus.com/roundup-2006-do-cisos-matter/article/34254/

- Of the companies with CISO, "50%"[10] were planning to manage information security at an enterprise level whereas "21%"[10] were considering managing it at a more granular level such as a department. "37%"[10] companies with no CISO were planning to manage information security at an enterprise level and "8%"[10] were considering department level approach [SC Magazine, Roundup 2006: Do CISOs matter?].

In a more recent research (for year 2009), Ponemon Institute[11] under sponsorship from PGP Corporation looked into 45 companies from 15 different industries which had a data breach[11]. It was found that cost incurred per breached data record was $157[11] when CISO (or a similar/equal role) was leading the data breach response effort. Whereas, cost incurred per breached data record was $236[11] when there was no CISO leading the breach response effort.

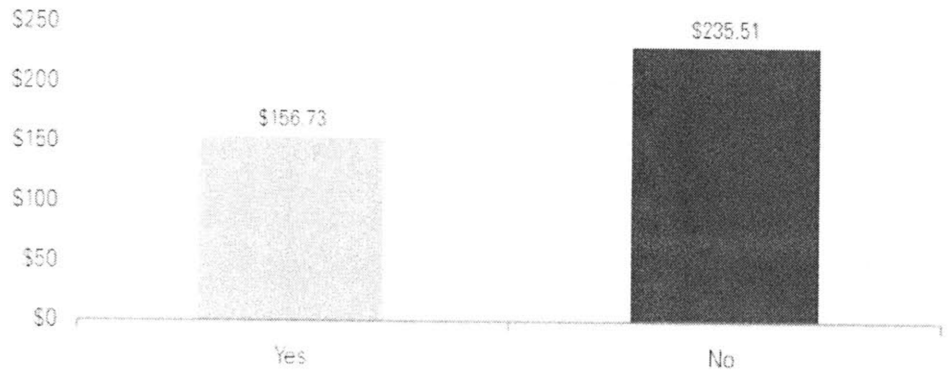


Figure 13: Cost incurred per breached record when CISO is involved-2009

(Source: Ponemon Institute[11])

In yet another recent report, Information Systems Audit and Control Association (ISACA)[12] reported "benefits of CISOs" based on research conducted by IT Policy Compliance Group

[11] Ponemon Institute, Fifth Annual US Cost of Data Breach, January 2010 - 2009 Annual Study: Cost of a Data Breach, Page 25, Retrieved on August 11, 2010 from http://www.ponemon.org/data-security

[12] Information Systems Audit and Control Association (ISACA), New Report Shows Benefits of CISOs, Retrieved on August 11, 2010 from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/New-Report-Shows-Benefits-of-CISOs.aspx

involving "809 organizations"[12]. This research found the following:

- Companies who have CISO or equivalent person get more return on their information related investment [ISACA]
- Improved ability to retain current customers/users [ISACA]
- Decreased information breach [ISACA]
- Better security of monetary information [ISACA]
- Reduction in yearly audit expense by half [ISACA]

From all of the above reports, it is clear that we can successfully leverage organizational structure for pro-actively managing and protecting information. Based on these reports, other literature research and personal IT experience, the author recommends organizations to have a full time CISO position. CISO should report directly to CIO/CTO as shown in Figure 14.

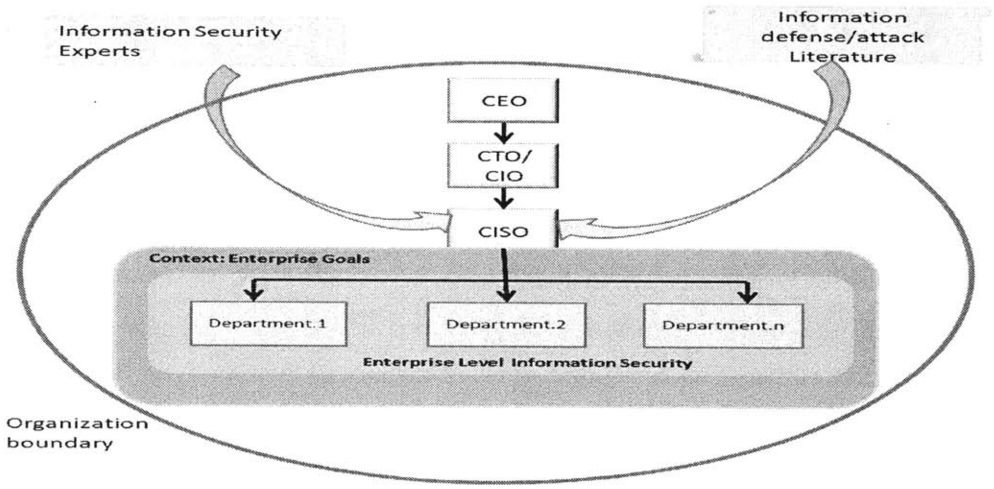

Information Security Experts
Information defense/attack Literature
CEO
CTO/ CIO
CISO
Context: Enterprise Goals
Department.1
Department.2
Department.n
Enterprise Level Information Security
Organization boundary

Figure 14: Organizational Structure - CISO

CISO should act as a "technological gatekeeper" [Allen, Thomas 2009]. In the context of our discussion we can think of CISO as an *information security gatekeeper*. Prof. Thomas J. Allen (MIT Sloan School and School of Engineering professor emeritus) describe "technological gatekeepers as a link to outside technology". The function of a "technological gatekeeper" is to bring knowledge into an organization from outside sources such as journals, books, other publications, meetings, seminars, conferences or through domain experts. CISO should leverage the latest available outside knowledge for information protection and management. This is critical for an organization because information threat landscape is constantly changing and CISO must be able to keep up with information on latest threats so that pro-active prevention steps can be undertaken. CISO should encourage *information security gatekeepers* across the enterprise. These people are extremely important from security perspective especially because numerous information security threats are born every day somewhere on the internet. Hence, enterprise information security goals are better met when CISO encourages more people within an organization to always on the look for latest and greatest events in information security domain and bring them to his or her attention.

In the author's framework, CISO or equivalent person is responsible for implementation of all of the remaining items namely: House of compliance, Policy and Procedures, Risk Management, Employee awareness and training, Personnel Security, Physical Security, Network Security, Software Security, Identity Management and Access control, Information Operations Management, Assurance and Evaluation, Incident Management and Future planning.

3.2 House of Compliance

Widespread global adoption of computers and the internet has led us into an information age where information has become a critical asset for any organization. Information can be shared fairly rapidly, even without proper authorization. This has led to privacy concerns and concerns regarding overall security of information. Organization started by developing their own best practices, which led to shared best practices across organizations through various industry standards. However, this was insufficient because organizations were not legally required to follow industry best practices and focus on information security. Due to heightened information security concerns in the public domain, information security became subject of legal discussion leading to several laws and regulations.

Author's *house of compliance* (Refer Figure 15) is a comprehensive list of information security related laws/regulations, standards, frameworks and best practices.

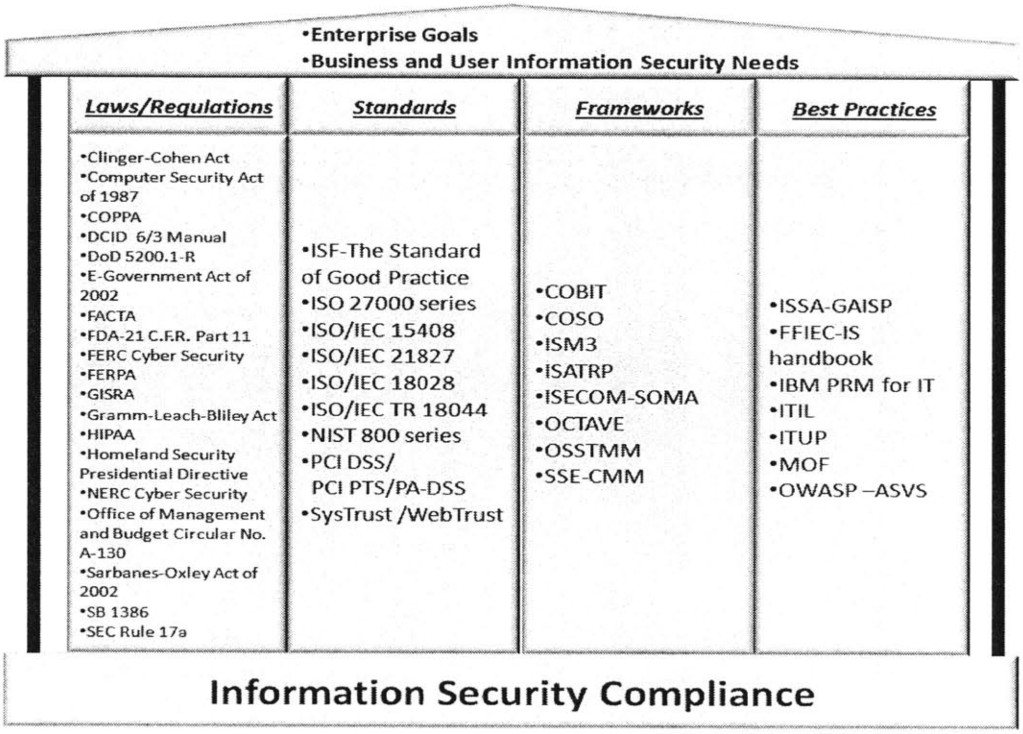


Figure 15: House of Compliance

(Refer abbreviations towards the beginning of this thesis document)

Organizations should abide by applicable laws/legislations and follow relevant standards, frameworks and best practices. Some of the benefits of following standards, frameworks and best practices are as follows:

- It is more reassuring for stakeholders when standards are followed coupled with proven frameworks and industry tested best practices
- Alignment of information security goals with overall enterprise goals.
- Increased level of information security awareness and coordination among employees thereby reinforcing overall information security.
- Improved quality of overall information security management
- Improved traceability and record keeping

Implementation of house of compliance should start with thorough understanding of enterprise goals followed by business and consumer information security needs. Applicable laws and regulations must then be identified. Next step is to determine relevant standards, frameworks and best practices. Implementation should be customized in such a way so that duplication of effort is prevented. In cases, where more than single law, standard, framework or best practice is applicable, stricter one should be followed. Idea is to give minimal needed authorization for access to information. No one should get more access to information than what a job requires.

In the author's framework, CISO or equivalent person is responsible for implementation house of compliance. Remainder of author's framework should be followed after conforming to house of compliance.

3.3 Policy and Procedures

Clear communication is a key element of successful business operation. To facilitate clear information security management, an enterprise information security policy document should be put in place and employees made familiar with its content.

Drivers:

Information security policy and procedures should be developed after a thorough analysis of the business domain and enterprise business strategy. CISO or equivalent person should develop a comprehensive list of information security concerns by studying business domain and specific business model which his or her organization uses. Depending on type of business, certain information security practices must be put in place which would go into information security policy document. An organization's own business strategy and their tolerance level towards certain information security concerns may influence policy document as well.

House of compliance is the next driver for information security policy and procedures. Certain laws and regulations require organizations to have an explicit information security policy document. Similarly certain standards may require such a policy as well. Applicable laws, regulations, standards and frameworks may provide guidelines as to what should go into an information security policy document.

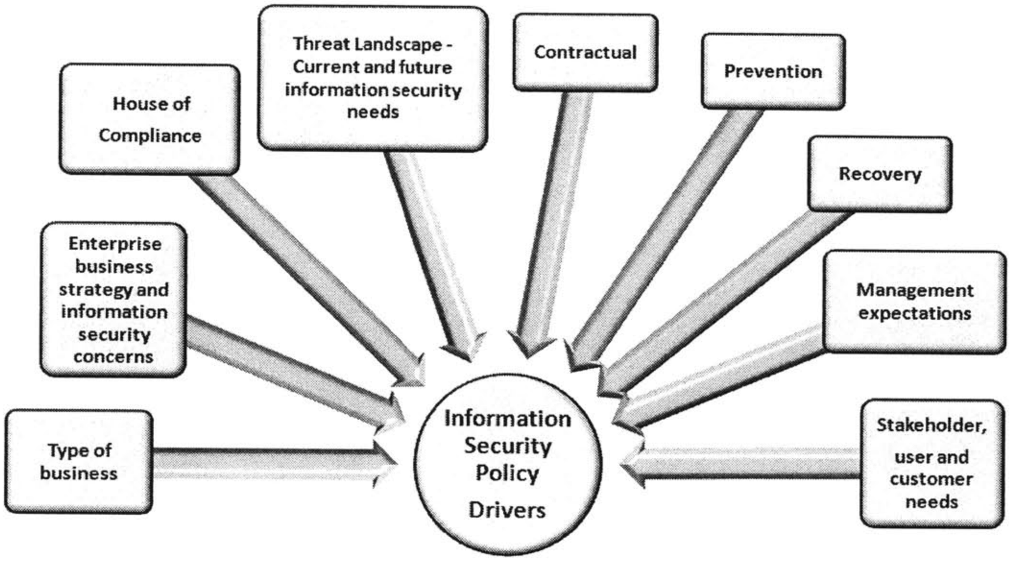

House of Compliance
Threat Landscape - Current and future information security needs
Contractual
Prevention
Recovery
Enterprise business strategy and information security concerns
Management expectations
Type of business
Information Security Policy Drivers
Stakeholder, user and customer needs

Figure 16: Enterprise Information Security Policy Drivers

CISO or equivalent person should develop a clear picture of current and emerging threats to information termed as information threat landscape [Refer Figure 17]. These include but not limited to physical attack, natural disaster, human error, denial of service, man in the middle, virus/malware, phishing, identity theft, social engineering, and cyber warfare. Some of the information threats may be of greater concern to an organization than others. Information security policy document must be written to address broad range of information threats. It covers a broad base. Enterprise information security policy document may refer a reader to other documents which cover specialized areas in greater depth.

There are contractual requirements and obligations which require an organization to take certain steps towards securing client information. These considerations drive need for information security policy and also the content of the document. A particular highlight of the policy document is prevention measures. Prevention is a key driver for the policy document because at an enterprise level it is helpful to make employees aware of certain key practices that can prevent potential damage. Similarly, steps that should be taken after an information security breach occurred are captured under recovery. Employees should plan ahead and take certain required steps to ensure recovery as well as facilitate forensics.

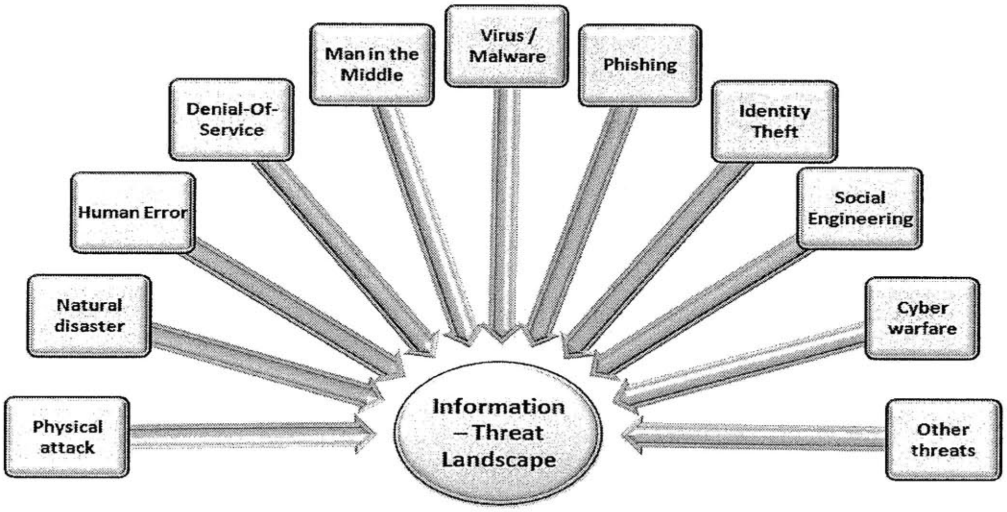


Figure 17: Information Threat Landscape

Management expectations are a key driver for the policy document because through the help of one all encompassing document, they are able to convey their stand and preferences to all readers as well as show organizational commitment towards information security.

Finally, stakeholders, users and customers may want to ensure that their information is secured. This document proves that organizations understand information security concerns and have planned ahead for prevention and recovery measures.

Policy Content:

Policy must contain policy statement and scope. It should cover the physical as well as logical information security requirements, discussion on how frequently backups should be taken, precautions when setting up a new system or infrastructure resource, maintenance frequency, information system upgrade, retirement and replacement guidelines, required and recommended password strength, frequency of information security patch, comprehensive risk assessment, moral and ethical guidelines for employees, communication requirements in case of security breach (who needs to be informed, when and how), acceptable use of internet, email, instant messaging software, caution on downloading information from the internet, consequences of information security policy violation, and policy revision timeline (monthly/quarterly/semi-annually/annually). Information security policy document must be updated periodically and employees need to be informed whenever an update is made.

Following sources of information can be taken for writing information security policy *(based on drivers)*:

- Review of type of business, enterprise business strategy and information security concerns.
- Review of current and future security requirements
- Review of applicable laws, regulation, standards, frameworks and best practices (i.e. house of compliance)
- Review of contractual requirements and obligations
- Review of prevention and mitigation strategy. It could be department specific before a policy at enterprise level is put in place.
- Review of existing / planned recovery procedures
- Understanding of management expectations
- Interviewing stakeholders, users and customers (where possible) and taking their concerns into account
- Review of any existing information security policy or documentation

Procedures:

This covers a wide range of activities. Some of the procedural activities are as follows:

- Regular backups for all information stores (electronic storage or otherwise)
- Regular testing of recovery steps including testing of recovery from information storage devices such as tapes or external hard drives.
- Internal and external communication in case of security breach
- Setting up a contact channel for reporting security breach such as email, phone or online form
- Information security considerations when buying new products or services

- Disposal methods of electronic or other devices including disposal of devices such as hard drives or tapes
- Security coverage of common printer, photocopier, scanner or fax area
- Blocking access to certain types of websites, monitoring incoming or outgoing electronic messages such via email, scanning downloads as well as email attachments for potential threats
- Recurring procedure review and updates
- Employee awareness when procedures are updated

3.4 Risk Management

There are a broad range of definitions available for risk management. One such definition from National Institute of Standards and Technology (NIST) is as follows:

"Risk Management is the total process of identifying, controlling, and mitigating information system–related risks. It includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws." [NIST Special Publication 800-30, p54]

Similar to risk management, there are a broad range of definitions available for risk assessment which differ in approach (qualitative versus quantitative) and scope. Estimation of risks to information assets and ways to mitigate them remain the ultimate objective irrespective of any approach taken. Below is one such definition for risk assessment from National Institute of Standards and Technology (NIST):

"Risk assessment is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact." [NIST Special Publication 800-30, p54]

Numerous processes are available to help organizations with risk management. Below is a generic process which has steps commonly found in most processes. However, author's risk management process stresses a holistic picture with clear understanding of the context and house of compliance.

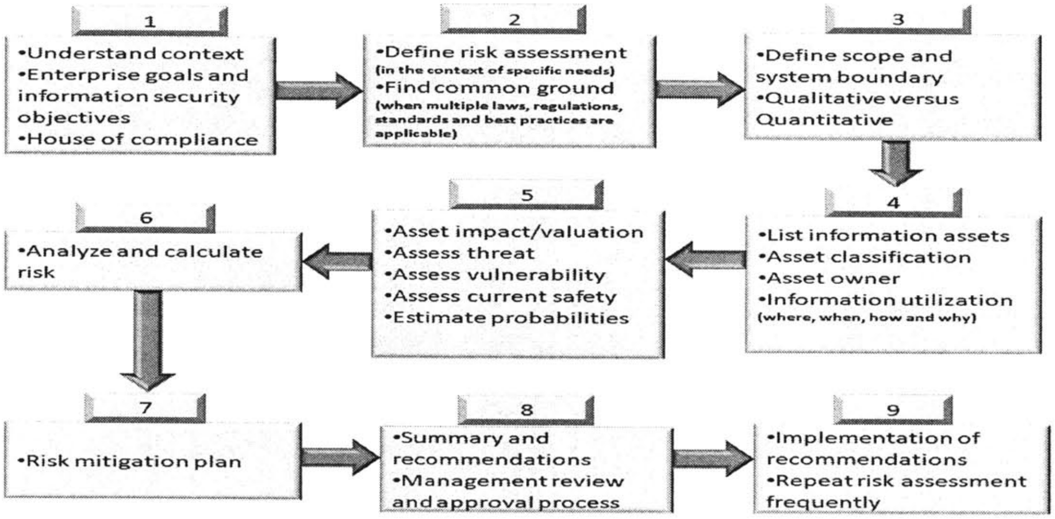

1
•Understand context
•Enterprise goals and information security objectives
•House of compliance
2
•Define risk assessment
(in the context of specific needs)
•Find common ground
(when multiple laws, regulations, standards and best practices are applicable)
3
•Define scope and system boundary
•Qualitative versus Quantitative
4
•List information assets
•Asset classification
•Asset owner
•Information utilization
(where, when, how and why)
5
•Asset impact/valuation
•Assess threat
•Assess vulnerability
•Assess current safety
•Estimate probabilities
6
•Analyze and calculate risk
7
•Risk mitigation plan
8
•Summary and recommendations
•Management review and approval process
9
•Implementation of recommendations
•Repeat risk assessment frequently

Figure 18: Generic Information Security Risk Management Process

- *Step 1:*

First step towards a holistic risk management is to understand the overall context which includes enterprise and information security management objectives. Any process which we put in place to facilitate information security management must be aligned towards corporate goals. Different laws, regulations, frameworks and best practices may already have a risk assessment process. When complying with any of them, it is important to understand appropriate applicable risk management process before selecting an approach.

- *Step 2:*

Once we have a holistic picture, we need to drill down to writing our own or selecting an appropriate definition of risk assessment. This definition would bring a common understanding among all stakeholders and would go into employee training program. As discussed earlier, different laws, regulations, frameworks and best practices may already have a risk assessment process. It would be cost and effort saving exercise to come up with common risk assessment steps/phases. Once, we have common steps, additional customized steps/phases could be added to meet specific business needs.

- *Step 3:*

Similar to any other project plan, clearly defined scope would help set the stakeholder expectations. Risk assessment could be carried out at an enterprise level or at department, division, regional or business unit level. Hence, system boundary is another area which should be agreed upon with stakeholders. Another important decision is whether to follow quantitative or qualitative approach.

Strengths of quantitative approach include easy to understand formulation, easy to justify/explain, useful for cost benefit analysis, useful for budgeting or any other statistical analysis. Weaknesses include significant work effort in determining probabilities, difficulty in convincing some managers, and possibility of a significant error in estimating probabilities leading to unreliable result. [Landoll, 2006]

Qualitative approach involves subjective assessment of security risks to information assets using terminology such as *most likely-likely- unlikely* or *high-medium-low.* Advantages include, easy implementation, relatively easy to get needed data, and most managers can easily understand both approach as well as results. Disadvantages include inability to convince managers who believe in absolute numbers, and challenges around estimating progress. For example, due to risk mitigation effort, risk is reduced from *most likely* to *likely.* This improvement is questionable and difficult to convince mangers of accuracy about the approach and results. [Landoll, 2006]

- *Step 4:*

Within system boundary a comprehensive list of information assets should be prepared. Organizations may choose to classify information assets into categories or levels which could be project specific. Asset owners should be identified. Through discussion or documentation, more details needs to be ascertained such as information asset description, and *where, when, how* and *why* information asset is used.

- *Step 5:*

After we have a good understanding of an information asset, we need to determine value of asset from organization's perspective. Any potential threats needs to be assessed and vulnerability needs to be determined. Many organizations already have safeguards in place for certain assets. Comprehensive understanding of current safeguards helps in assessing probability of information compromise. After understanding current safety, probability of successful attack could be estimated.

- *Step 6:*

Analysis of information gathered should be conducted next. Using previously agreed qualitative or quantitative approach, risk calculations, discussions and observations should be made.

- *Step 7:*

After estimating risk associated with different assets, a risk mitigation plan should be put in place. This is dependent on how much risk an organization is willing to take for different assets as well as budget and schedule (i.e. time needed to put safeguards in place). Plan should focus on safeguards involving people, processes or technology. People safeguard may include complete background check of personnel, and continuous upgrade of technical skills as well as general awareness of staff. Process safeguard may include better documentation, implementation of well known and established standards, frameworks, and best practices. Technology safeguard may include using latest information security products and services such as better user authentication and authorization products which include logging every activity of a user in software electronic transaction. For budget, cost benefit analysis must be done for selecting an appropriate cost effective safeguard.

- *Step 8:*

Finally, an executive summary should be created highlighting areas which needs management attention. Management usually prefers graphical presentation with concise statements describing the approach, observations and results coupled with suggested solution. Summary and recommendations should be sent for management review through CISO or equivalent person.

- *Step 9:*

After management's approval, recommendations should be implemented. Risks should be assessed frequently depending on the type of business, overall business goals and information security objectives.

3.5 Employee awareness and training

Employee training and awareness is just as critical as putting any technological information threat protection solution in place such as computer software or hardware. There are numerous ways through which employees can give away information either knowingly or unknowingly. Employees must be made aware on a regular basis about the enterprise information security policy, common knowledge procedures (for example, informing promptly whenever some suspicious activity is observed) and what Rothke (2005) calls, "20 things that every employee should know"[13] and these include the following:

"Beware of phishing and spyware, Protect your identity, Be responsible and be aware, Choose your password wisely, Practice safe access, Protect your work outside the office, Reduce email risks, Suspect e-mail hoaxes, Work wisely with the web, Avoid internet dangers, Master instant messaging, Use firewalls and patches, Use PDAs safely, Backup and secure data, Manage data wisely, Secure your workspace, Beware of social engineers, Use corporate resources only for work, Call the experts when things go wrong, Keep things in context" (Rothke (2005)).

In addition, employees should be made aware of threats from portable information storage devices such as external hard drives. Employees should understand internet browser privacy settings.

There are several excellent resources available to help organizations get started with a formal employee awareness and training program. For example, NIST Special Publication 800-16 –"Information Technology Security Training Requirements: A Role- and Performance-Based Model" and NIST Special Publication 800-50- "Building an Information Technology Security

[13] Rothke, Ben (2005), Computer Security: 20 Things Every Employee Should Know (Paperback), McGraw-Hill Professional Education (ISBN-10: 0072262826, ISBN-13: 978-0072262827)

Awareness and Training Program" are two excellent resources. These standards stress that learning is a three stage continuous process. In the first stage is "awareness" which is applicable to everyone in an organization. Next stage is "training" which is more restricted to people responsible for information systems. Final stage is "education" where formal education in specialized area is more relevant (Refer Figure 19).

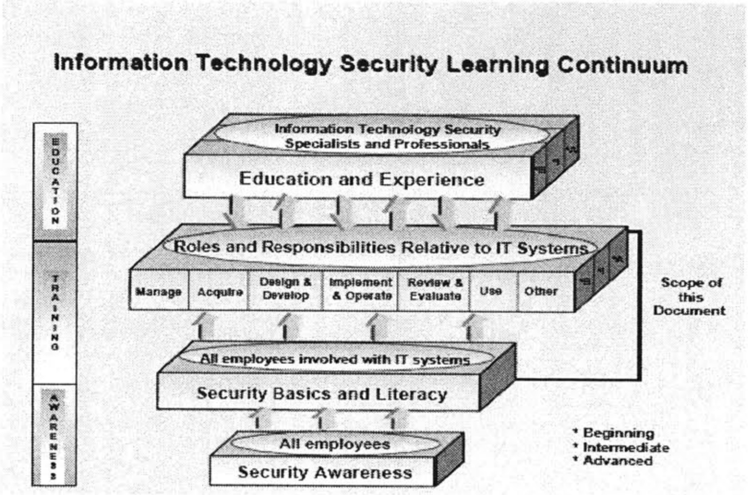

Information Technology Security Learning Continuum
EDUCATION
TRAINING
AWARENESS
Information Technology Security Specialists and Professionals
Education and Experience
Roles and Responsibilities Relative to IT Systems
Manage
Acquire
Design & Develop
Implement & Operate
Review & Evaluate
Use
Other
Scope of this Document
All employees involved with IT systems
Security Basics and Literacy
All employees
Security Awareness
* Beginning
* Intermediate
* Advanced

Figure 19: Information Technology Security Learning Continuum

(Source: NIST Special Publication 800-16, p22)

Employees who are directly responsible for maintaining information systems should be trained in *house of compliance* so that they fully understand the legal aspect of their job responsibility in addition to standards, frameworks and best practices.

In summary, employee awareness and training is utmost important for overall information security in an organization. There are several structured approaches available which an organization can leverage to implement a comprehensive information security awareness and training program.

3.6 Personnel Security

According to the Washington Post article titled "Data Theft Common By Departing Employees" [14] dated February 26, 2009, Ponemon Institute reported that more than half (nearly 60%) of employees who are let go or quit on their own are involved in information theft. Of these, 79%[14] were aware that they are not authorized to take organizational information with them when leaving. This brings an important aspect of information security management. Training and awareness may not be sufficient to prevent information security breach. Organization must take extra measures to facilitate information security. This brings us to – Personnel Security.

Below is a checklist which organizations could customize for their own specific needs:

- Use of identification methods such as identity cards, retina scan, numeric lock and key etc.
- Perform a complete background check before hiring. This includes full/part time employees, contractors and other temporary workers. Essentially, anyone who works for an organization irrespective of the duration should be checked.
- Appropriate system access to all employees and contractors at all times. No one should have access to system, resource or facility which he or she does not need.
- Electronic surveillance of facility
- Internal and external audits for all system access
- Individual physical, mental and psychological assessment must be made prior to hiring. This may be more applicable to high stress jobs such as military personnel in a war zone.
- Individuals must be required to report any change to their security clearance level or any constraint which limit them to perform the job.
- For information systems such as computer hardware and software, monitoring should include logging and complete traceability of who accessed the system, when and what was done.
- Employee/contractors must be made aware of the consequences of information theft.
- Employees should be asked to report any suspicious activities. Peer vigilance is critical.

[14] Washington Post, "Data Theft Common By Departing Employees", World Wide Web, Retrieved on June 26, 2010 from http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html

However, organizations should note that other laws and regulations such as individual privacy laws might be applicable here because organizations cannot carry out background checks on an individual for employment reasons without prior written consent of the applicant.

3.7 Physical Security

Physical security is a critical component of over all information security. If physical security is compromised, everything else falls apart really quickly. For example, if an intruder physically gets into a computer server room and simply disconnects a server from its power supply, it has the potential to bring down customer facing internet website or bring down several critical software applications. There are several sources of physical threats. Physical threat can come from nature. For example, earthquake, lightening, flood, storms etc. Physical threat can come from human side in the form of theft, actual physical attack, vandalism, mistakes etc. Other sources of physical threat could be structural failure due to old infrastructure, power outage etc. Figure 20 (on next page) shows the physical threats to Information assets.

Companies can save a great deal of effort by implementing physical security such as outlined below:

Protection against natural disaster:

Companies can make careful building/office area selection by selecting areas with less probability of natural disasters. Office buildings can be built with some earthquake resistance. Office space elevation could be higher than surrounding to protect against floods. Lightening conductors can be installed on building for grounding lightening. Buildings can be constructed in such a way as to have dedicated area within buildings for protection against hurricane. As is clear, management must make decisions for protection against natural disaster very early on. Its significance could vary based on type of business and type of work which is planned for the new facility.

Controls for human factors:

Controls include badge and identity cards, alarms, video monitoring and motion sensors, biometrics, barriers and doors, door locks, fencing, fortification, physical security personnel, proper lighting within and outside buildings. Note that video monitoring is not sufficient by itself as it requires security personnel to keep an eye on the monitors. There are smart software based video monitoring solutions available now-a-days that can analyze real time video and alert security personnel when a suspicious activity is happening. Physical access to all information devices such as routers and other network devices, physical servers etc. should be restricted.

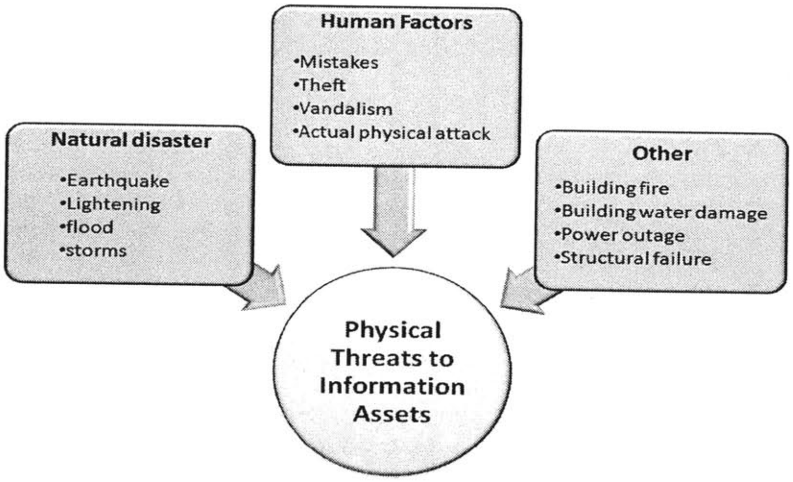


Figure 20: Physical Threats to Information Assets

Protection against other threats:

Management needs to put a comprehensive plan for building or facility specific threats such as building fire, water system damage, power outage due to internal/external reasons, and building maintenance.

It may be helpful for organizations to have documented plan for protection against natural, physical or other threats. A checklist containing areas which should be inspected frequently should be maintained by staff responsible for overall physical security and shared with department heads and employees. Employees should be encouraged to report any suspicious activity anywhere inside or in the immediate vicinity of the office space.

3.8 Network Security

Computer network is the backbone of information in most enterprises these days. CISO or equivalent should put special policy in place or create a clear section in the enterprise information security policy giving details of different roles and responsibilities of different network security personnel. For external suppliers, vendors and contractors who need access to the network, a special agreement must be put in place so that all the parties involved clearly understand their roles, responsibilities and repercussions. Make sure that network administrator is well trained and caught up with the latest in network security threats and protection.

Once we have policy in place, a detailed analysis of existing network or planning for a new network must be done. This should help in taking appropriate protection measure at different point in the network. Below could be used as a checklist:

- Access to all physical network devices such as routers and switches must be secured. Only a limited number of persons should have access to secured area where network devices are physically located. Physically securing the network devices lays down the foundation for network security.
- Software patches must be applied regularly as recommended by their vendors.
- Passwords for all network devices must be managed with utmost care. High strength passwords must be used. Network administrators should be aware or made aware of the best practices in password management. Generally high strength password is a mix of uppercase and lowercase letters along with numbers and other characters, and more than 8 characters long. Administrators or other network personnel should never write down a password and never share it with other co-workers.
- All system default passwords must be changed to strong passwords with periodic password change
- Some organizations may allow their employees ability to access network devices from a remote place such as employee home. Remote access to a critical infrastructure such as network device must be authorized for a very limited number of persons only.
- Legal notice must be put upfront when logged into a network resource clearly stating that unauthorized access is not allowed and any such access would be investigated to the fullest extent.
- Administrators should set a timeout for a given session. For example, when there is no activity during a session for more than 5 minutes that session should automatically close.
- If any service is not needed, it should be stopped. Nothing should be running on any device which is not required.

- No electronic communication should occur in clear text. All electronic communication must be encrypted. Keys to encryption algorithm must be changed regularly just as we change passwords and key must be stored in a secure place.
- Access to network devices should be logged (both successful and unsuccessful attempts to login) so that organization knows who accessed it a particular device, when was it accessed, and what was done.
- Network security is an area where management can take professional expert help by using the services of well established companies in this area.
- Network can be segmented into logical sub-networks as per business needs.
- Continuous system monitoring and maintenance of audit trails.
- User (employee/contractor) education plays a vital role in network security

3.9 Software Security

Software security is another critical component of effective enterprise information security management. Software security must be a planned forethought rather than an afterthought. Software development life cycle popularly known as SDLC usually consists of following steps:

- *Requirements gathering:* Includes meeting with sponsor department or organization and capturing their needs in plain English. This is mostly done by project managers who may or may not be technical.

- *Analysis:* Usually done by experienced technical professionals who perform requirement analysis. They may go back to project manager to ask for revisions from the project sponsors. Requirements are frozen after the analysis phase so that technical design could be done. Sometimes technical professionals may create a quick prototype for proof of concept.

- *Design:* Usually done by same experienced professionals who did the analysis. This step involves selecting appropriate programming language, database, and other software/hardware. This is followed by detailed architecture diagram to show how everything functions individually and together. Use cases are drawn to show the functioning of individual components. Sometimes, pseudo code is written describing programming logic in plain English. Pseudo code is meant for programmers and not for machine interpretation.

- *Development:* This step is mostly done by programmers who are familiar or well versed with a certain programming language or technology. It usually consists of actual coding, database creation etc. At the end of this step, we have a fully functional product ready for testing.

- *Testing:* This step is usually conducted by a team of testers who were not involved with coding the software product. This allows an independent look into the functionality provided by product under development. Usually, testers independently look into the requirements, analysis and design documents and come up with test cases. When bugs are found, they are reported to the development team that fixes them and submits the functionality for retesting.

- *Implementation:* This step consists of delivering the product to its intended users. Management plays a key role in estimating when product should be released.

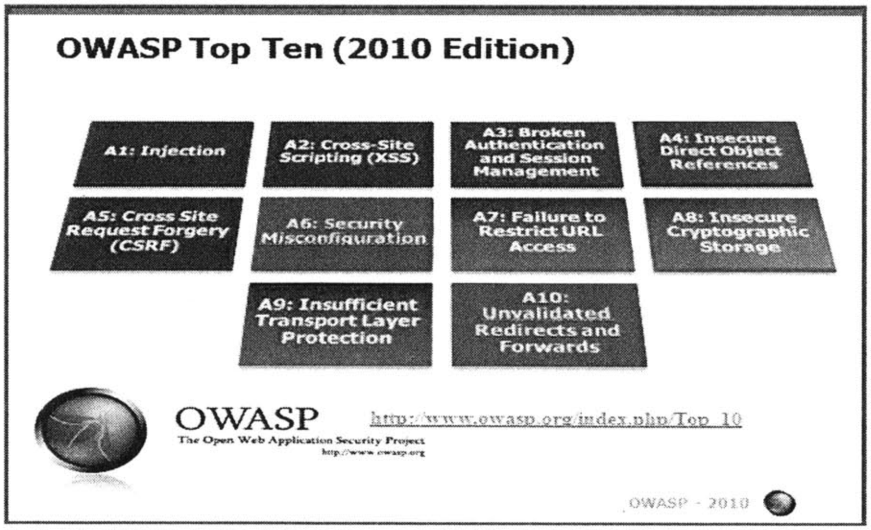
- *Maintenance:* A team is maintained for supporting a software product. This team fixes any bugs that may come up. New enhancements that users may need are also developed by the maintenance team.

As we saw above, in common practice software security is not emphasized in software development life cycle. We need software applications to have built in appropriate level of security. In real life, documented business functionality takes precedence over non documented security needs. In order to build secure software applications, we need to modify software development life cycle so that security needs are considered at every stage.

There are many business benefits of incorporating security into software development life cycle which includes cost benefits and brand value retention. Cost of retrofitting security into software because of reported bugs either at testing stage or after implementation would be significantly higher as compared to building security into software application right from the user requirements stage. In addition, reported application security breach can cause big damage to an organization which may affect sale of other products as well. OWASP very nicely puts it as follows:

"If security vulnerabilities built into your applications' source code survive into production, they can become corporate liabilities with broad and severe business impact on your organization. In view of the consequences of exploited security vulnerabilities, there is no reasonable alternative to using best practices of application security as early as possible in — and throughout — your software development lifecycle."[15]

Protecting the network by putting firewalls, deploying intrusion detection and protection systems, using latest anti-virus software etc. may not be sufficient to prevent information security breach because hackers may exploit vulnerabilities in the software application itself. OWASP in its 2010 edition came up with top 10 software web applications vulnerabilities as shown in the Figure 21.



OWASP Top Ten (2010 Edition)

A1: Injection

A2: Cross-Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Failure to Restrict URL Access

A8: Insecure Cryptographic Storage

A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

OWASP - 2010

Figure 21: Top 10 Software Vulnerabilities *(Source: OWASP)*

[15] Open Web Application Security Project (OWASP), CLASP Best Practice, World Wide Web, Retrieved on August 18, 2010 from http://www.owasp.org/index.php/Category:CLASP_Best_Practice

As discussed earlier, software vulnerabilities such as shown in Figure 21 must be handled in the code when writing software. Hence, we should look into modifying our software development life cycle to incorporate security considerations at various stages. One such modified software development life cycle is shown in Figure 22.

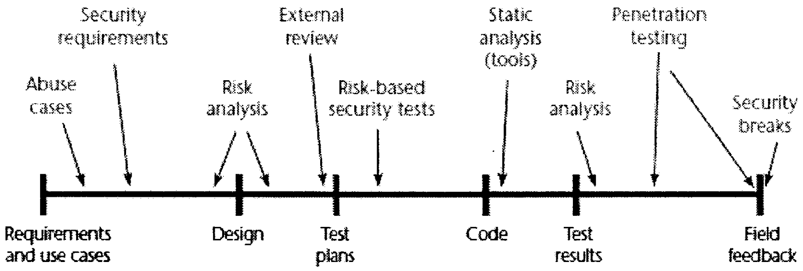


Figure 22: SDLC with security considerations ***(Source: McGraw, 2004)***

"Software security best practices applied to various software artifacts. Although the artifacts are laid out according to a traditional waterfall model in this illustration, most organizations follow an iterative approach today, which means that best practices will be cycled through more than once as the software evolves." *(Source: McGraw, 2004)*

In summary, organizations can modify their own custom SDLC to incorporate software application security at every stage. It is imperative that software security should be considered as seriously as personnel, network , or physical security. CISO or equivalent person can highlight this in the enterprise information security policy document. As discussed earlier, considering software security requirements at an early stage in the development cycle would bring monetary as well as non-monetary benefits to the organization.

3.10 Identity Management and Access control

Identity management and access control have been implemented in some form or the other since the beginning of computing. It deals with establishing the identity of a person or process trying to access a secured resource (for example, file system, database, email account etc.). Once a person or process is successfully identified, system needs to determine what authenticated user can do within the system. This is called access control or authorization. For example, a user X has "read" only access to a database server whereas user Y has CRUD (Create, Read, Update and Delete) privileges. When user X successfully authenticates to the database system and tries to delete data, user X will get permission denied message. On the other hand, when user Y tries to delete data after successful authentication, he or she would be able to do so.

There are several solutions available in the market which companies can use to meet their needs. CISO or equivalent person should come up with objectives and deliverables for identity management and access control based on business drivers. Key components of identity management and access control are shown in Figure 23.

- *User information repository*:

It is useful to have a centralized data store for storing user profile information such as name, address, designation, contact phone numbers etc. and authentication information which in most cases is password information. Additionally, access control information such as roles, permissions, and access control lists could be centrally stored as well. Choice of data stores may include but not limited to relational, object or LDAP (Lightweight Directory Access Protocol) stores.

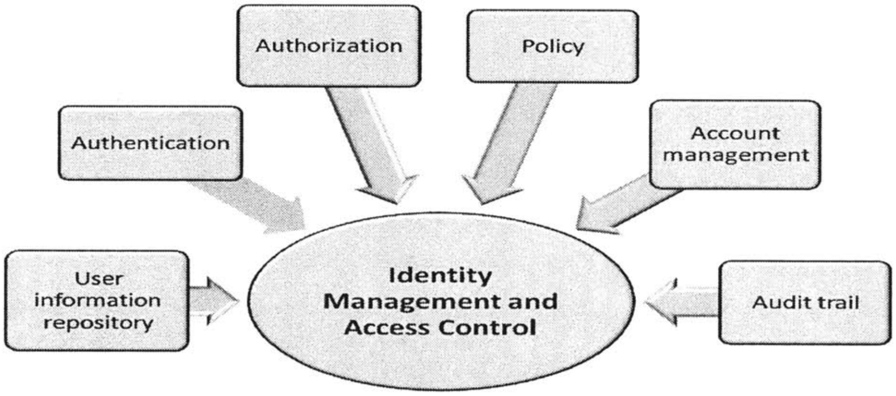

Authorization
Policy
Authentication
Account management
User information repository
Identity Management and Access Control
Audit trail

Figure 23: Key components of identity management and access control

- *Authentication*:

There are several authentication methods available such as username/password, biometrics, personal identification number, smart cards, digital certificates, and digital signatures. Depending on user needs, available user interface options and overall business drivers, company can decide on authentication method. One or more authentication method could be used. Widely used authentication protocols include Secure Socket Layer (SSL) which is a secure method for communicating over TCP (Transmission Control Protocol) connections especially HTTP (Hyper Text Transfer Protocol) connections. IP Sec is another authentication protocol. It secures the Internet Protocol (IP) communications by making use of cryptographic security services. Secure Shell (SSH) is an authentication protocol proving remote login in a secure way. Kerberos developed at Massachusetts Institute of Technology is yet another authentication protocol. Kerberos is used for verifying the user identity. There are products available in the market for single sign-on (SSO) which allows users to provide credentials (such as username/password) one time only and save user effort in signing on multiple times.

- *Authorization*:

Authorization is what user can do after successful authentication. Within an application user may be able to do (update / delete) or see (read) certain things. For example, user may be able to view certain information and not able to edit it. Role Based Access Control (RBAC) is a common authorization model. Enterprise wide application based roles could be created and appropriate users can be assigned to those roles.

- *Policy*:

Businesses can follow a policy of *least privilege.* The idea is to give access to secured resources to those who need it to fulfill their job needs and no more.

- *Account management*:

It is useful to have a single user interface to manage requests for new accounts, account changes and account removals. Depending on business needs, account management system can be real time or batch process based.

- *Audit trail*:

For compliance needs as well as for non-repudiation, all user activities must be logged in a database or file system and audit trail should be maintained for certain number of years depending on legal requirements.

3.11 Information Operations Management

Due to rapid change in technologies these days, organizations that can leverage these technologies to meet enterprise business needs would flourish. Information security personnel must keep up with the fast pace of ever evolving threat and protection technologies. Organizations should have a flexible design in order to effectively bring in latest information security technologies and retire the existing ones. Key components of a flexible information operations management include asset acquisition and inventory management, change management, backup and recovery, asset retirement and disposal as shown in Figure 24.

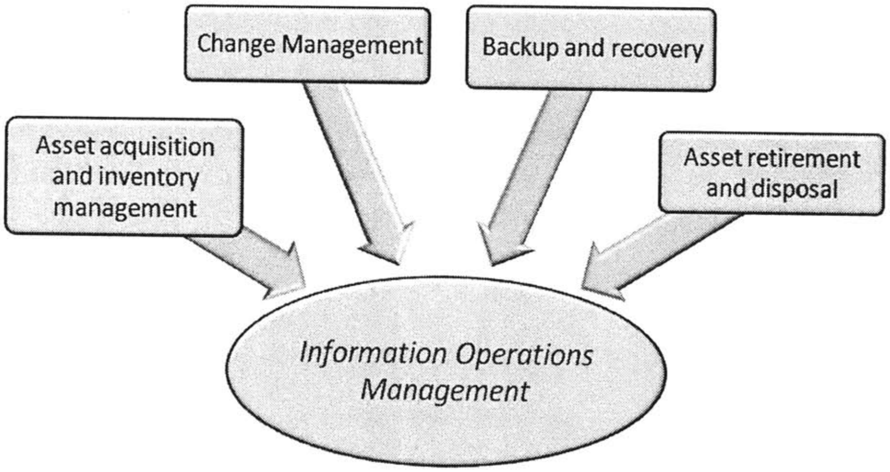

Change Management
Backup and recovery
Asset acquisition and inventory management
Asset retirement and disposal
Information Operations Management

Figure 24: Key components of information operations management

Asset acquisition and inventory management:

An organization should keep a centralized repository of all information assets and license information. Most software applications come with authorized number of users or per user license basis. Sometimes software can be purchased on a *floating license* basis which allows multiple users to share use of an application. A list of preferred software vendors can be maintained and updated on a regular basis.

Change Management:

A clear change management methodology should be implemented. Roles and responsibilities of persons performing the change management should be clearly defined. Separation of software application environments (For example, development, test and production) should be made so as to minimize impact on an unrelated software application. Failover and rollback procedures should be planned ahead. Review process should be put in place for accepting any system upgrades.

Backup and recovery:

Regular backups of data (especially production data) should be made. A process (preferably automatic) can be put in place to test the quality of backups. Sometimes in case of a failure, recovery data may not work. For example, data backup may be taken on a tape. But tape may not work at the time of recovery. It is important to verify that backups work. Recovery procedures should be planned ahead for each and every software application.

Asset retirement and disposal:

All form of information stores (tapes, hard drives, CDs etc.) should be disposed of in a safe way. NIST Special Publication 800-88 ("Guidelines for Media Sanitation") explains the roles and responsibilities of persons involved, decision making process and sanitization techniques. However, the organization may come up with their custom techniques for data storage disposal.

3.12 Assurance and Evaluation

From an information security perspective, *assurance* deals with checking whether information system would work in a secure way by calculating probability of information security breach in the system. Organizations may set an assurance goal based on their enterprise information security objectives. On the other hand, *evaluation* is the process of establishing (through documentary or technological methodology) whether an information system meets information security assurance goals set by an organization.

Assurance:

Depending on type of business, this can be either a continuous process or a one-time effort. There are few options available for assurance.

- First one is rigorous testing. A series of security testing can be performed which can check for implementation flaws such as buffer overflow, SQL injection, command injection etc. Testers have choice to either conduct a white box testing or black box testing. White box test cases are written after thoroughly reviewing all available product documentation as well as the software program source code (for software testing). Black box test cases are written without going through any product documentation or software program source code (for software testing).
- Second approach is the review of implemented architecture. The architecture review can bring forth possible flaws by critically looking at all available options that laid the design foundation.
- Third option is to review the team and individual programmers who coded the software application.
- Finally, there are some standards that can help bring process improvement. For example, ISO/IEC 15408 is a helpful standard for organizations to consider when considering implementing information security assurance and evaluation. CMMI (Capability Maturity Model Integration) covers product and service development, service establishment, management, and delivery, and product and service acquisition. ISO 9001 is another standard which emphasizes proper documentation of complete software development lifecycle (SDLC).

Reliability based calculations are becoming important part of assurance process. Anderson (2008) mentions that Poisson distribution is a great approximation for coming up with a probabilistic estimate that a problem with code is not caught after certain number of tests as shown below:

$$p = e^{-\lambda t} \qquad \text{[Anderson (2008)]}$$

where, p = probability that problem with code is NOT caught

t = number of tests.

λ = depends on feasible test data sets for conducting tests

As mentioned earlier, organization may set a target for acceptable assurance.

Evaluation:

Key driver for evaluation is to build confidence among stakeholders that product does meet minimum acceptable assurance criteria. ISO/IEC 15408 is a helpful standard for organizations to consider when considering information security assurance and evaluation implementation. ISO/IEC 15408 does not cover areas which require certain specific skills or not closely related to computer security. Various countries may have their own evaluation standard as well. Organizations should select appropriate applicable standard.

In summary, there are many assurance and evaluation methods that organizations can leverage. However, effort should be made to avoid making every process overly bureaucratic. Organizations would gradually learn which processes are more suited to their particular environment and culture. This would lead to eventual benefit from assurance and evaluation standards.

3.13 Incident Management

Due to ever changing threat landscape, no matter how many defenses we put in place, we should always be ready to manage information security breach whenever it happens. CISO or equivalent person should create a comprehensive information security incident management plan and put together a team responsible for action whenever needed. Standard such as ISO/IEC TR 18044:2004 could be used by organizations to implement comprehensive information security incident management plan.

Figure 25 shows a custom information security incident management plan. Organizations could either use an existing standard or create one of their own depending on legal requirements and enterprise objectives.

When an information security incident occurs, measures taken so far such as employee awareness, personnel security, physical security, network security, and software security should be able to detect the incident. Incident could be reported directly by external users who call organization customer service telephone number or send an email to customer support team. CISO or equivalent person should have a core team in place to look into the incidents. They may not fix the problem themselves but knowledge of incidents helps them to improve defenses as well as inform senior management on a regular basis. This core team has two sides to look into for each incident. One is external management and the other is internal management.

External management deals with legal and regulatory side as well as requirements put in place by adopted standards, frameworks and best practices (i.e. house of compliance). Another part of external management is to communicate with stakeholders such as shareholders, business partners or consumers. Organization must have clear policy in place for efficiently managing its reputation after an incident happens. External management is mostly the responsibility of CISO or core incident management team who work closely with CIO. CIO works with CEO and strategy group to communicate with external stakeholders.

Internal management includes putting a framework in place for who will actually work on the problem. Depending on the size of the organization, this could be done in multiple ways. One way is to create different levels. Incident is first handled by first level team. Depending on complexity and other factors, level one team may refer to next higher level team. Usually bigger organizations prefer to go this way. Smaller organizations may have one expert person handling all kinds of incidents. Usually organizations have a software product to record the incident and create an incident ticket number for tracking purpose. Assigned person or team should respond to the incident and escalate appropriately to next level.

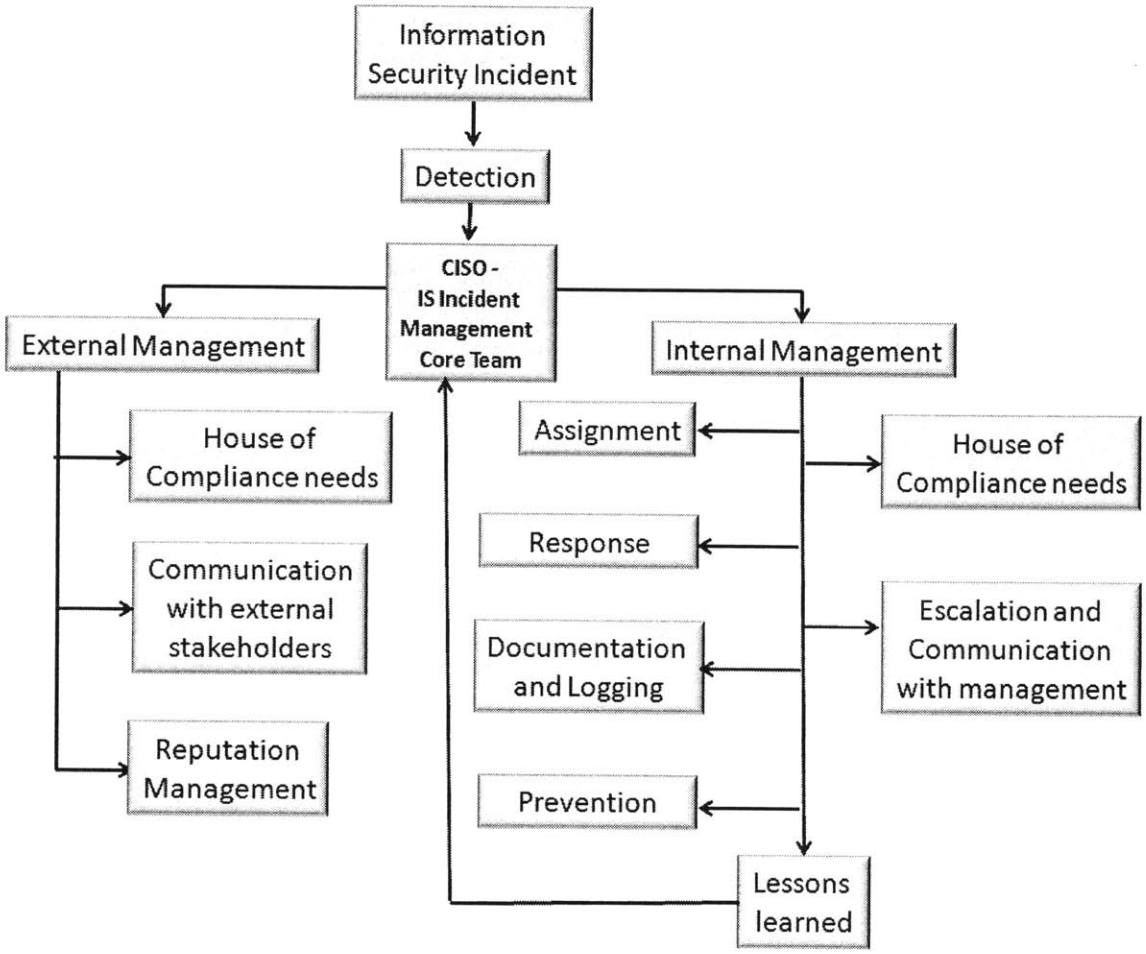

Information Security Incident
Detection
CISO - IS Incident Management Core Team
External Management
Internal Management
House of Compliance needs
Communication with external stakeholders
Reputation Management
Assignment
Response
Documentation and Logging
Prevention
House of Compliance needs
Escalation and Communication with management
Lessons learned

Figure 25: Custom Information Security Incident Management Plan

Complete documentation of every incident should be done for better forensics and future planning. Where possible (for example, in electronic transactions) log should be captured of the time window in which incident occurred as well as all the work that was done to fix the problem. Technical person should describe in plain words (as much as possible) what the problem was and what fix was put in. Technical person who worked on the problem should have a placeholder for putting in recommendations on prevention of similar incident in the future.

Internally, due to house of compliance needs, organizations may perform certain procedural tasks such as comprehensive documentation, audit trail and communication. Depending on the severity of the problem, person or team working on the incident should inform their management about the incident. For example, database table containing customer information was truncated. This could essentially imply that customers are no longer able to access their information online. Person or team working on the incident may be quickly able to restore the customer information database table. However, incident response person or team should know that for such a critical incident, senior management must be informed. Hence, CISO or equivalent person must come up with clear guidelines on *when* and *how* to escalate an incident and inform senior management.

Finally, as part of internal management, core information security incident management team should review all the incidents in comprehensive detail including incident description, impact analysis, symptoms, diagnostics, action taken, and prevention recommendations. This should be done at a pre-established frequency (for example, once a month or quarterly). Lessons learned provide a great input for improving information security management process and infrastructure thereby leading to better protection.

In summary, organizations should approach information security incident management from compliance, technological, management, and learning perspective. A sound incident management plan would go a long way in keeping organization reputation intact and not lose business due to an incident.

3.14 Future Planning

In the fast changing information security domain, we should always be on the lookout for potential new threats. Just as with everything else so far, a careful planning and comprehensive approach is needed for information security future planning as well. Below are key the components for an effective information security future planning at an enterprise level.

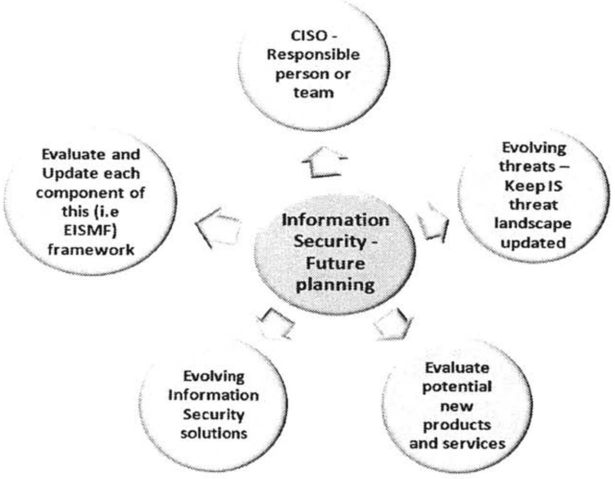

CISO - Responsible person or team
Evolving threats – Keep IS threat landscape updated
Evaluate potential new products and services
Evolving Information Security solutions
Evaluate and Update each component of this (i.e EISMF) framework
Information Security - Future planning

Figure 26: Key components of Information Security Future Planning

CISO -Responsible person or team

CISO or equivalent person should put a person or a team responsible for future planning of overall information security. CISO should work closely with CIO and various department heads so that a comprehensive information security future planning could be done with everyone on board. CISO would need information from various departments on what new products or services they are planning to buy or currently evaluating for future use. CIO could act as a liaison between CISO and various department heads. Future planning is a continuous process because departments are always working on something new or improving the existing products and services. However, CISO or equivalent person may create an annual future planning report. In the report, all components of EISMF may be covered (discussed later).

Evolving threats

This involves study of constantly emerging new threats in the information security domain. They may not be currently applicable to the organization. However, they may help from a learning perspective as well as potential to modify existing defenses. This study could include geographic location specific emerging threats (for example, possibility of flooding), technology specific threats (for example, information security concerns over cloud computing), and regional threats (for example, civil problems such as riots etc.). Also, one emerging threat could pose a threat from multiple perspectives. For example, a potential threat to a building could not only pose a threat to physical security personnel but also to employees and computer hardware devices. Organization must ensure that information security threat landscape is always up-to-date.

Evaluate potential new products and services

Organizations use new products and services all the time. Existing products and services could be modified to meet new requirements. All of these activities bring potential new risks to information security. It is highly recommended that information security threats from these products and services should be analyzed preferably before making a purchase. Most products and services come with a trial period. During the trial period, comprehensive information security assessment should be done.

Evolving Information Security solutions

Organizations need to keep up with the latest emerging information security solutions. This helps from two perspectives. Firstly, these solutions may help in learning more about emerging threats. Secondly, organizations may consider these solutions for a future purchase. Therefore, it helps in future cost planning and technical environment planning.

Evaluate and Update each component of this (i.e. EISMF) framework

Organizations should consider evaluating and updating their information security management approach periodically (for example, annually). This involves going through each component of EISMF.

- *Organizational Structure:* Each year, an assessment should be done whether organization needs an organizational structure change. For example, they may need additional personnel for information security management.

- *House of compliance*: There may be modifications to the existing laws and regulations. New standards, frameworks or best practices may be coming. House of compliance needs to be revisited each year. However, for legal compliance, organizations should act promptly and not wait for yearly cycle.

- *Policy and Procedures:* Enterprise information security policy must be current. It should reflect lessons learned, drop whatever is no longer a threat, and accommodate new threats. Procedures should be updated as well.

- *Risk Management:* As new threats emerge from adoption of new products or services, or from technological advances made in the underworld economy, organizations must assess risks all the time. New methods, products or services may emerge for performing risk assessment. It is imperative to keep assessed risks current.

- *Employee awareness and training:* Employees must be educated about emerging threats and what they can do to prevent information security breach. Yearly evaluation of employee training should be done to accommodate new lessons.

- *Personnel Security:* Personnel security checklist should be updated annually.

- *Physical Security:* Physical threat landscape should be evaluated for possible future threats.

- *Network Security:* This is key area because network threats are varying very rapidly. Hence, network security must be analyzed for possible future upgrades.

- *Software Security:* This is constantly changing area as well. Key threats keep emerging. New frameworks may emerge for incorporating information security into software development life cycle. Organizations should let their software architects plan for future in this area.

- *Identity Management and Access control:* This is an exciting area where new products and services are brought in for organization to manage identity and access control. CISO or equivalent person should consider looking into details for future use of a new product or service.

- *Information Operations Management:* This is a big area. Organization should evaluate changes in the future for all components- Asset acquisition and inventory management, Change Management, Backup and recovery, Asset retirement and disposal.

- *Assurance and Evaluation:* If an organization is using ISO/IEC 15408, then any modifications or revisions to the standard should be considered. Organizations may look for possible custom extension to the current standard.

- *Incident Management:* If ISO/IEC TR 18044:2004 is being used in an organization, then upcoming changes to the standard should be evaluated for budget and planning purpose. Any custom extensions to the standard or custom framework should be evaluated for future changes as well.

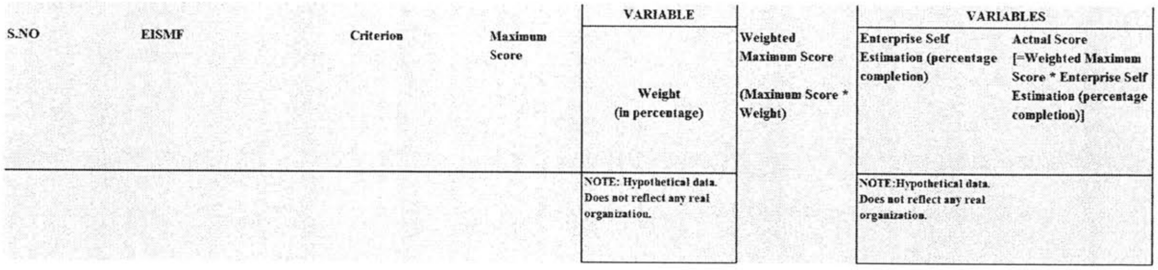
- *Future Planning:* Dedicated time should be allocated by CISO or equivalent person for future planning of overall information security management.

In the next chapter, we use the discussion so far to come up with key criteria for each of the fourteen points in the EISMF and use the criteria to come up with an information security management maturity level.

CHAPTER 4: Information Security Management Maturity Level based on EISMF

Organizations can use EISMF to get started with information security management. However, organizations may find it more useful to know where they stand with regards to information security management. In addition, organizations would want a way to track progress made in the overall information security management. This brings us to the concept of information security management maturity level. Based on detailed discussion in Chapter 3, the author using extensive personal information technology experience came up with key criteria for each of the fourteen points in EISMF. Author's *assumptions* and *approach* for coming up with information security management maturity level are described below:

- Criteria under each point of EISMF are generic and should be applicable to most organizations irrespective of the industry, size (revenue or number of employees) and type of business.



				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	

Table 4: Enterprise Information Security Maturity Level Calculations – *Various Columns*

- Each point in the fourteen point EISMF carries a maximum total of one hundred points. Refer Table 4, column- *EISMF* for a listing of fourteen points.
- For each of EISMF points, one or more key criterion is listed under column – *Criterion (Refer Table 4)*. Each of these criteria carries *approximately* same number of points so that sum of points for different criteria is one hundred. In Table 4, number of points for each criterion is given under column -*Maximum Score.* Note that this is absolute positive number with no decimals.
- For each criterion weight needs to be assigned by the organization leveraging EISMF. Weights may vary depending on type of business, size of organization, and geographical

location due to differences in criterion such as regulatory and privacy laws or for other reasons. CISO or equivalent person and other key stakeholders should discuss relevancy or applicability of each criterion to their particular business. Weight could be assigned between 0% and 100%. 0% weight implies not relevant or not applicable to a business. Whereas, 100% weight implies completely relevant or applicable. Organizations must carefully come up with weights and should review and update them periodically while keeping track of what changed and why. Refer Table 4, column- *Weight* for assigning weight to each criterion. Weight is captured in percentage.

- Once, we have weight for each criterion, we calculate weighted maximum score. This is maximum score considering type of business, size of organization, and geographical location. In Table 4, column- *Weighted Maximum Score* is the product of *Maximum Score* and *Weight* rounded to two decimal places.
- Organizations should make a self assessment as to how far they fulfill or meet a specific criterion. In Table 4, this is captured under column - *Enterprise Self Estimation (percentage completion).* Percentage should be rounded to nearest value (i.e. no decimals). Note that author does not recommend any particular method for arriving at these percentages. Organizations may find it useful to conduct interviews of concerned personnel and take an average to fill in the percentages. Too much variance in the percentage value from different interviews should immediately get management's attention. Management should first resolve those differences and then come up with an agreed upon percentage value.
- In Table 4, actual score for each criterion is calculated under column – *Actual Score.* Actual score for each criteria is calculated as follows:

  *Actual Score = Weighted Maximum Score * Enterprise Self Estimation (percentage completion)*

  Note that actual score is rounded to two decimal places.

- To compute percentage compliance with EISMF, we sum the Weighted Maximum Score and Actual Score separately. Percentage compliance is calculated as follows:

  Percentage Compliance = [Σ (Actual Score) /Σ (Weighted Maximum Score)]*100

- After calculating percentage compliance, information security management maturity levels are determined as follows
    - Level I : 0% < Percentage Compliance <= 20%
    - Level II : 20% < Percentage Compliance <= 40%
    - Level III : 40% < Percentage Compliance <= 60%
    - Level IV : 60% < Percentage Compliance <= 80%
    - Level V : 80% < Percentage Compliance <= 100%
- Disclaimer: *Please note that in Enterprise Information Security Maturity Level Calculations, data shown under columns - Weight (in percentage) and Enterprise Self Estimation (percentage completion) is purely hypothetical. It was NOT obtained from any organization. Any match with any organization is purely coincidental.*

Key criteria for each of the fourteen points in EISMF are discussed below.

4.1 Organizational Structure

Organizational structure of many large organizations does have a dedicated C-level person responsible for information security management. Enterprise Security Group[16] found more than half of 227[16] large organizations covered in their survey had a CISO. There are clear cost benefits when CISO is leading data breach effort. Ponemon[17] Institute found that cost incurred per breached data record was $157[17] when CISO (or a similar/equal role) was leading the data breach response effort. Whereas, cost incurred per breached data record was $236[17] when there was no CISO leading the breach response effort. IT Policy Compliance Group[18] studied 809[18] companies looking for effect of "organizational structure and strategy on managing the value of information and information assets" [18]. The study found out that presence of a CISO

[16] SC Magazine, Roundup 2006: Do CISOs matter?, Dated December 14, 2006, Retrieved on September 15,2010 from http://www.scmagazineus.com/roundup-2006-do-cisos-matter/article/34254/

[17] Ponemon Institute, Fifth Annual US Cost of Data Breach, January 2010 - 2009 Annual Study: Cost of a Data Breach, Page 25, Retrieved on September 15, 2010 from http://www.ponemon.org/data-security

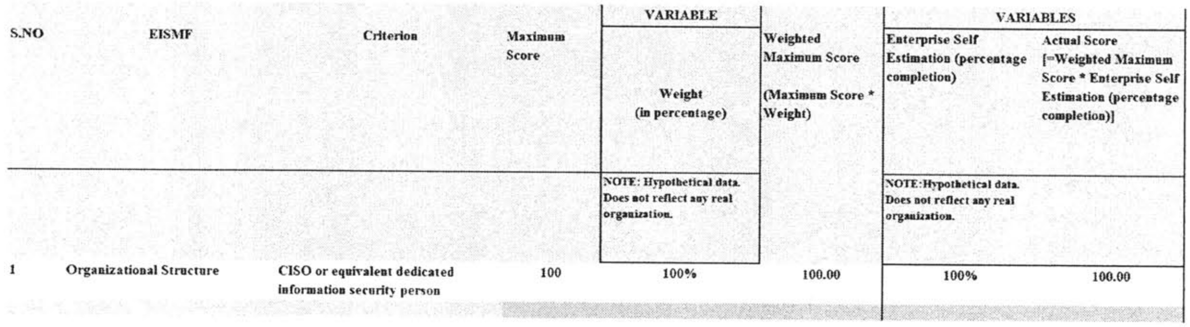
[18] ISACA, ITpolicycompliance.com (18 February 2010), New Report Shows Benefits of CISOs, Retrieved on September 16, 2010 from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/New-Report-Shows-Benefits-of-CISOs.aspx

within an organization results in effective utilization of information property by way of increased ability to keep existing customer base, decreased information loss, and reduced audit costs[18].

Based on above data, it is clear that a top level dedicated person for information security management would be greatly beneficial to an organization. CISO or equivalent person would find it extremely valuable to follow key principles for managing overall information security strategy and innovation. Cusumano (2010) describes six generic principles for effective strategy and innovation management. These are: "(a) Platforms, Not Just Products (b) Services, Not Just Products (or Platforms) (c) Capabilities, Not Just Strategy (d) Pull, Don't Just Push (e) Scope, Not Just Scale (f) Flexibility, Not Just Efficiency" [Cusumano (2010)].

Hence, for organization structure, CISO or equivalent dedicated information security person is a key criterion. There are no other criteria under organizational structure.

For maturity level calculations, author gives 100 points out of 100 points for having a dedicated information security management person at a top level. Part time person could be accommodated by adjusting weight. Author strongly recommends a full time top level person for information security management. Author's information security maturity level calculation sheet is shown below (Table 5) covering organizational structure (first point under EISMF).



				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
1	Organizational Structure	CISO or equivalent dedicated information security person	100	100%	100.00	100%	100.00

Table 5: Enterprise Information Security Maturity Level Calculations - *Organizational Structure*

As shown in *Table 5*, for our sample calculation a weight of 100% is given to CISO or equivalent dedicated information security person. Note that depending on the size of an organization, weight may vary. For example, for a startup where generally one person wears multiple hats, it may be more practical to choose a percentage much lesser than 100%. Weighted Maximum Score is calculated by multiplying Maximum Score (=100) and Weight (=100%). For an enterprise with a CISO or equivalent dedicated information security person, value of Enterprise Self Estimation would be 100%. Finally, Actual Score is calculated by multiplying Weighted Maximum Score (=100) and Enterprise Self Estimation (=100%). For our sample, we get an Actual Score of 100.00.

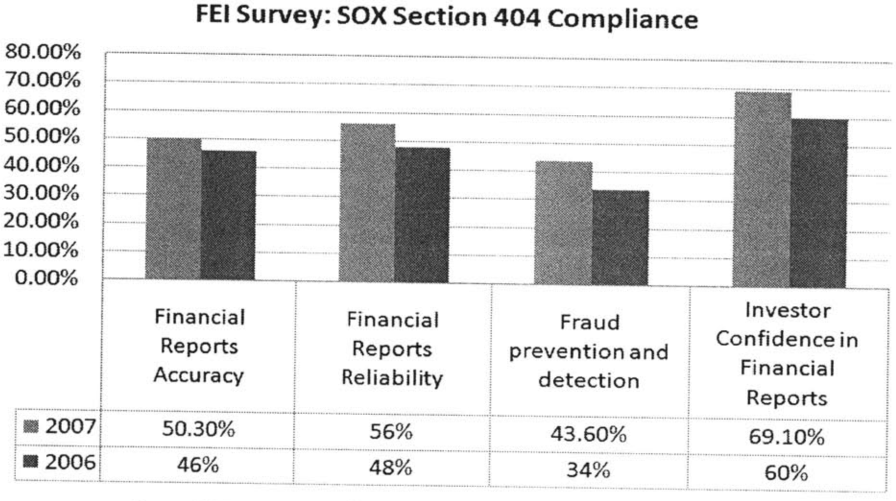
4.2 House of Compliance

House of compliance comprises of information security related laws and regulations, standards, frameworks, and industry best practices. In Figure 15 (House of Compliance), one of the laws is Sarbanes Oxley Act of 2002 which is “an act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes”[19]. Financial Executives International (FEI)[20] surveyed 185[20] organizations averaging $4.7 billion[20] in yearly revenue and looked for feedback on compliance with Section 404 (“*Management assessment of internal controls*”[21]) of Sarbanes Oxley Act of 2002. FEI found that cost of compliance with Section 404 of Sarbanes Oxley Act of 2002 (or SOX) declined over the years as organizations found ways to improve and integrate practices needed for compliance into their regular work practices. In particular, FEI found that cost of compliance in the fourth year was less than beginning three years. Other results from FEI survey are shown in Figure 27. From Figure 27, we learn that through legal compliance organizations do find improvement in their financial reports both from reliability and accuracy standpoint. From information security perspective, organizations find sufficient improvements in fraud prevention as well as detection. Overall investor confidence is improved.

[19] Sarbanes Oxley Act of 2002, The Library of Congress (Thomas), World Wide Web, Retrieved on September 22, 2010 from http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107Tl2MyO:e0:

[20] FEI Survey, Financial Executives International (FEI), World Wide Web, Retrieved on September 22, 2010 from http://fei.mediaroom.com/index.php?s=43&item=204

[21] Sarbanes Oxley Act of 2002, Section 404, The Library of Congress (Thomas), World Wide Web, Retrieved on September 22, 2010 from http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107Tl2MyO:e0:



	Financial Reports Accuracy	Financial Reports Reliability	Fraud prevention and detection	Investor Confidence in Financial Reports
▨ 2007	50.30%	56%	43.60%	69.10%
■ 2006	46%	48%	34%	60%

Source: FEI Survey at http://fei.mediaroom.com/index.php?s=43&item=204

Figure 27: FEI Survey - Sarbanes Oxley Act of 2002 Section 404 Compliance ***(Source: FEI)***

In Figure 15 (*House of Compliance*), one of the information security standards is ISO 27000 series (also called ISO 27k). IsecT Ltd[22], a New Zealand based information security consulting firm studied "business benefits of ISO27k"[23] and found that successful implementation of ISO27k help organizations to improve system dependability in addition to improving overall security of information systems. Other benefits found by IsecT Ltd include increase in number of customers due to increased customer confidence, improved information security efficiency, better utilization of information systems, and help with meeting legal requirements. In addition, ISO 27k emphasize clear enterprise wide communication that helps in building better relationship between management and rest of the employees.

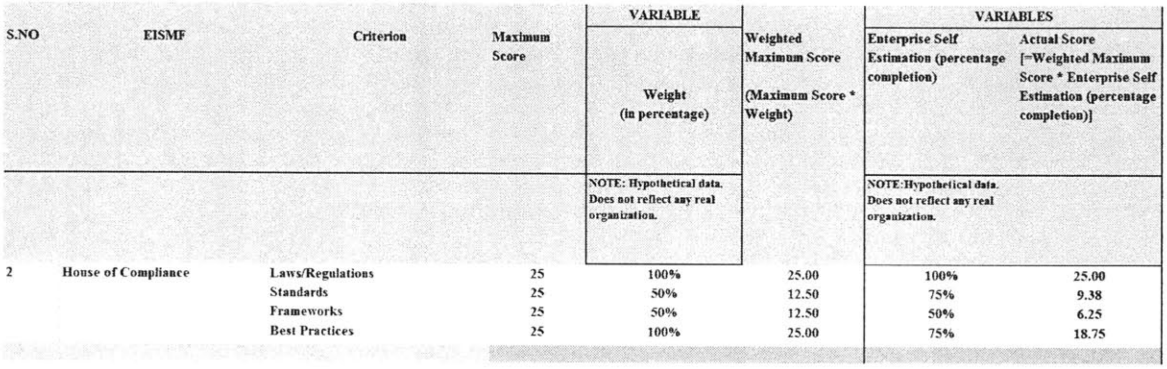
Use of information security frameworks and industry best practices facilitate regulatory compliance as well as help in implementing standards. Therefore, author has four criteria under house of compliance each with a Maximum Score of 25 points. Each criterion has equal number

[22] ISecT Ltd., World Wide Web, Retrieved on September 22, 2010 from http://www.isect.com/

[23] ISO 27001 Security, World Wide Web, Retrieved on September 22, 2010 from www.iso27001security.com/ISO27k_The_business_value_of_ISO27k_case_study.pdf

of points because the author would like to emphasize that each of these criterion are equally important for an organization and CISO (or equivalent person) should ensure all four are implemented with same level of care and attention to details.

Author's information security maturity level calculation sheet covering house of compliance (second point under EISMF) is shown in Table 6.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE		VARIABLES	
				Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
2	House of Compliance	Laws/Regulations	25	100%	25.00	100%	25.00
		Standards	25	50%	12.50	75%	9.38
		Frameworks	25	50%	12.50	50%	6.25
		Best Practices	25	100%	25.00	75%	18.75

Table 6: Enterprise Information Security Maturity Level Calculations – *House of Compliance*

As shown in *Table 6*, each criterion carries Maximum Score of 25 points. However, enterprise may weigh each criterion differently as shown in Weight column in *Table 6*. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.3 Policy and Procedures

Enterprise information security policy and procedures is a clear indicator of an organizations' seriousness about information security. It is a complex document that requires both extensive knowledge in information security domain and art of presentation for easy understanding by all employees and stakeholders. Most government agencies are required by law (Federal Information Security Management Act- FISMA) to have an official enterprise information security policy. Public companies complying with Sarbanes–Oxley Act of 2002 are required to have an official information security policy.

Many government agencies, educational institutions, and other organizations have posted their information security policy in the public domain to show their seriousness in dealing with information security. There are free and commercial solutions available for creation and management of information security policy. For example, SANS (SysAdmin, Audit, Network, Security) Institute has posted information security policy templates for free on their website[24]. Commercial custom solutions are available from leading companies such as IBM, PricewaterhouseCoopers LLP, and Verizon Business. Many Fortune 500 organizations are using products and/or services from these established information technology companies so they tend to leverage existing suppliers in helping them to come up with enterprise information security policy and procedures. There are niche players offering information technology consulting services in a particular domain such as healthcare industry, and energy industry.

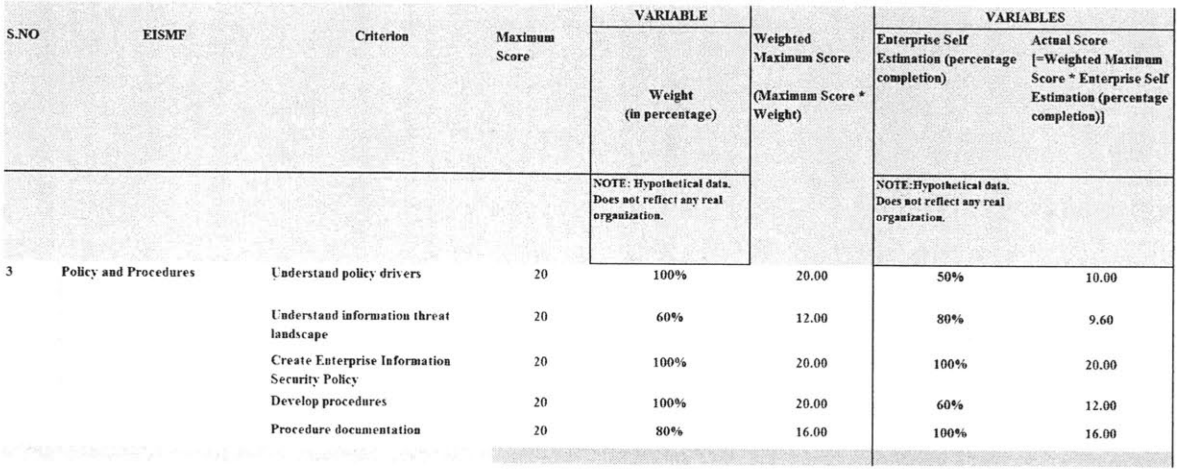
Organizations are reaping several benefits of enterprise information security policy and procedures. Enterprise information security policy and procedures show that organization is committed to securing its own and customer information assets. This has potential to win more customers as well as retain existing ones. There are cost benefits in terms of savings resulting from reduction in number of information security breaches due to increased awareness among employees. Employees become more vigilant and immediately report suspicious activities. This helps in prevention before any significant damage is done. All employees can contribute towards enterprise information security irrespective of what they do at work.

Based on author's personal experience and web searches, there are five key criteria for *policy and procedures* (Refer *Table 7*) that include (a). Understand policy drivers (b). Understand information threat landscape (c). Create enterprise information security policy (d). Develop procedures (e).Procedure documentation. For effective creation and management of *policy and procedures*, each of these is equally important. Each criterion carries Maximum Score of 20 points. However, enterprise may weigh each criterion differently as shown in Weight

[24] SANS (SysAdmin, Audit, Network, Security) Institute , Information Security Policy Templates, World Wide Web, Retrieved on September 26, 2010 from http://www.sans.org/security-resources/policies/

column in Table 7. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

Author's information security maturity level calculation sheet covering policy and procedures (third point under EISMF) is shown in Table 7.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score (Maximum Score * Weight)	VARIABLES	
				Weight (in percentage)		Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
3	Policy and Procedures	Understand policy drivers	20	100%	20.00	50%	10.00
		Understand information threat landscape	20	60%	12.00	80%	9.60
		Create Enterprise Information Security Policy	20	100%	20.00	100%	20.00
		Develop procedures	20	100%	20.00	60%	12.00
		Procedure documentation	20	80%	16.00	100%	16.00

Table 7: Enterprise Information Security Maturity Level Calculations – ***Policy and Procedures***

In summary, information security policy and procedures is a key requirement for complying with certain government regulations. Enterprise wide scope reiterates the fact that information security extends beyond technology domain and it is of a significant business concern in addition to technology challenge. Free and commercial solutions are available to help businesses come up with appropriate information security policy and procedures. There are several monetary and non-monetary benefits of creating an enterprise wide information security policy as well as a set of information security procedures.

4.4 Risk Management

Risk assessment is an integral part of risk management process. There are several free and commercial products available in the market to help an organization with both risk assessment and risk management. Some companies in the risk assessment business have created risk assessment solutions targeted towards particular industry (*For example, banks, hospital etc.*), compliance with specific regulation (*For example, HIPAA, Sarbanes Oxley Act of 2002 etc.*), or general purpose risk assessment templates for company in house use. Tremendous information is available online on various government websites regarding information security risk assessment. For example, in the United States, state of Massachusetts has posted "Information Security Risk Assessment Guidelines"[25] on its official website. Virginia Information Technology Agency (VITA) has posted "IT Risk Management Guideline"[26] on the official website of state of Virginia. Organizations can leverage information from trusted sources such as government websites, educational institutions, or reputed companies to create custom risk management process. Microsoft has "Security Risk Management Guide"[27] available for free download from its website.

Based on author's risk management process covered in Section 3.4, there are five criteria which are critical for comprehensive risk management as shown in Table 8. These five key criteria for effective *risk management* (Refer *Table 8*) are (a). Clearly established risk assessment process (b). List of information assets, asset classification, asset owner, and information utilization details (c). Asset impact/valuation, threat assessment, vulnerability assessment, current safety assessment, probabilistic estimates (d). Clearly documented risk management process (e). Documented risk management process implementation.

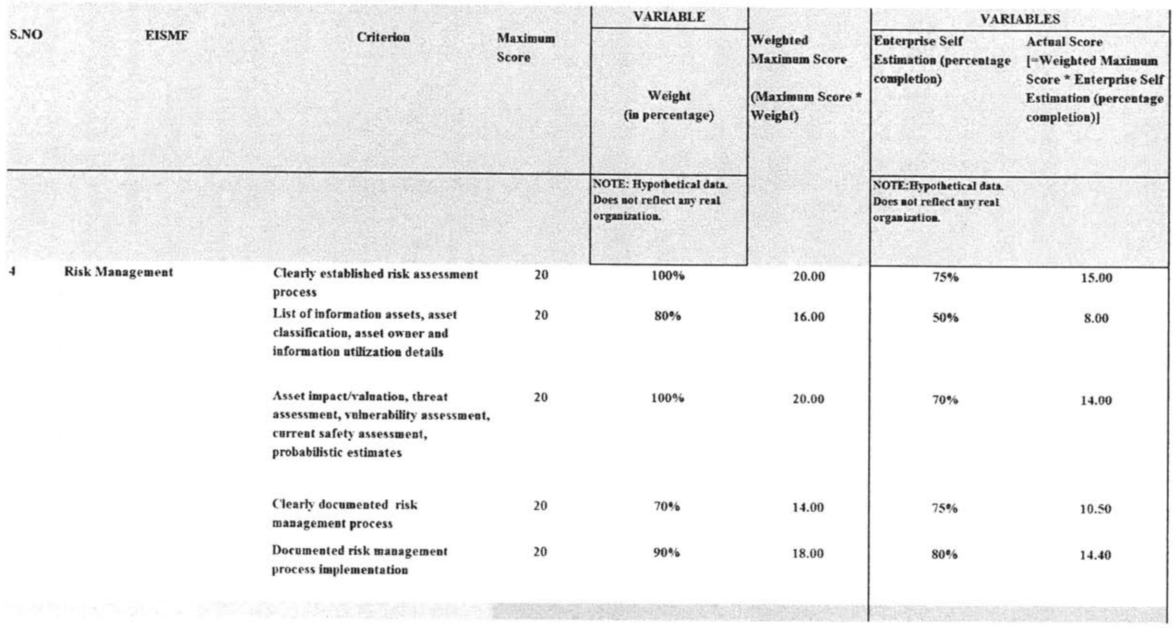
For effective creation and management of *risk assessment*, each of these is equally important. Each criterion carries Maximum Score of 20 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 8. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to

[25] The Official Website of the Commonwealth of Massachusetts, Information Security Risk Assessment Guidelines, World Wide Web, Retrieved on September 28, 2010 from http://www.mass.gov/?pageID=afterminal&L=4&L0=Home&L1=Research+%26+Technology&L2=IT+Policies%2C+Standards+%26+Guidance&L3=Technical+Guidance&sid=Eoaf&b=terminalcontent&f=itd_policies_standards_it_security_risk_assessment_guidelines&csid=Eoaf

[26] Virginia Information Technology Agency (VITA), IT Risk Management Guideline, World Wide Web, Retrieved on September 28, 2010 from http://www.vita.virginia.gov/library/default.aspx?id=537

[27] Microsoft, Security Risk Management Guide , World Wide Web, Retrieved on September 28, 2010 from http://technet.microsoft.com/en-us/library/cc163143.aspx

estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score (Maximum Score * Weight)	VARIABLES	
				Weight (in percentage)		Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
4	Risk Management	Clearly established risk assessment process	20	100%	20.00	75%	15.00
		List of information assets, asset classification, asset owner and information utilization details	20	80%	16.00	50%	8.00
		Asset impact/valuation, threat assessment, vulnerability assessment, current safety assessment, probabilistic estimates	20	100%	20.00	70%	14.00
		Clearly documented risk management process	20	70%	14.00	75%	10.50
		Documented risk management process implementation	20	90%	18.00	80%	14.40

Table 8: Enterprise Information Security Maturity Level Calculations – *Risk Management*

In summary, there are plenty of options available for enterprises to study *risk management* domain and establish an appropriate risk management process suitable to their own particular business environment.

4.5 Employee awareness and training

Organizations should opt for more structured training programs for all of their existing employees. For new hires, training should be provided right at the beginning of employment term. More sophisticated training programs should be offered to employees who are directly responsible for information security or more generally in the information technology department. There are many training programs available for increasing employee information security awareness. For example, Software Engineering Institute (Carnegie Mellon)[28] and SANS (SysAdmin, Audit, Network, Security) Institute[29] both offer information security training and certification courses. Organizations may hire people who hold certification or a degree in information security. These employees can help put together a comprehensive information security awareness and training program for other employees. Now a days, many universities offer program in information security.

Following should be covered as part of employee awareness and training program:

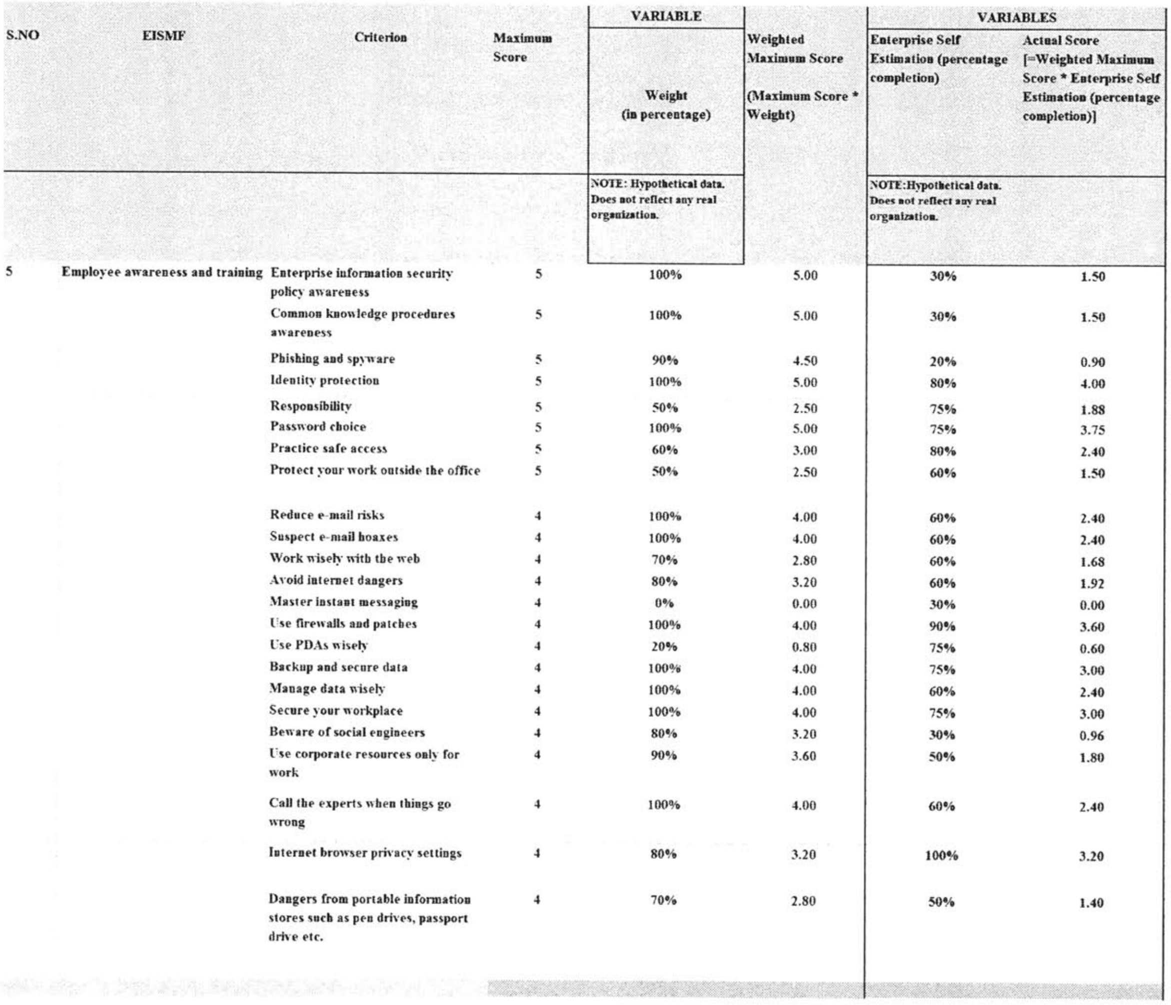
- Enterprise information security policy awareness
- Common knowledge procedures awareness
- "Beware of phishing and spyware "(Rothke, Ben (2005))
- "Protect your identity " (Rothke, Ben (2005))
- "Be responsible and be aware " (Rothke, Ben (2005))
- "Choose your password wisely " (Rothke, Ben (2005))
- "Practice safe access" (Rothke, Ben (2005))
- "Protect your work outside the office" (Rothke, Ben (2005))
- "Reduce e-mail risks" (Rothke, Ben (2005))
- "Suspect e-mail hoaxes" (Rothke, Ben (2005))
- "Work wisely with the web" (Rothke, Ben (2005))
- "Avoid internet dangers" (Rothke, Ben (2005))
- "Master instant messaging" (Rothke, Ben (2005))
- "Use firewalls and patches" (Rothke, Ben (2005))
- "Use PDAs wisely" (Rothke, Ben (2005))
- "Backup and secure data" (Rothke, Ben (2005))
- "Manage data wisely" (Rothke, Ben (2005))
- "Secure your workplace" (Rothke, Ben (2005))
- "Beware of social engineers " (Rothke, Ben (2005))

[28] SEI Carnegie Mellon, World Wide Web, Retrieved on September 29, 2010 from http://www.sei.cmu.edu/training/

[29] SANS Institute, World Wide Web, Retrieved on September 29, 2010 from http://www.sans.org/

- "Use corporate resources only for work " (Rothke, Ben (2005))
- "Call the experts when things go wrong" (Rothke, Ben (2005))
- Internet browser privacy settings
- Dangers from portable information stores such as pen drives, passport drive etc.

Author's criteria for efficient employee awareness and training are shown in Table 9 for Enterprise Information Security Maturity Level Calculations.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score (Maximum Score * Weight)	VARIABLES	
				Weight (in percentage)		Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
5	Employee awareness and training	Enterprise information security policy awareness	5	100%	5.00	30%	1.50
		Common knowledge procedures awareness	5	100%	5.00	30%	1.50
		Phishing and spyware	5	90%	4.50	20%	0.90
		Identity protection	5	100%	5.00	80%	4.00
		Responsibility	5	50%	2.50	75%	1.88
		Password choice	5	100%	5.00	75%	3.75
		Practice safe access	5	60%	3.00	80%	2.40
		Protect your work outside the office	5	50%	2.50	60%	1.50
		Reduce e-mail risks	4	100%	4.00	60%	2.40
		Suspect e-mail hoaxes	4	100%	4.00	60%	2.40
		Work wisely with the web	4	70%	2.80	60%	1.68
		Avoid internet dangers	4	80%	3.20	60%	1.92
		Master instant messaging	4	0%	0.00	30%	0.00
		Use firewalls and patches	4	100%	4.00	90%	3.60
		Use PDAs wisely	4	20%	0.80	75%	0.60
		Backup and secure data	4	100%	4.00	75%	3.00
		Manage data wisely	4	100%	4.00	60%	2.40
		Secure your workplace	4	100%	4.00	75%	3.00
		Beware of social engineers	4	80%	3.20	30%	0.96
		Use corporate resources only for work	4	90%	3.60	50%	1.80
		Call the experts when things go wrong	4	100%	4.00	60%	2.40
		Internet browser privacy settings	4	80%	3.20	100%	3.20
		Dangers from portable information stores such as pen drives, passport drive etc.	4	70%	2.80	50%	1.40

Table 9: Enterprise Information Security Maturity Level Calculations – *Employee awareness and training*

Author views each of the above criteria as roughly equally important for effective *employee awareness and training program* in an organization. Therefore, each criterion carries either 4 or 5 points so that sum of all the points under *employee awareness and training* is 100 points *(Refer Table 9)*. However, enterprise may weigh each criterion differently as shown in Weight column in Table 9. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.6 Personnel Security

Generally, most organizations are looking for three key areas when it comes to personnel security. *First*, whether person working for the organization is trustworthy. This usually involves checking background, driving history, looking for criminal record, credit history, and any problems with any law enforcement agency. In addition, physical and mental conditions are evaluated. These are not one time tasks. All these checks are repeated at regular intervals. *Second*, organizations look for whether person is skilled enough to handle the job. If person is not capable, it may lead to frustration which could result in mental and psychological problems. Therefore, organizations look for a match between skills needed for a job and skill set of the person under consideration for the job. Past work experience, education, vocational and other training could be used to establish whether a person is capable to handle the job. *Finally*, organizations try to make sure work environment is safe for the person to work. This includes allowing only authorized personnel to enter work area by checking ID card, retina scan, numeric lock or other methods. Work facility is electronically monitored. Complete track of who entered or left work area is kept in a system which is regularly internally and externally audited. Employees are made aware of the consequences of information theft. Note that organization must ensure that by enforcing security they are not violating rights of an individual. For example, United States constitution does not allow discrimination based on race, age, accent etc.

Organizations can leverage several excellent resources online or otherwise to carve out an effective personnel security program. U.S Department of Homeland Security has posted

"Personnel Security Guidelines"[30] online prepared by the Idaho National Engineering and Environmental Laboratory. Another document- "The DHS Personnel Security Process"[31] published by Department of Homeland Security from Office of Inspector General is also available online. A very detailed document titled –"Department of the Navy Personnel Security Program"[32] from the Secretary of the Navy is available online as well. Some non-government organizations have posted personnel security program details online. There are several organizations that are in the business of providing personnel security and help organizations build an effective personnel security program.

Based on above discussion, author has following ten criteria under personnel security.

- Complete background check- Driving history, criminal check, credit history
- Match skill of a person with job requirements
- Identification method (ID Cards/ Retina scan, pass-code etc.)
- Proper system access at all times (prompt action when employee/contractor moves on)
- System and system access internal / external audit
- Mandatory reporting of change in security clearance by employee/contractor
- Automatic logging and audit trail of human access to any system or application
- Awareness of consequences of information theft
- Peer alertness at all times
- Awareness of individual rights as provided by the constitution

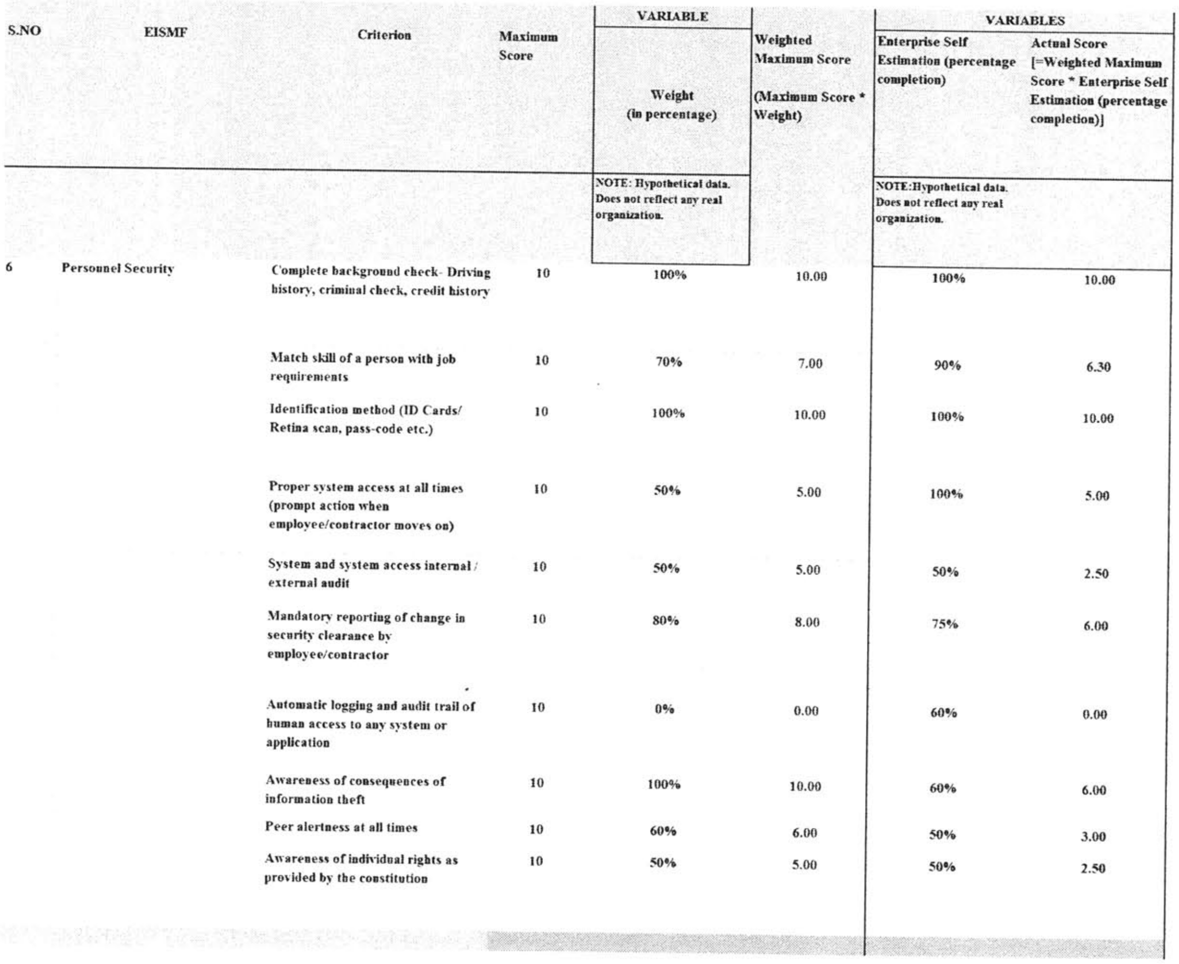
[30] U.S Department of Homeland Security, Idaho National Engineering and Environmental Laboratory , Personnel Security Guidelines, World Wide Web, Retrieved on October 1, 2010 from www.us-cert.gov/control_systems/pdf/**personnel**_guide0904.pdf

[31] U.S Department of Homeland Security, Office of Inspector General , The DHS Personnel Security Process, World Wide Web, Retrieved on October 1, 2010 from www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-65_May09.pdf

[32] U.S Department of Navy, The Secretary of Navy, Personnel Security Program, Published By Chief of Naval Operations (N09N) Special Assistant for Naval Investigative Matters and Security, World Wide Web, Retrieved on October 01, 2010 from http://www.ncis.navy.mil/securitypolicy/Personnel/SECNAVINST/SECNAV%20M-5510.30%20-%20Complete%20Manual.pdf

Author views each of the above criteria as equally important for effective *personnel security* in an organization. Therefore, each criterion carries 10 points so that sum of all the points under *personnel security* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table above. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

Above criteria are shown in the Table 10 for Enterprise Information Security Maturity Level Calculations.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score (Maximum Score * Weight)	VARIABLES	
				Weight (in percentage)		Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
6	Personnel Security	Complete background check- Driving history, criminal check, credit history	10	100%	10.00	100%	10.00
		Match skill of a person with job requirements	10	70%	7.00	90%	6.30
		Identification method (ID Cards/ Retina scan, pass-code etc.)	10	100%	10.00	100%	10.00
		Proper system access at all times (prompt action when employee/contractor moves on)	10	50%	5.00	100%	5.00
		System and system access internal / external audit	10	50%	5.00	50%	2.50
		Mandatory reporting of change in security clearance by employee/contractor	10	80%	8.00	75%	6.00
		Automatic logging and audit trail of human access to any system or application	10	0%	0.00	60%	0.00
		Awareness of consequences of information theft	10	100%	10.00	60%	6.00
		Peer alertness at all times	10	60%	6.00	50%	3.00
		Awareness of individual rights as provided by the constitution	10	50%	5.00	50%	2.50

Table 10: Enterprise Information Security Maturity Level Calculations – *Personnel Security*

4.7 Physical Security

Physical security deals with physically protecting access to information storage in electronic or print form. In the mainframe days of computing, mainframe devices were secured in a secure room and physical access to them was limited to a few responsible persons. With widespread adoption of personnel computer, physical security has become more of a challenge. Office space is full of desktop or laptop computers and most people inside the workplace can physically access other persons' computer. These devices can be easily physically taken by a malicious person. Introduction of net books, handheld smart devices and remote work have further complicated physical security.

Concerns on physical security are very realistic and should never be underestimated. Laptop theft at Boeing in year 2006 compromised personal information such as name, address, social security number of "382,000 current and former employees"[33]. Criminals are finding vulnerabilities in the office physical security system and thus find office buildings an easy target for carrying out physical thefts. According to 8th Annual 2010 BSI Computer Theft Survey, in last three years in the United States, more than 5.5 million[34] computing devices were stolen.

Several solutions are available in the market suited for different budgets to help companies with physical security. An article by Paul F. Roberts in the InfoWorld[35] brings out how electronic devices are changing physical access to a facility.

> "The cameras are watching when you drive up to IBM's Watson Research Lab in Hawthorne, N.Y. They're also noticing things … things such as the color of vehicle you're driving and its license plate. When you get out of the car, another camera zooms in on your face, capturing its image and transmitting it (along with snapshots of your car and license plate) to third-party analytics systems, which then compare those bits against a database of lab employees and authorized visitors. By the time you get to the door at Hawthorne, says Arun Hampapur, manager of IBM's Exploratory Vision Group, the cameras

[33] McMillan, R., Computerworld, Boeing laptop theft puts U.S. data breach tally over 100M, World Wide Web, Retrieved on October, 04 2010 from http://www.computerworld.com/s/article/9006140/Boeing_laptop_theft_puts_U.S._data_breach_tally_over_100M

[34] MACTECH, Key findings of the 8th Annual 2010 BSI Computer Theft Survey, World Wide Web, Retrieved on October, 04 2010 from http://www.mactech.com/2010/08/03/key-findings-8th-annual-2010-bsi-computer-theft-survey

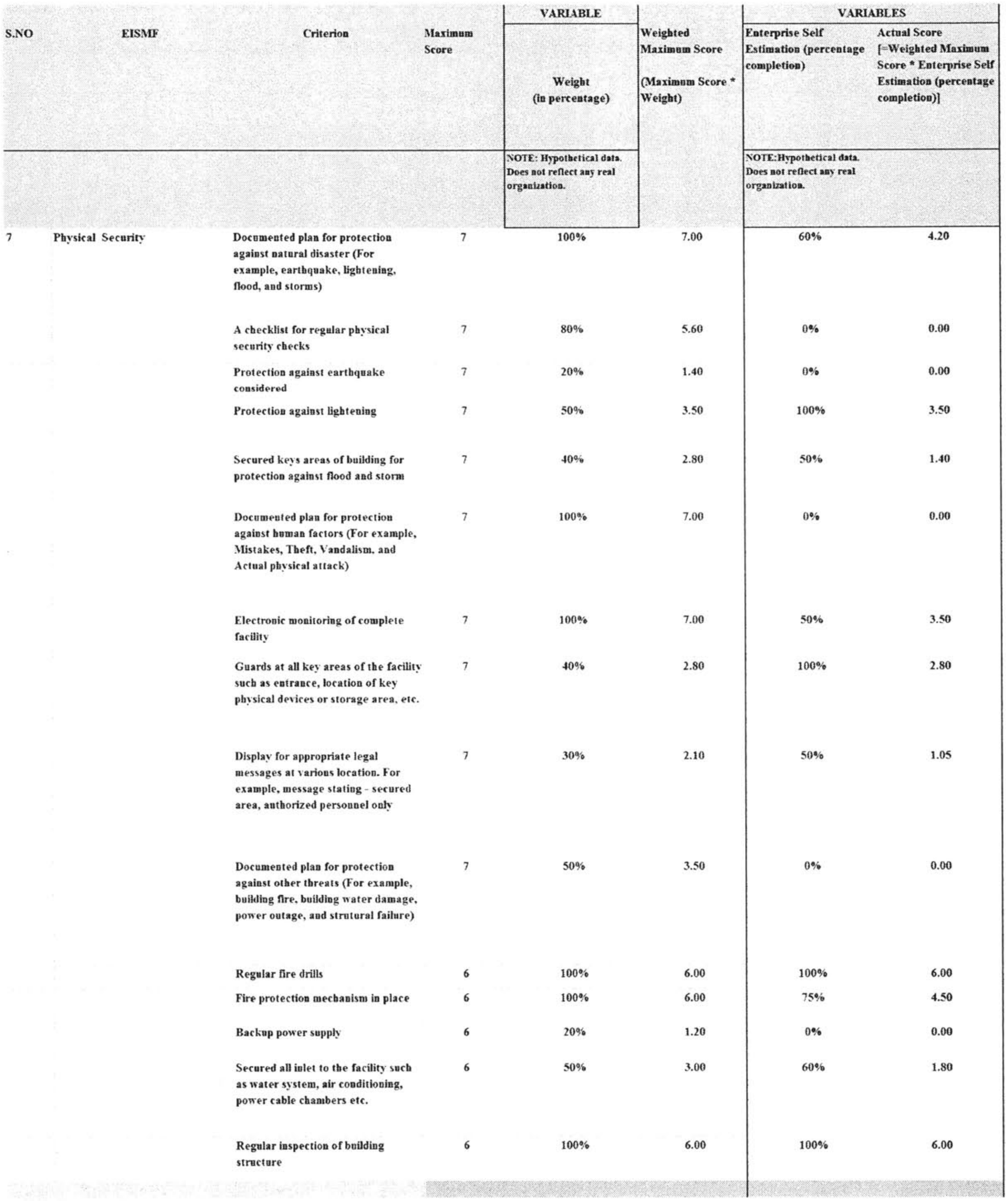
[35] Roberts, P., InfoWorld, IT security gets physical, World Wide Web, Retrieved on October, 04 2010 from http://www.infoworld.com/d/security-central/it-security-gets-physical-876

have, in theory, already *collected enough data to grant you access to the facility without you having to wave a key card or check in at the front desk.*" [Roberts, P., InfoWorld]

Above case is still far from common practice in the industry. However, it brings out progress being made in the physical security domain and how electronic devices are helping secure physical space. Apart from physical theft of computing devices or information in paper form, there are several other sources of physical threats such as floods, earthquake, lightening, war, storms, vandalism, fire, power outage, and structural failure of building. Based on web searches and personal information technology experience, author has come up with following criteria for physical security:

- Documented plan for protection against natural disaster (For example, earthquake, lightening, flood, and storms)
- A checklist for regular physical security checks
- Protection against earthquake considered
- Protection against lightening
- Secured keys areas of building for protection against flood and storm
- Documented plan for protection against human factors (For example, Mistakes, Theft, Vandalism, and Actual physical attack)
- Electronic monitoring of complete facility
- Guards at all key areas of the facility such as entrance, location of key physical devices or storage area, etc.
- Display for appropriate legal messages at various location. For example, message stating - *secured area, authorized personnel only*
- Documented plan for protection against other threats (For example, building fire, building water damage, power outage, and structural failure)
- Regular fire drills
- Fire protection mechanism in place
- Backup power supply
- Secured all inlet to the facility such as water system, air conditioning, power cable chambers etc.
- Regular inspection of building structure

Above criteria are shown in the *Table 11* for Enterprise Information Security Maturity Level Calculations.



				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
7	Physical Security	Documented plan for protection against natural disaster (For example, earthquake, lightening, flood, and storms)	7	100%	7.00	60%	4.20
		A checklist for regular physical security checks	7	80%	5.60	0%	0.00
		Protection against earthquake considered	7	20%	1.40	0%	0.00
		Protection against lightening	7	50%	3.50	100%	3.50
		Secured keys areas of building for protection against flood and storm	7	40%	2.80	50%	1.40
		Documented plan for protection against human factors (For example, Mistakes, Theft, Vandalism, and Actual physical attack)	7	100%	7.00	0%	0.00
		Electronic monitoring of complete facility	7	100%	7.00	50%	3.50
		Guards at all key areas of the facility such as entrance, location of key physical devices or storage area, etc.	7	40%	2.80	100%	2.80
		Display for appropriate legal messages at various location. For example, message stating - secured area, authorized personnel only	7	30%	2.10	50%	1.05
		Documented plan for protection against other threats (For example, building fire, building water damage, power outage, and strutural failure)	7	50%	3.50	0%	0.00
		Regular fire drills	6	100%	6.00	100%	6.00
		Fire protection mechanism in place	6	100%	6.00	75%	4.50
		Backup power supply	6	20%	1.20	0%	0.00
		Secured all inlet to the facility such as water system, air conditioning, power cable chambers etc.	6	50%	3.00	60%	1.80
		Regular inspection of building structure	6	100%	6.00	100%	6.00

Table 11: Enterprise Information Security Maturity Level Calculations – ***Physical Security***

Author views each of the above criteria as roughly equally important for effective *physical security* management in an organization. Therefore, each criterion carries either 6 or 7 points so that sum of all the points under *physical security* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 11. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.8 Network Security

Network security is a significant technological and management challenge. Computer networks could be attacked using malware such as viruses, Trojan horses, worms, root kits, and spyware. Other forms of attack include denial-of-service attack, hacking, identity theft, and man in the middle (i.e. interception). Per Symantec Global Internet Security Threat Report, in the year 2009, 15%[36] of data breaches were caused by hacking. Many solutions are available in the market for helping organizations meet their network security challenges. Organizations should first assess their needs using the expertise of people in network security domain and then work out a comprehensive network security management solution which include technological solution as well as appropriate management measures.

Author has identified following key criteria for effective network security management:

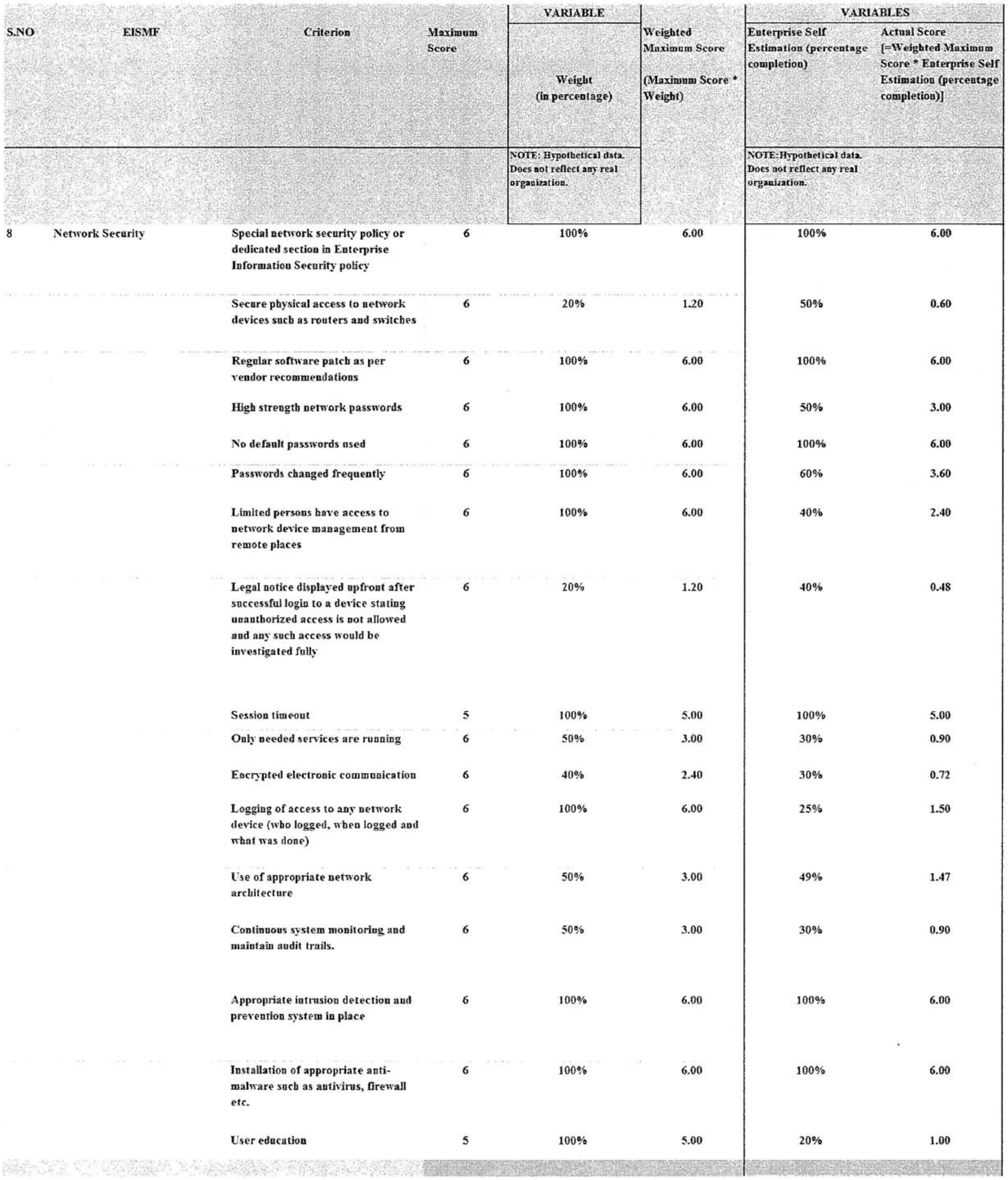
- Special network security policy or dedicated section in Enterprise Information Security policy
- Secure physical access to network devices such as routers and switches
- Regular software patch as per vendor recommendations
- High strength network passwords
- No default passwords used

[36] Symantec Corp. (2010), Symantec Global Internet Security Threat Report, Trends for 2009, Volume XV, Published April 2010, World Wide Web, Retrieved on October 05, 2010 from http://www.symantec.com/business/theme.jsp?themeid=threatreport

- Passwords changed frequently
- Limited persons have access to network device management from remote places
- Legal notice displayed upfront after successful login to a device stating unauthorized access is not allowed and any such access would be investigated fully
- Session timeout
- Only needed services are running
- Encrypted electronic communication
- Logging of access to any network device (who logged, when logged and what was done)
- Use of appropriate network architecture
- Continuous system monitoring and maintain audit trails.
- Appropriate intrusion detection and prevention system in place
- Installation of appropriate anti-malware such as antivirus, firewall etc.
- User education

Author views each of the above criteria as roughly equally important for effective *network security* management in an organization. Therefore, each criterion carries either 5 or 6 points so that sum of all the points under *network security* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 12. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

Above criteria are shown in the Table 12 for Enterprise Information Security Maturity Level Calculations.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score	VARIABLES	
				Weight (in percentage)	(Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
8	Network Security	Special network security policy or dedicated section in Enterprise Information Security policy	6	100%	6.00	100%	6.00
		Secure physical access to network devices such as routers and switches	6	20%	1.20	50%	0.60
		Regular software patch as per vendor recommendations	6	100%	6.00	100%	6.00
		High strength network passwords	6	100%	6.00	50%	3.00
		No default passwords used	6	100%	6.00	100%	6.00
		Passwords changed frequently	6	100%	6.00	60%	3.60
		Limited persons have access to network device management from remote places	6	100%	6.00	40%	2.40
		Legal notice displayed upfront after successful login to a device stating unauthorized access is not allowed and any such access would be investigated fully	6	20%	1.20	40%	0.48
		Session timeout	5	100%	5.00	100%	5.00
		Only needed services are running	6	50%	3.00	30%	0.90
		Encrypted electronic communication	6	40%	2.40	30%	0.72
		Logging of access to any network device (who logged, when logged and what was done)	6	100%	6.00	25%	1.50
		Use of appropriate network architecture	6	50%	3.00	49%	1.47
		Continuous system monitoring and maintain audit trails.	6	50%	3.00	30%	0.90
		Appropriate intrusion detection and prevention system in place	6	100%	6.00	100%	6.00
		Installation of appropriate anti-malware such as antivirus, firewall etc.	6	100%	6.00	100%	6.00
		User education	5	100%	5.00	20%	1.00

Table 12: Enterprise Information Security Maturity Level Calculations – *Network Security*

4.9 Software Security

Thorough analysis of software security is critical whether building or buying software. When building software, it is strongly recommended to analyze security aspects along with business requirements and take security perspective through the remaining phases of design, development, testing and implementation along with business functionalities. When buying software, it is extremely important to understand security functionalities of software under consideration. For some software products, additional security package may be needed.

In the context of software development, Cusumano et al [1995] coined a phrase "Synch-and-stabilize"[37] after studying successful Microsoft software development projects. At the heart lies the idea to let software developers write code in an innovative way. However, new/modified code should be "synchronized" with code from other developers at regular intervals so as to create a "build". This should be followed by code "stabilization" which includes code integration and debugging.

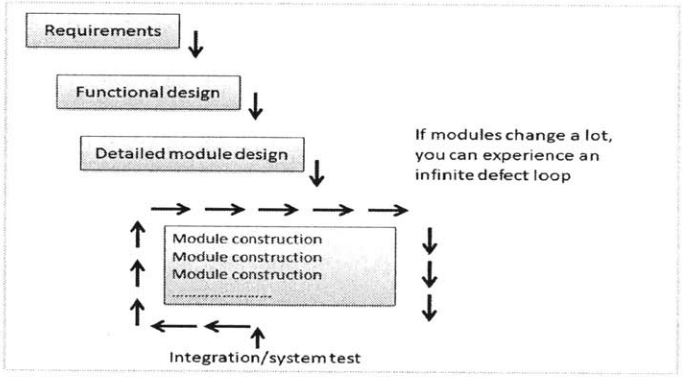
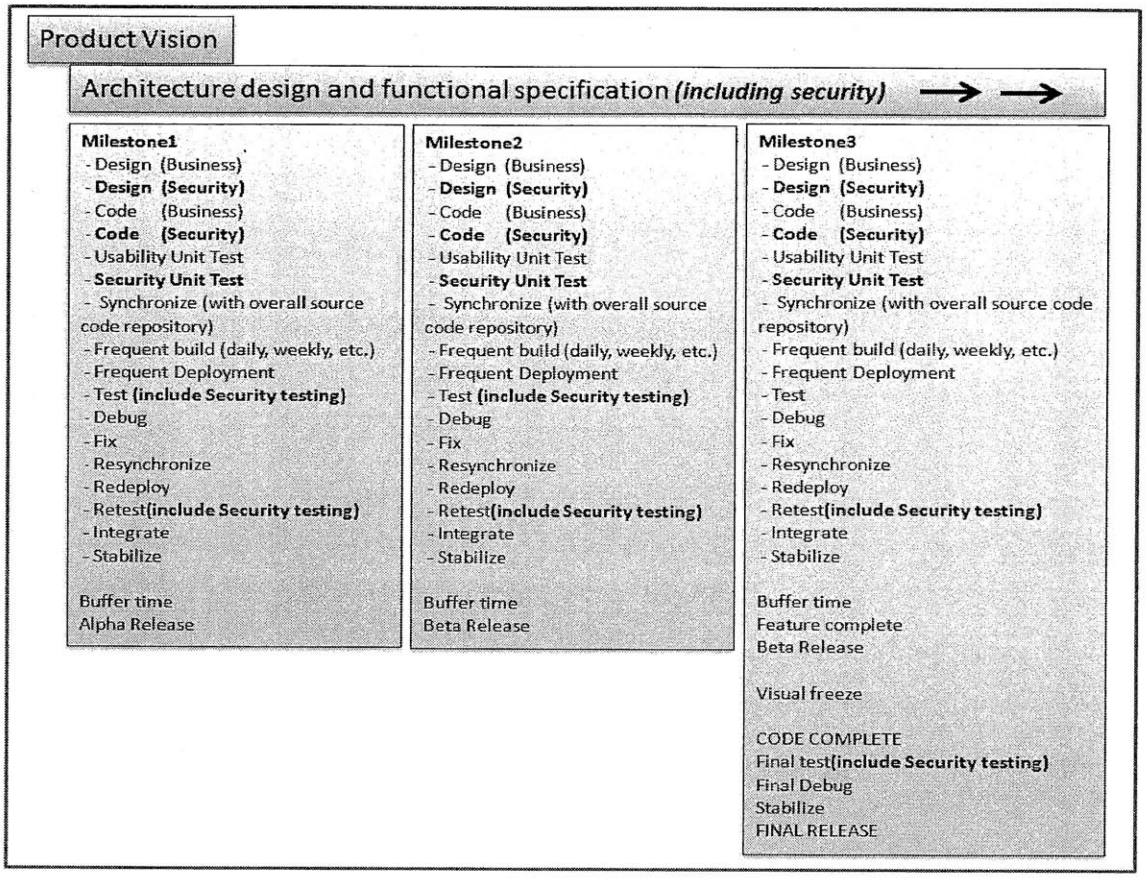


Figure 28: Waterfall Model with Infinite Defect Loop ***[Source: Cusumano (2004), page 151]***

The "synch-and-stabilize" approach offers several benefits over sequential development models such as "waterfall" model. Cusumano [2004] explains one such benefit is that project

[37] Cusumao, Michael, Selby, Richard W Selby, 1995, Microsoft Secrets: How the World's Most Powerful Software Company Creates Technology, Shapes Markets, and Manages People, Publisher: Free Press (A division of Simon & Shuster, Inc.), New York

teams would be able to save themselves from getting into "Infinite Defect Loops" [38] *(Refer Figure 28).* The author adapted the synch-and-stabilize process model *(See Figure 29)* for incorporating software security at every stage of software development lifecycle.



Product Vision

Architecture design and functional specification ***(including security)*** → →

Milestone1
- Design (Business)
- **Design (Security)**
- Code (Business)
- **Code (Security)**
- Usability Unit Test
- **Security Unit Test**
- Synchronize (with overall source code repository)
- Frequent build (daily, weekly, etc.)
- Frequent Deployment
- Test **(include Security testing)**
- Debug
- Fix
- Resynchronize
- Redeploy
- Retest**(include Security testing)**
- Integrate
- Stabilize

Buffer time
Alpha Release

Milestone2
- Design (Business)
- **Design (Security)**
- Code (Business)
- **Code (Security)**
- Usability Unit Test
- **Security Unit Test**
- Synchronize (with overall source code repository)
- Frequent build (daily, weekly, etc.)
- Frequent Deployment
- Test **(include Security testing)**
- Debug
- Fix
- Resynchronize
- Redeploy
- Retest**(include Security testing)**
- Integrate
- Stabilize

Buffer time
Beta Release

Milestone3
- Design (Business)
- **Design (Security)**
- Code (Business)
- **Code (Security)**
- Usability Unit Test
- **Security Unit Test**
- Synchronize (with overall source code repository)
- Frequent build (daily, weekly, etc.)
- Frequent Deployment
- Test
- Debug
- Fix
- Resynchronize
- Redeploy
- Retest**(include Security testing)**
- Integrate
- Stabilize

Buffer time
Feature complete
Beta Release

Visual freeze

CODE COMPLETE
Final test**(include Security testing)**
Final Debug
Stabilize
FINAL RELEASE

Figure 29: Synch-and-Stabilize Process Model with Security [Based on Cusumano (2004), page 155]

Many organizations especially those in retail business have online stores in addition to brick and mortar stores. It is extremely important for these organizations to understand vulnerabilities in popular software such as web browsers (Refer Figure 30).

Author has identified following key criteria for effective software security management:

- Documented list of application vulnerabilities for technical staff to use when developing applications.

[38] Cusumao, Michael, 2004, The Business of Software: What Every Manager, Programmer, and Entrepreneur Must Know to Thrive and Survive in Good Times and Bad, ISBN 0-7432-1580-X, Publisher: Free Press (A division of Simon & Shuster, Inc.), New York

(*For example, OWASP top 10 software web applications vulnerabilities for web application developers*)

- Secured Software Development Lifecycle when building software product or service
- Security considerations when buying software product or service
- Regular software security patches and software upgrades

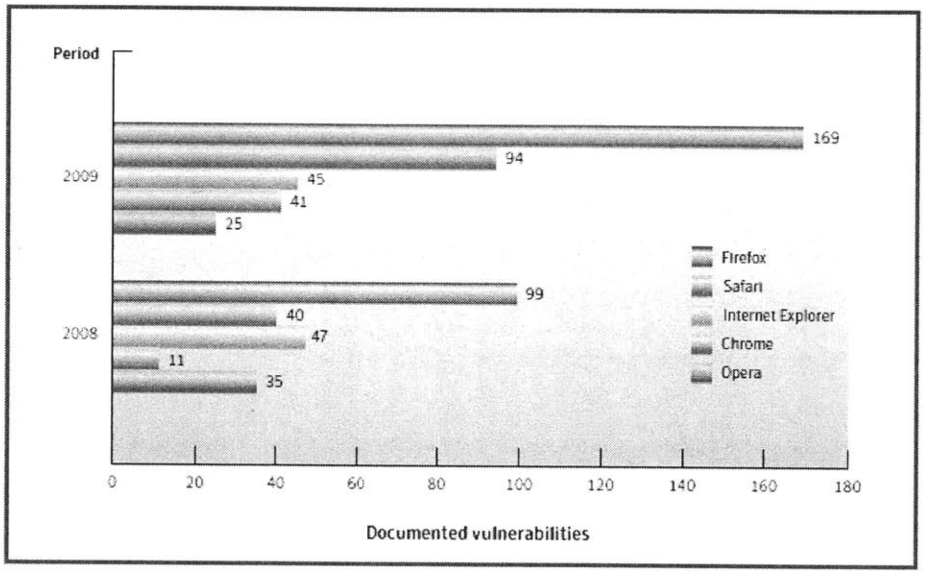
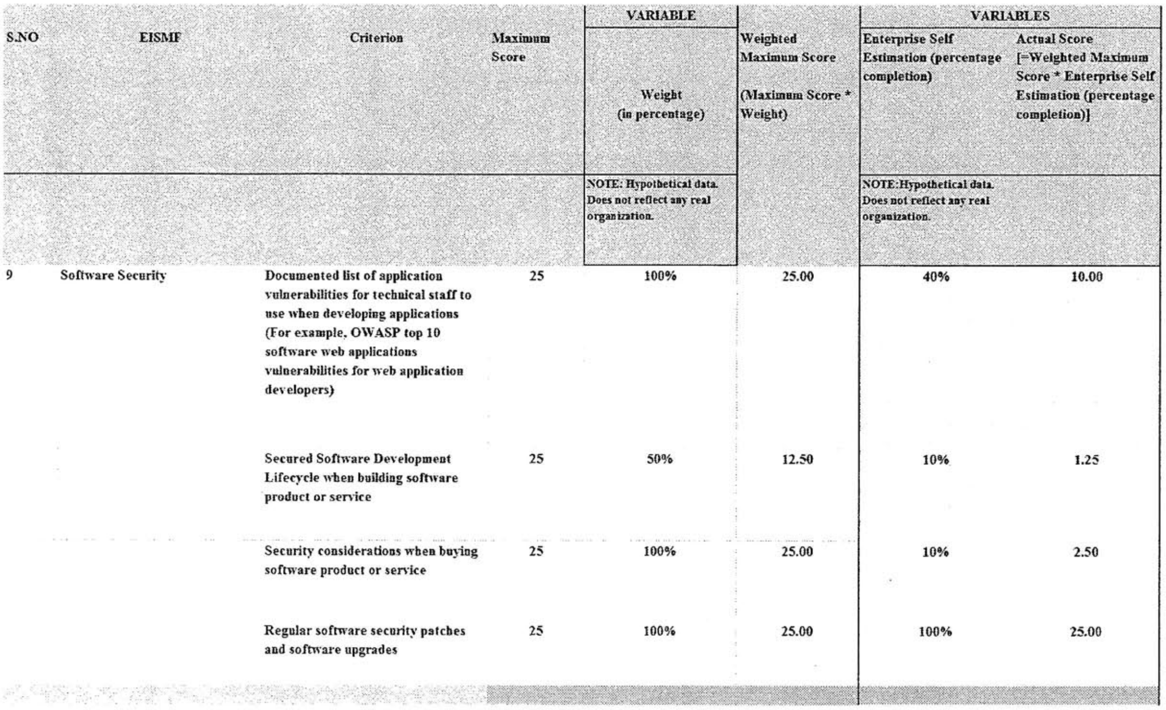


Figure 30: Web browser vulnerabilities (Source: Symantec[39])

Above criteria are shown in the Table 13 for Enterprise Information Security Maturity Level Calculations. Author views each of the above criteria as equally important for effective *software security* management in an organization. Therefore, each criterion carries 25 points so that sum of all the points under *software security* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 13.

[39] Symantec Corp. (2010), Symantec Global Internet Security Threat Report, Trends for 2009, Volume XV, Published April 2010, World Wide Web, Retrieved on October 06, 2010 from http://www.symantec.com/business/theme.jsp?themeid=threatreport



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score	VARIABLES	
				Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
9	Software Security	Documented list of application vulnerabilities for technical staff to use when developing applications (For example, OWASP top 10 software web applications vulnerabilities for web application developers)	25	100%	25.00	40%	10.00
		Secured Software Development Lifecycle when building software product or service	25	50%	12.50	10%	1.25
		Security considerations when buying software product or service	25	100%	25.00	10%	2.50
		Regular software security patches and software upgrades	25	100%	25.00	100%	25.00

Table 13: Enterprise Information Security Maturity Level Calculations – *Software Security*

Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.10 Identity Management and Access control

This is an area which deals with who can access a system and what an authenticated user is authorized to do within a system. For example, when we log into our bank account online, we can view only our account information and can perform certain transactions such as transfer money from debit account to pay off credit card debt. We cannot view some other persons account information. However, bank employee who takes our customer service call can view our account information and perform certain transactions on our account which we cannot perform on our own account such as roll back a transaction. Difference between two users is in authorization. Both users authenticate to the system using their own user id and password. Based on identity of the authenticated users, system looks for authorization. Authorization tells the system what a user can do after successful authentication. In our example above, bank employee who is a customer service agent has a different set of privileges attached to his or her user id which allows authenticated user to view other persons account information and perform certain transactions.

Currently, leading information technology companies such as Microsoft, Oracle, IBM and Novell, each have identity management solutions for organization to use. However, this is an active research area and work is going on for standardization of identity management. For example, The Open Group is "working jointly with the US InterNational Committee for Information Technology Standards (INCITS CS1), which serves as the US Technical Advisory Group to ISO/IEC JTC1, and also under Category C Liaison status directly with ISO JTC1 SC27, to develop an International Standard Framework for Identity Management"[40]. Similarly, International Telecommunication Union has an Identity Management Global Standards Initiative (or IdM-GSI). "IdM-GSI focuses on developing the detailed standards necessary for deployment of Identity management (IdM) capabilities that enables secure and trustworthy assertions about digital identities used in telecommunications, control networks, and a variety of service offerings. IdM-GSI harmonizes, in collaboration with other bodies, different approaches to IdM worldwide"[41].

Irrespective of whether an organization uses off the shelf identity management solution or develops one internally, following are the key criteria for effective identity management:

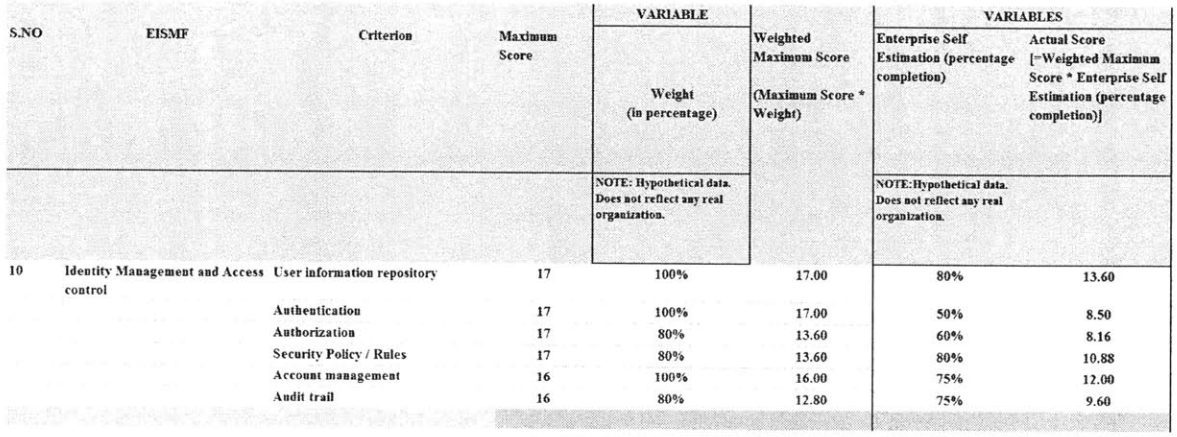
- User information repository
- Authentication
- Authorization
- Security Policy/Rules
- Account management

[40] The Open Group, Identity Management Forum, World Wide Web, Retrieved on October 06, 2010 from http://www.opengroup.org/tech/idm/

[41] International Telecommunication Union, Identity Management Global Standards Initiative, World Wide Web, Retrieved on October 06, 2010 from http://www.itu.int/en/ITU-T/gsi/idm/Pages/default.aspx

- Audit trail

Above criteria are shown in the Table 14 for Enterprise Information Security Maturity Level Calculations.



				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
10	Identity Management and Access control	User information repository	17	100%	17.00	80%	13.60
		Authentication	17	100%	17.00	50%	8.50
		Authorization	17	80%	13.60	60%	8.16
		Security Policy / Rules	17	80%	13.60	80%	10.88
		Account management	16	100%	16.00	75%	12.00
		Audit trail	16	80%	12.80	75%	9.60

Table 14: Enterprise Information Security Maturity Level Calculations – ***Identity Management and Access control***

Author views each of the above criteria as roughly equally important for effective *identity management and access control* in an organization. Therefore, each criterion carries either 16 or 17 points so that sum of all the points under *identity management and access control* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 14. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.11 Information Operations Management

This is relatively well developed area in terms of expertise. Several universities offer programs in information and operations management. This domain holds a very special place when it comes to information security management for an enterprise. In the information technology domain, threats are emerging and evolving very rapidly. Enterprise operations management people need to ensure that information security management operation run smoothly and inputs in terms of technology and expertise are converted into output in terms of information security.

Organizations can leverage standards such as ISO/IEC 27002:2005 which cover "communications and operations management"[42].Information operations management include estimation of existing information security related products and services which an organization currently have. It is followed by acquiring latest version of existing products and services or new products which show up in the market with a different value proposition. Change management helps smooth adoption of new versions of existing products / services as well as new products and services across the enterprise. It is vital that all information is completely backed up and tested for recovery. Author is personally been in a situation when recovery from a backup tape did not work! Hence, taking multiple backups is extremely important before existing products or services are upgraded. Finally, as we all know information security is a domain where changes happen at a very rapid pace. Existing products become obsolete very fast and needs to be retired in a safe manner with proper disposal. Note that disposal of information storage medium (for e.g., paper/ electronic) needs special techniques so that information stored on the medium is not readable by anyone. For example, paper needs to be shredded properly. In the United States, Department of Defense (DoD) has published DoD 5220.22-M-National Industrial Security Program Operating Manual (NISPOM) which describe destruction, degaussing (electronic storage medium such hard drive is exposed to magnetic force) and overwriting for sanitizing electronic storage medium such as hard drives.

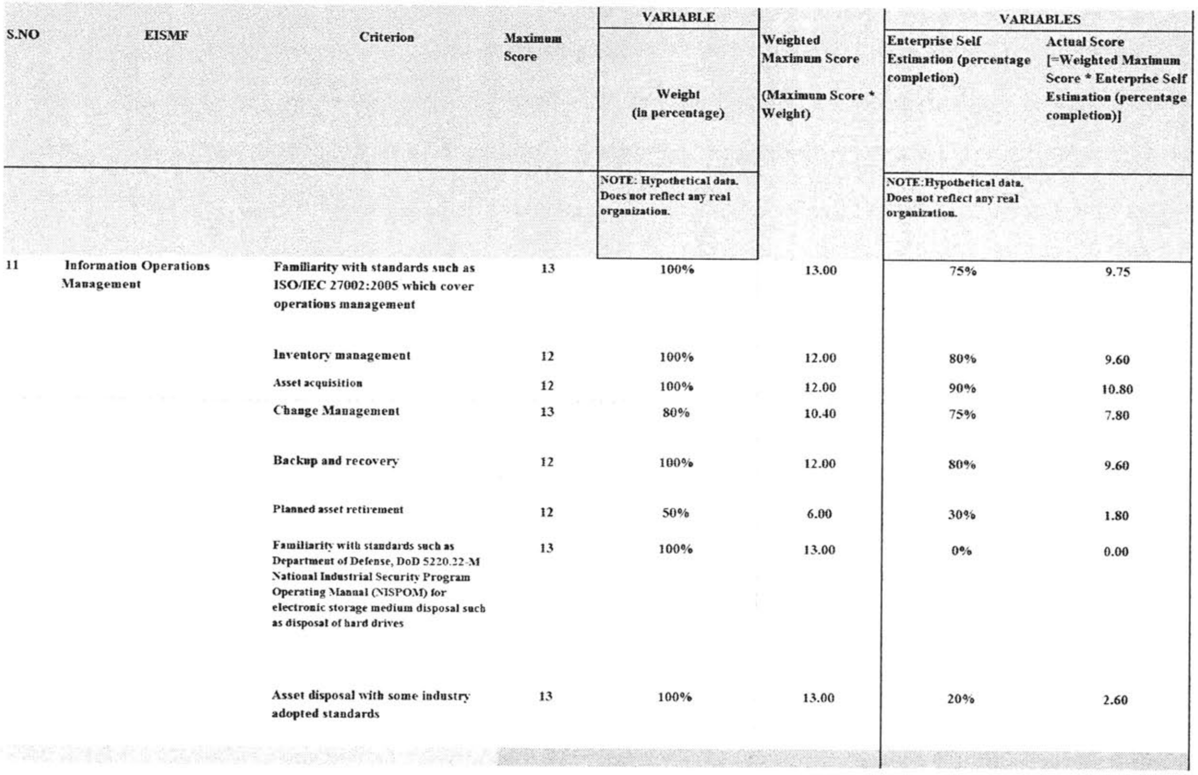
Author has identified following key criteria for effective information operations management:

- Familiarity with standards such as ISO/IEC 27002:2005 which cover operations management
- Inventory management
- Asset acquisition
- Change Management
- Backup and recovery

[42] International Organization for Standardization (ISO), ISO/IEC 27002:2005— Information technology -- Security techniques -- Code of practice for information security management , World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/catalogue_detail?csnumber=50297

- Planned asset retirement
- Familiarity with standards such as Department of Defense, DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) for electronic storage medium disposal such as disposal of hard drives
- Asset disposal with some industry adopted standards

Above criteria are shown in the Table 15 for Enterprise Information Security Maturity Level Calculations.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score	VARIABLES	
				Weight (in percentage)	(Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
11	Information Operations Management	Familiarity with standards such as ISO/IEC 27002:2005 which cover operations management	13	100%	13.00	75%	9.75
		Inventory management	12	100%	12.00	80%	9.60
		Asset acquisition	12	100%	12.00	90%	10.80
		Change Management	13	80%	10.40	75%	7.80
		Backup and recovery	12	100%	12.00	80%	9.60
		Planned asset retirement	12	50%	6.00	30%	1.80
		Familiarity with standards such as Department of Defense, DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) for electronic storage medium disposal such as disposal of hard drives	13	100%	13.00	0%	0.00
		Asset disposal with some industry adopted standards	13	100%	13.00	20%	2.60

Table 15: Enterprise Information Security Maturity Level Calculations – *Information Operations Management*

Author views each of the above criteria as roughly equally important for effective *information operations management* in an organization. Therefore, each criterion carries either 12 or 13 points so that sum of all the points under *information operations management* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 15. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.12 Assurance and Evaluation

Organizations may leverage framework such as COBIT (Control Objectives for Information and related Technology)[43] to implement an information *assurance* program across the enterprise. For information security *evaluation,* framework such as OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)[44] may be used. ISO/IEC 15408-1:2009[45], ISO/IEC 15408-2:2008[46], and ISO/IEC 15408-3:2008[47] are a set of related standards which cover both evaluation and assurance. These frameworks and standards can tremendously help organizations to design an information security assurance and evaluation program for their specific needs.

Author has identified following key criteria for effective assurance and evaluation:

- Standardized or frameworks based approach for information assurance and evaluation (For example, use of ISO/IEC 15408, CMMI, COBIT, OCTAVE)
- Rigorous testing

[43] Information Systems Audit and Control Association (ISACA) ."COBIT" World Wide Web, Retrieved October 11, 2010 from http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[44] Carnegie Mellon University Computer Emergency Response Team.(CERT), "OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation)" World Wide Web, Retrieved October 11,2010 from http://www.cert.org/octave/

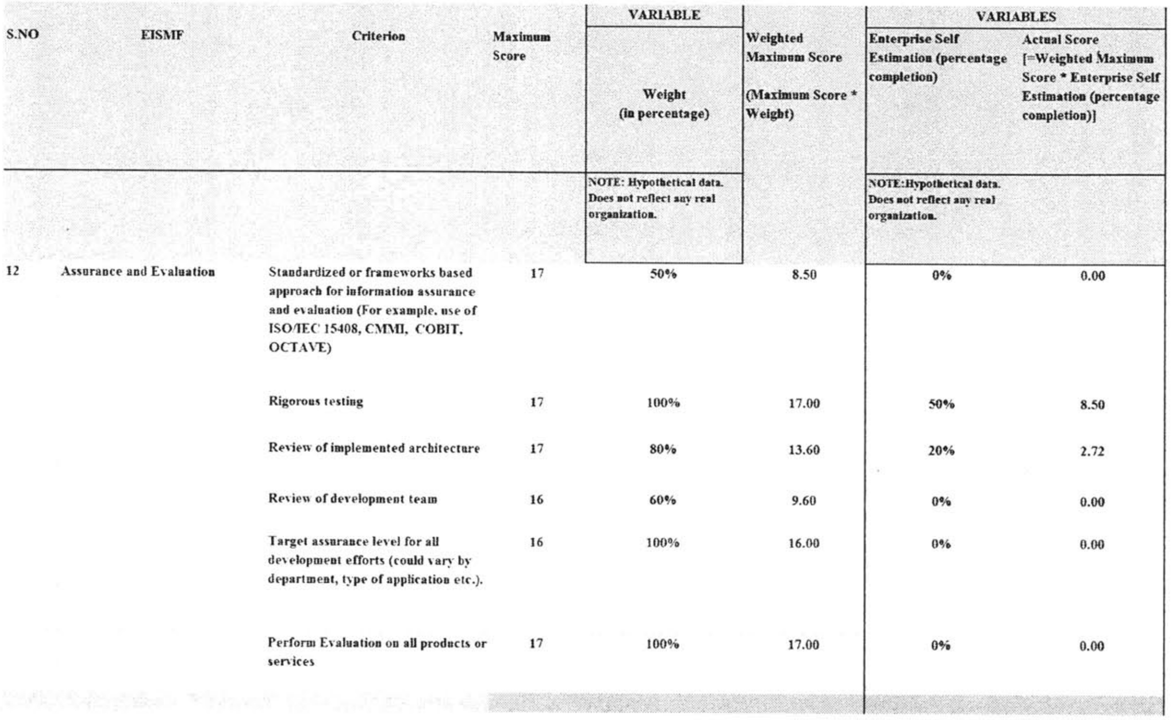
[45] International Organization for Standardization (ISO), "ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341

[46] International Organization for Standardization (ISO), "ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414

[47] International Organization for Standardization (ISO), "ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46413

- Review of implemented architecture
- Review of development team
- Target assurance level for all development efforts (could vary by department, type of application etc.).
- Perform Evaluation on all products or services

Above criteria are shown in the Table 16 for Enterprise Information Security Maturity Level Calculations.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score (Maximum Score * Weight)	VARIABLES	
				Weight (in percentage)		Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
12	Assurance and Evaluation	Standardized or frameworks based approach for information assurance and evaluation (For example, use of ISO/IEC 15408, CMMI, COBIT, OCTAVE)	17	50%	8.50	0%	0.00
		Rigorous testing	17	100%	17.00	50%	8.50
		Review of implemented architecture	17	80%	13.60	20%	2.72
		Review of development team	16	60%	9.60	0%	0.00
		Target assurance level for all development efforts (could vary by department, type of application etc.).	16	100%	16.00	0%	0.00
		Perform Evaluation on all products or services	17	100%	17.00	0%	0.00

Table 16: Enterprise Information Security Maturity Level Calculations – ***Assurance and Evaluation***

Author views each of the above criteria as roughly equally important for effective *assurance and evaluation* in an organization. Therefore, each criterion carries either 16 or 17 points so that sum of all the points under *assurance and evaluation* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 16. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.13 Incident Management

Organizations should have a comprehensive information security incident management program to take care of information security breach. National Institute of Standards and Technology (NIST) has a special publication - SP 800-61 Rev. 1("Computer Security Incident Handling Guide")[48] that provides a great starting point to organizations to develop a customized information security incident management program. ISO/IEC TR 18044:2004 ("Information technology -- Security techniques -- Information security incident management") is another standard that covers information security incident management.

Organizations should have a prevention / detection mechanism in place. It should be a combination of technical and personal communication system. Technical system could be intrusion prevention and detection software. Personal communication system could include a way for employees to report an incident such as telephone number to call or submit incident using organization intranet based web portal or an email address dedicated for reporting information security incidents. CISO or equivalent person should have a incident response team already in place. External and internal communications should be handled with care. Pre-planning helps!

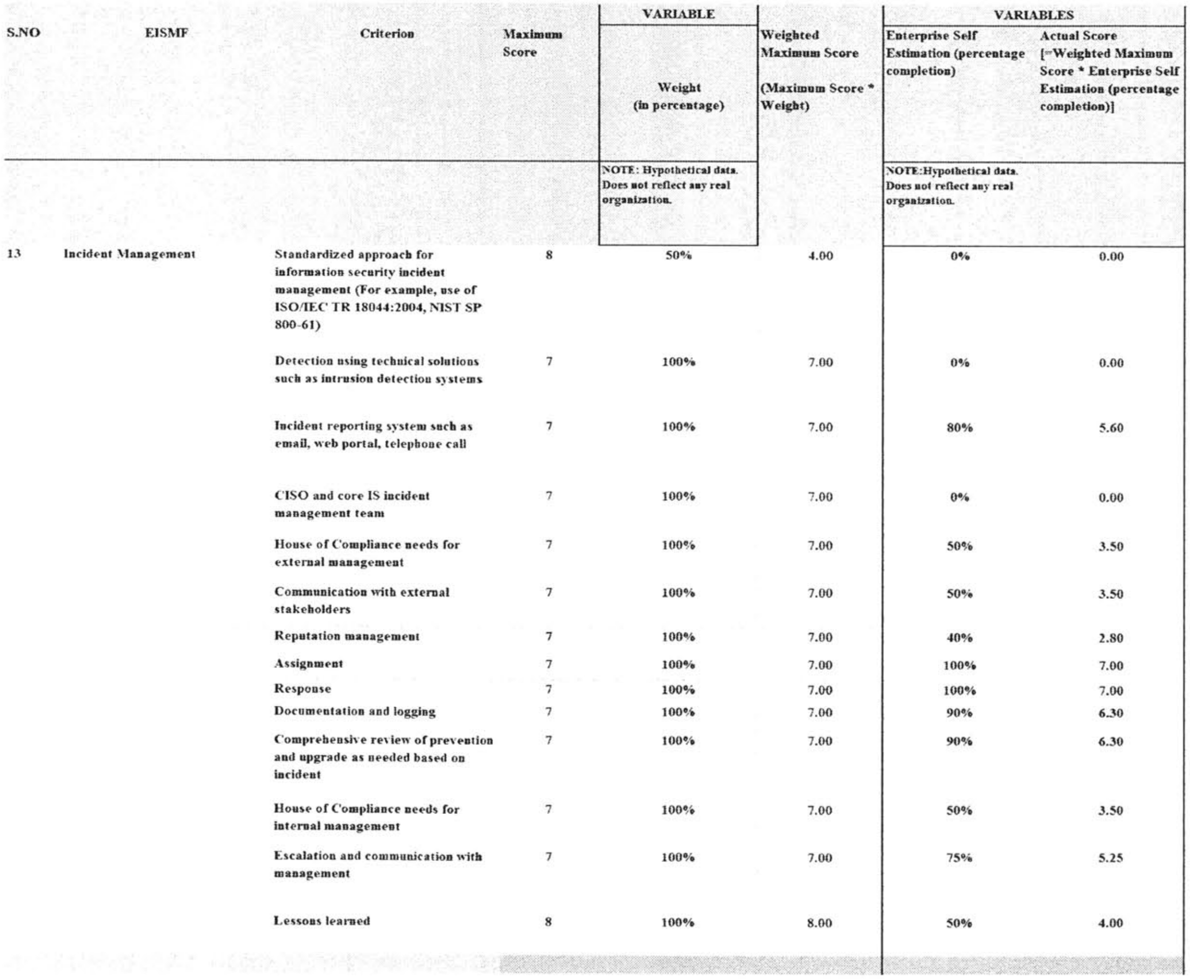
Author has identified following key criteria for effective incident management:

- Standardized approach for information security incident management (For example, use of ISO/IEC TR 18044:2004, NIST SP 800-61)
- Detection using technical solutions such as intrusion detection systems
- Incident reporting system such as email, web portal, telephone call
- CISO and core IS incident management team
- House of Compliance needs for external management

[48] National Institute of Standards and Technology (NIST), SP 800-61 Rev. 1(Computer Security Incident Handling Guide), World Wide Web, Retrieved on October 11, 2010 from http://csrc.nist.gov/publications/PubsSPs.html

- Communication with external stakeholders
- Reputation / brand management
- Assignment
- Response
- Documentation and logging
- Comprehensive review of prevention and upgrade as needed based on incident
- House of Compliance needs for internal management
- Escalation and communication with management
- Lessons learned

Above criteria are shown in the Table 17 for Enterprise Information Security Maturity Level Calculations.



				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
13	Incident Management	Standardized approach for information security incident management (For example, use of ISO/IEC TR 18044:2004, NIST SP 800-61)	8	50%	4.00	0%	0.00
		Detection using technical solutions such as intrusion detection systems	7	100%	7.00	0%	0.00
		Incident reporting system such as email, web portal, telephone call	7	100%	7.00	80%	5.60
		CISO and core IS incident management team	7	100%	7.00	0%	0.00
		House of Compliance needs for external management	7	100%	7.00	50%	3.50
		Communication with external stakeholders	7	100%	7.00	50%	3.50
		Reputation management	7	100%	7.00	40%	2.80
		Assignment	7	100%	7.00	100%	7.00
		Response	7	100%	7.00	100%	7.00
		Documentation and logging	7	100%	7.00	90%	6.30
		Comprehensive review of prevention and upgrade as needed based on incident	7	100%	7.00	90%	6.30
		House of Compliance needs for internal management	7	100%	7.00	50%	3.50
		Escalation and communication with management	7	100%	7.00	75%	5.25
		Lessons learned	8	100%	8.00	50%	4.00

Table 17: Enterprise Information Security Maturity Level Calculations – *Incident Management*

Author views each of the above criteria as roughly equally important for effective *incident management* in an organization. Therefore, each criterion carries either 7 or 8 points so that sum of all the points under *incident management* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 17. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

4.14 Future Planning

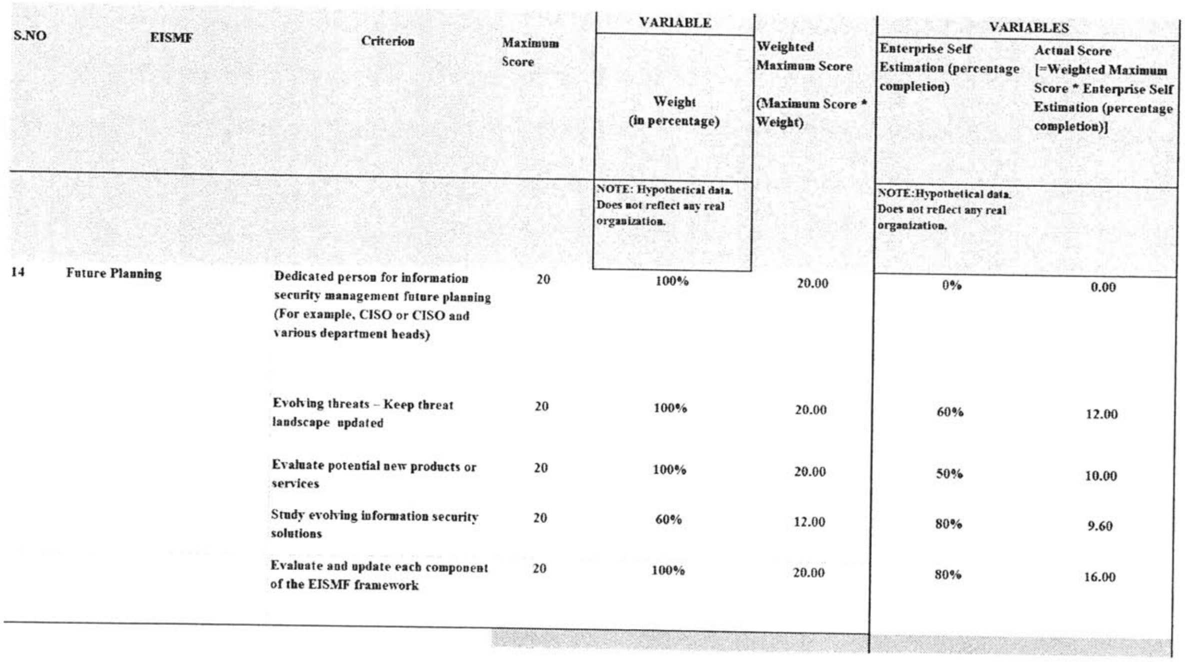
Information security threats keep evolving at a very rapid pace. It is an ongoing battle to mitigate the effects of information security threats. Therefore, it is extremely important to have a formal process in place for analyzing future information security needs. This includes a dedicated person for future planning especially for large organizations. For smaller organizations, some percentage of CISO or equivalent persons' time should be spent on evaluating options for the future. It could be based on strategic direction of the company especially on the technology side. For example, if a company is planning to move to internet based web applications from current client server applications in next two years, it is important for CISO or equivalent person to start analyzing what is needed to secure the web applications for ensuring information security. Information threat landscape (*see Figure 17*) that we developed as part of Policy and Procedures needs to be constantly updated. New information security products and services keep showing up in the market which different parts of organizations might want to use. Each such new product or service brings in a new set of information security challenges which should be evaluated as part of purchase evaluation. As part of future planning, applicable new information security products or services should be evaluated as well. Finally, when using EISMF it is recommended that organizations should evaluate and add more criteria as needed for their specific needs.

- Dedicated person for information security management future planning (For example, CISO or CISO and various department heads)

- Evolving threats – Keep threat landscape updated
- Evaluate potential new products or services
- Study evolving information security solutions
- Evaluate and update each component of the EISMF framework

Author views each of the above criteria as equally important for effective *future planning* in an organization. Therefore, each criterion carries 20 points so that sum of all the points under *future planning* is 100 points. However, enterprise may weigh each criterion differently as shown in Weight column in Table 18. Weighted Maximum Score is calculated by multiplying Maximum Score and Weight. Enterprise using EISMF needs to estimate to what extent they fulfill each criterion and record this estimation in Enterprise Self Estimate column. Finally, Actual Score for each criterion is calculated by multiplying Weighted Maximum Score and Enterprise Self Estimation.

Above criteria are shown in the Table 18 for Enterprise Information Security Maturity Level Calculations.



S.NO	EISMF	Criterion	Maximum Score	VARIABLE		VARIABLES	
				Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
14	Future Planning	Dedicated person for information security management future planning (For example, CISO or CISO and various department heads)	20	100%	20.00	0%	0.00
		Evolving threats – Keep threat landscape updated	20	100%	20.00	60%	12.00
		Evaluate potential new products or services	20	100%	20.00	50%	10.00
		Study evolving information security solutions	20	60%	12.00	80%	9.60
		Evaluate and update each component of the EISMF framework	20	100%	20.00	80%	16.00

Table 18: Enterprise Information Security Maturity Level Calculations – *Future Planning*

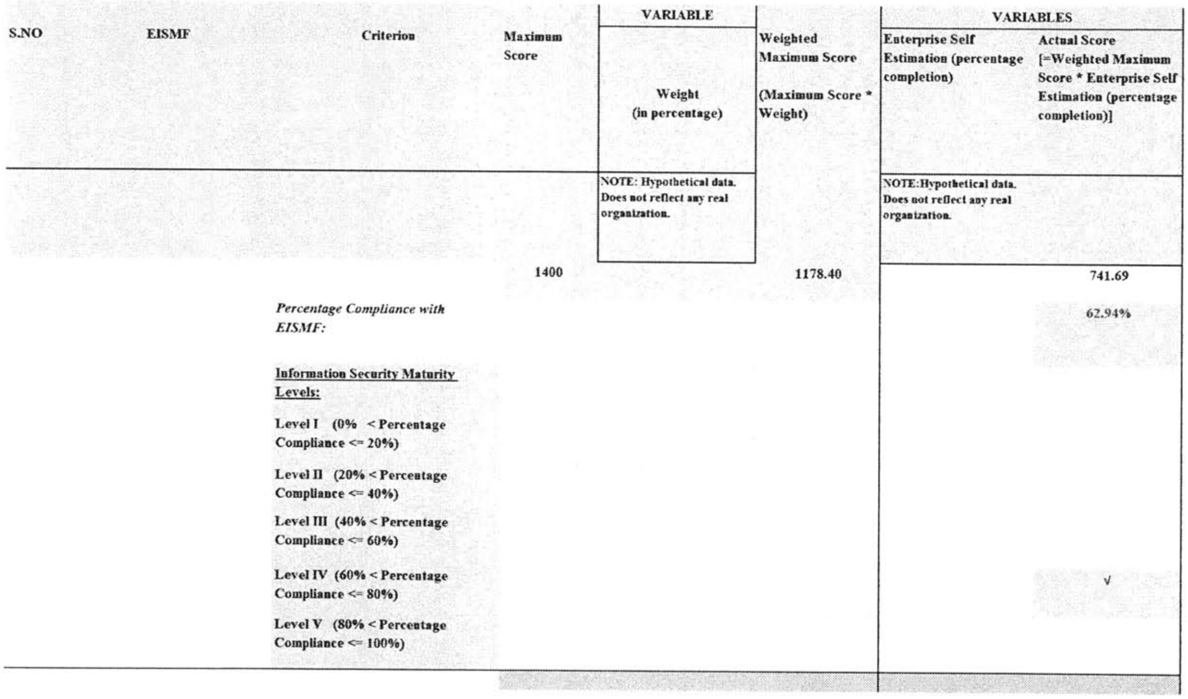
4.15 Maturity Level Calculations

Once we have established weight, calculated weighted maximum score, agreed on enterprise self estimation (percentage completion), and calculated actual score for each criterion, the final step is to calculate maturity level as follows:

- To compute percentage compliance with EISMF, we sum the Weighted Maximum Score and Actual Score separately. Percentage compliance is calculated as follows:

  Percentage Compliance = [Σ (Actual Score) /Σ (Weighted Maximum Score)]*100

  *For our sample scenario, sum of actual score is 741.69 and sum of weighted maximum score is 1178.40. Percentage compliance with EISMF is calculated as (741.69/1178.40)*100 ~ 62.94% [Refer Table 19]*



				VARIABLE		VARIABLES	
S.NO	**EISMF**	**Criterion**	**Maximum Score**	**Weight (in percentage)**	**Weighted Maximum Score** **(Maximum Score * Weight)**	**Enterprise Self Estimation (percentage completion)**	**Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]**
				NOTE: Hypothetical data. Does not reflect any real organization.		**NOTE:Hypothetical data. Does not reflect any real organization.**	
			1400		**1178.40**		**741.69**
		Percentage Compliance with EISMF:					**62.94%**
		<u>Information Security Maturity Levels:</u>					
		Level I (0% < Percentage Compliance <= 20%)					
		Level II (20% < Percentage Compliance <= 40%)					
		Level III (40% < Percentage Compliance <= 60%)					
		Level IV (60% < Percentage Compliance <= 80%)					√
		Level V (80% < Percentage Compliance <= 100%)					

Table 19: Enterprise Information Security Maturity Level Calculations – *Establish Maturity Level*

Refer Appendix I for complete information security management maturity level calculations worksheet.

- After calculating percentage compliance, information security management maturity levels are determined as follows
    - Level I : 0% < Percentage Compliance <= 20%
    - Level II : 20% < Percentage Compliance <= 40%
    - Level III : 40% < Percentage Compliance <= 60%
    - Level IV : 60% < Percentage Compliance <= 80%
    - Level V : 80% < Percentage Compliance <= 100%

  Maturity level for our example organization is Level IV because 62.94% falls between 60% and 80% [Refer Table 19].

In the next chapter, author compares progress made so far with the objectives outlined in the beginning of this document. Author made certain assumptions that open up new research areas. Potential future research work is outlined in the next chapter as well.

CHAPTER 5: Conclusion and Future Work

We started with three key objectives for this thesis. Below we see how met our stated objectives.

1. Comprehensive approach towards information security management and maturity level:

We wanted a comprehensive approach towards information security management. The fourteen point framework termed Enterprise Information Security Management Framework (EISMF) described in Chapter 3 fulfills this objective. EISMF emphasizes careful planning by top management and involves all employees to make information security management a success with in an enterprise. CISO or equivalent person dedicated 100% towards overall information security management is a key management resource who not only understands technological side of information security but also understands overall enterprise business objectives. Information security management goals are aligned with enterprise business objectives. CISO or equivalent person is responsible for creating a culture of information security driven business process development.

Once, we have clear understanding of enterprise business and information security goal, house of compliance is needed. House of compliance stresses importance of complying with applicable laws and legislations. Organizations should leverage existing standards, frameworks and best practices while complying with the applicable laws. Effort should be made to customize standards, frameworks and best practices to suit an individual organization's specific needs.

Next is development of an enterprise information security policy. This helps all employees across departments to have a common understanding of enterprise information security objectives and how employees could contribute to make information security management a success. There are several drivers which influence information security policy such as type of business, enterprise business strategy and information security concerns, house of compliance, threat landscape, contractual, prevention, recovery, management expectations, and stakeholder concerns. Certain key procedures should be clearly stated upfront such as regular backup of information, regular testing, internal and external communication when an information security breach occurs, etc.

Clear risk management approach is stressed. Organizations could either develop their own custom risk management process or leverage standard such as NIST Special Publication 800-30-"Risk Management Guide for Information Technology Systems". The idea is consider information security risks before buying or building any product or service. When purchasing a product or service, information security risks must be important part of the legal contract. Risk management approach should start with clear understanding of the context under which it is carried out as well as completely aligned with house of compliance. Quantitative or qualitative risk assessment methodologies could be adopted. Some organizations may choose to go with both and compare the results. Eventually, a risk mitigation plan should be created, implemented, continuously monitored and updated. Management should be aware of all the risks to information, mitigation plan and its implementation.

Employee awareness and training is where all the employees whether technical or otherwise get a chance to make a significant contribution towards information security management. Organizations should have a very structured employee awareness and training program geared towards information security. This program should not be a one-time affair such as only at recruitment. Employee awareness is a continuous process and employee training should be carried out at regular time intervals such as every six months or once a year. Standards such as NIST Special Publication 800-16 ("Information Technology Security Training Requirements: A Role- and Performance-Based Model") and NIST Special Publication 800-50 ("Building an Information Technology Security Awareness and Training Program") are available to help organizations build and implement an effective employee awareness and training program.

Personnel security is critical so that no one other than authorized personnel should be able to enter an organization premises. Organizations should keep a regularly updated checklist for personnel security which should include checks such as identity cards, background check on all persons who work for the organizations including full time employees, part time employees, and contractors, appropriate system access to all personnel, etc.

Physical security covers protection against physical threats to information assets. Natural disaster, human factors and other reasons could pose serious threats. For example, earthquake, lightening, flood, human mistakes, theft etc. A well planned proactive approach could save organizations from severe consequences of large scale losses.

Network security is the backbone of technological side of information security. This is an area where highly skilled professionals are needed. Either an exclusive security policy dedicated towards network security should be put in place or a section of enterprise information security policy must be dedicated to network security. A series of steps are needed for ensuring network security. Organizations would find use of checklists to be extremely useful for network security. Physical access to all network devices must be restricted, software patches must be applied as per vendor recommendations, high strength passwords must be used, never keep default system passwords – always change them, use encryption, monitor all systems and keep audit trail, etc.

Software security is an area where software development cycle should involve information security considerations at each stage. Programmers should be familiar with software vulnerabilities such as OWASP Top Ten vulnerabilities. When buying commercial off the shelf products, organizations should make sure to cover the information security aspect and include information security aspect in the contractual agreement. Software architects should lay out software design, architecture and development best practices for various teams to use within an organization.

Identity management and access control is another technological method for enforcing information security in the information technology systems. Identity of the user is established through a process called authentication using username-password combination, retina scan, digital certificate, etc. After successful authentication, authorization process kicks in which uses previously stored rules for letting authenticated user do certain things within the system. It is imperative that all successful and failed attempts are logged with details on what user did so that organizations have a complete audit trail. Audit trail may be required for house of compliance reasons especially legal.

Efficient information operations management should facilitate smooth transition to newer information security technologies as well as safe and planned retirement of existing ones. Key components for efficient information operations management include asset acquisition and inventory management, change management, backup and recovery, and asset retirement and disposal.

Organizations should set an information security assurance goal. Assurance process should include rigorous system testing, review of system architecture, and review of programmers' technical background. Standards such as ISO/IEC 15408, CMMI, or ISO 9001 may be leveraged for both assurance and evaluation. Evaluation is the process of checking whether assurance goal was met.

Information security incident management is an area where CISO or equivalent person should create a customized incident management plan. Standard such as ISO/IEC TR 18044:2004 could be leveraged. Effort should be made to approach incident management from compliance, technological, management and learning perspective.

CISO or equivalent person along with a team from various departments should be involved in the future planning for overall information security management. Organizations should study evolving threats and upcoming information security technologies. Potential products and services should be studied for possible information security threats. All components of EISMF should be updated.

Organizations may use information security management maturity level estimation to track progress made in meeting requirements described in EISMF.

2. *Role of senior management, alignment of information security and enterprise objectives, and role of all employees*

   We saw that senior management is a key player in the overall information security management. CISO or equivalent is a senior management person who thoroughly understands enterprise objectives and creates information security objectives at an enterprise level. CISO or equivalent person is a key player in EISMF. Employee awareness and training stresses that all employees can contribute towards information security by understanding common threats such as phishing, social engineering, understanding internet browser privacy settings, etc. Employees should report any suspicious activity anywhere inside or in the immediate vicinity of the office building. EISMF brings out the role of senior management, stresses laying out enterprise information security objectives based on overall enterprise objectives, and role of all employees.

3. *Holistic framework to address technological, business, and social aspects of information security*

EISMF clearly illustrates that information security is not just about technical challenges but it has significant management and social aspects as well. Management needs to hire a dedicated information security management person, ensure compliance with applicable laws, create an enterprise information security policy, develop risk management process, ensure personal and physical security, hire skilled technical people for network and software security, put process in place for information operations management, carefully develop incident management process and continuously think about the future threats and prevention. Information security incidents are a major social concern. Some laws require organizations to inform persons whose personal information is accessed by unauthorized persons. For example, SB 1386[49] is one such law in the state of California.

EISMF takes a *systems approach* towards information security management and provides senior management with a holistic picture of how different pieces fit. Information security management maturity level was developed to provide a way to track progress and compliance with EISMF. However, *author made certain assumptions which opens up new research areas as explained below.*

- Each point in the fourteen point framework was given one hundred points so that total points for EISMF are fourteen hundred. More research is needed to determine whether we can have variable points for different points in EISMF. For example, house of compliance may have different total points from policy and procedures. Extensive interviews from organizations across many industries may help estimate this distribution. This can change the total points from fourteen hundred to a different value.

[49] California State Government, —SB 1386, Retrieved on October 13, 2010 from http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

- Each component or point in the fourteen point EISMF was divided into various criteria and each criterion had approximately equal points. More research is needed to come up with distribution of points for various criteria. This distribution could be based on extensive field research such as conducting interviews with management and technical personnel from several different organizations across multiple industries combined with rigorous mathematical analysis

- Apart from distribution of points among various criteria, more research is needed to help organizations to come up with self estimated percentage completion values for different criteria. Research could focus on various standard mathematical distributions such as Binomial distribution, Poisson distribution, Beta distribution, etc. and calculate mean value for reporting percentages.

- It would help organizations to have a standard way for gathering data from various stakeholders for various criteria by dividing each criterion into sub-criterion. For example, House of Compliance has four criteria- Laws/Regulations, Standards, Frameworks, and Best Practices. To come up percentages for each one of the criteria, per the current assumptions, interviews should be conducted and average percentage reported here. If management finds a large discrepancy, action needs to be taken to resolve differences and report agreed upon percentage. In contrast, it would make things much clearer for stakeholders, if through more research we are able to break down each criterion in sub-criterion and create guidelines to help concerned persons report their percentage estimation. Afterwards, an algorithm based on appropriate mathematical distribution calculates mean percentage for reporting purpose.

- Through extensive field work and research, benchmarks should be created to show where an organization stands within industry with regards to different criterion. For example, it would be useful to know how many organizations (expressed as percentage) within a certain industry have official Enterprise Information Security Policy. This would help organizations within that industry to catch up with other organizations and implement an Enterprise Information Security Policy.

- Future research may help determine critical organization size when a dedicated information security management person such as CISO is absolutely essential for information security management.

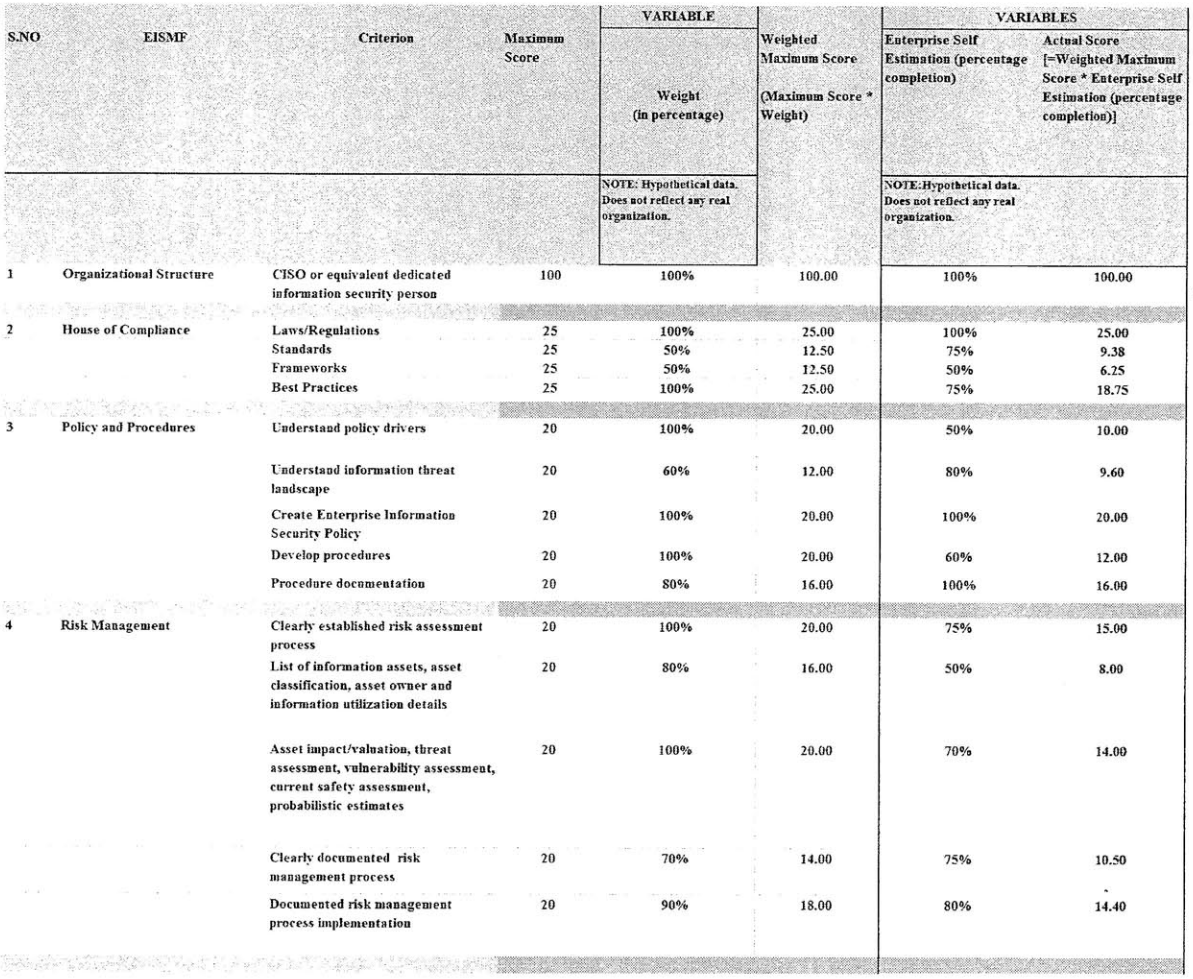
- Weights may vary depending on type of business and data, size of organization, and geographical location due to differences in criterion such as regulatory and privacy laws or for other reasons. It may be helpful to put together certain guidelines based on industry data to help organizations come up with weight for each criterion.

- It would be extremely useful to create a user interface such as an intranet web portal within an organization or commercial off the shelf software product called – Enterprise Information Security Management Dashboard. This web portal would report final compliance level as well as show where an organization stands with regards to each one of the fourteen points. Authorized users would drill down under each point to view/edit data for various criterion and possible sub-criterion. All computations are completed behind the scenes using programming logic. Such a dashboard would immediately bring management's attention towards areas which need improvement. This would be of immense value for information security budget and resource planning.

As we saw above, there are few research opportunities that could be explored in the future. Nevertheless, author believes that existing framework as described in this thesis would be greatly helpful to organizations in planning, estimation, development and implementation of an enterprise level information security roadmap for both strategic and tactical purposes. It gives both breadth and depth of work involved and brings all employees including senior management together to collectively contribute towards information security management.

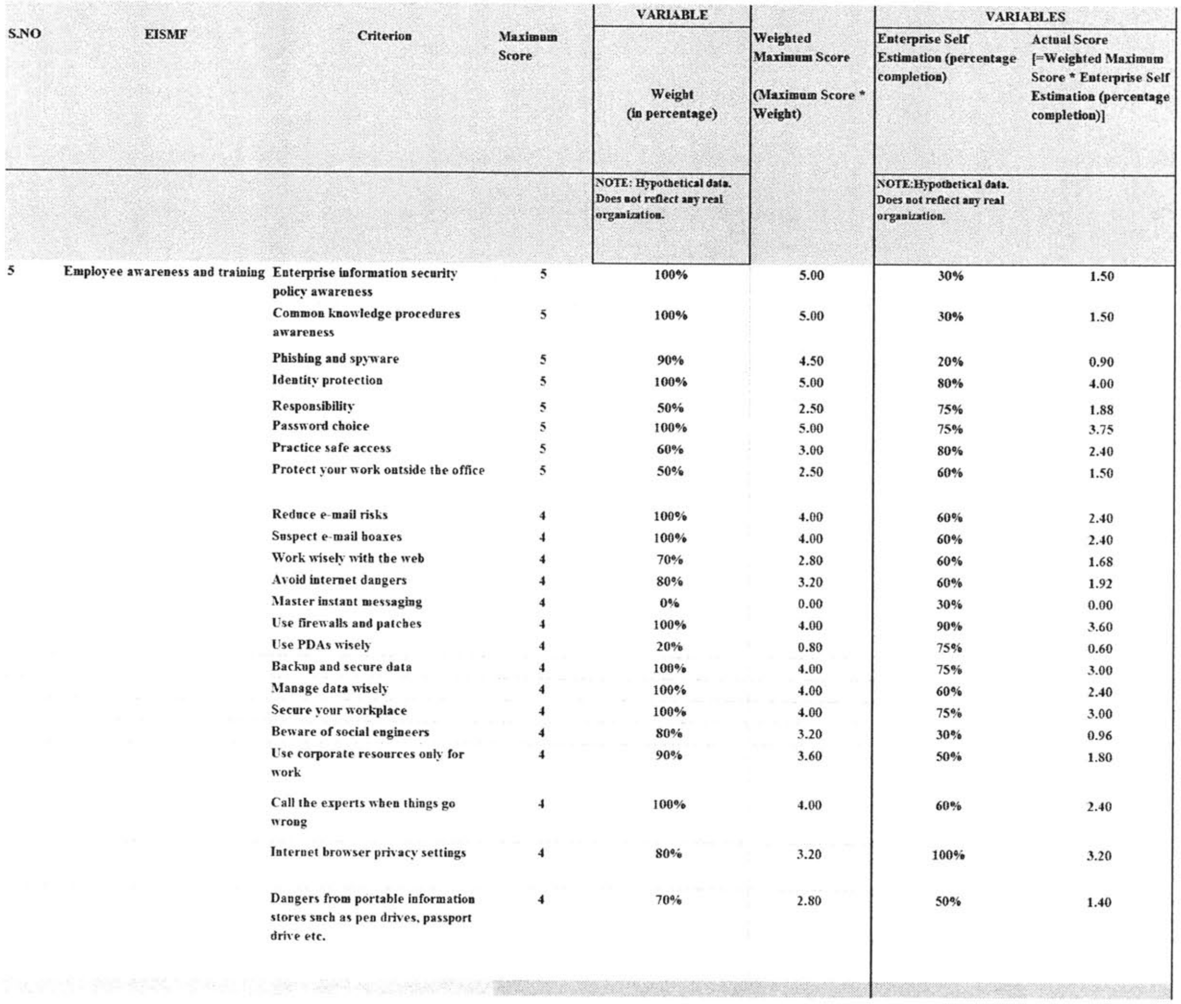
Appendix I: Complete worksheet for information security management maturity level calculations

Disclaimer: *Please note that in Enterprise Information Security Maturity Level Calculations, data shown under columns - Weight (in percentage) and Enterprise Self Estimation (percentage completion) is purely hypothetical. It was NOT obtained from any organization. Any match with any organization is purely coincidental.*



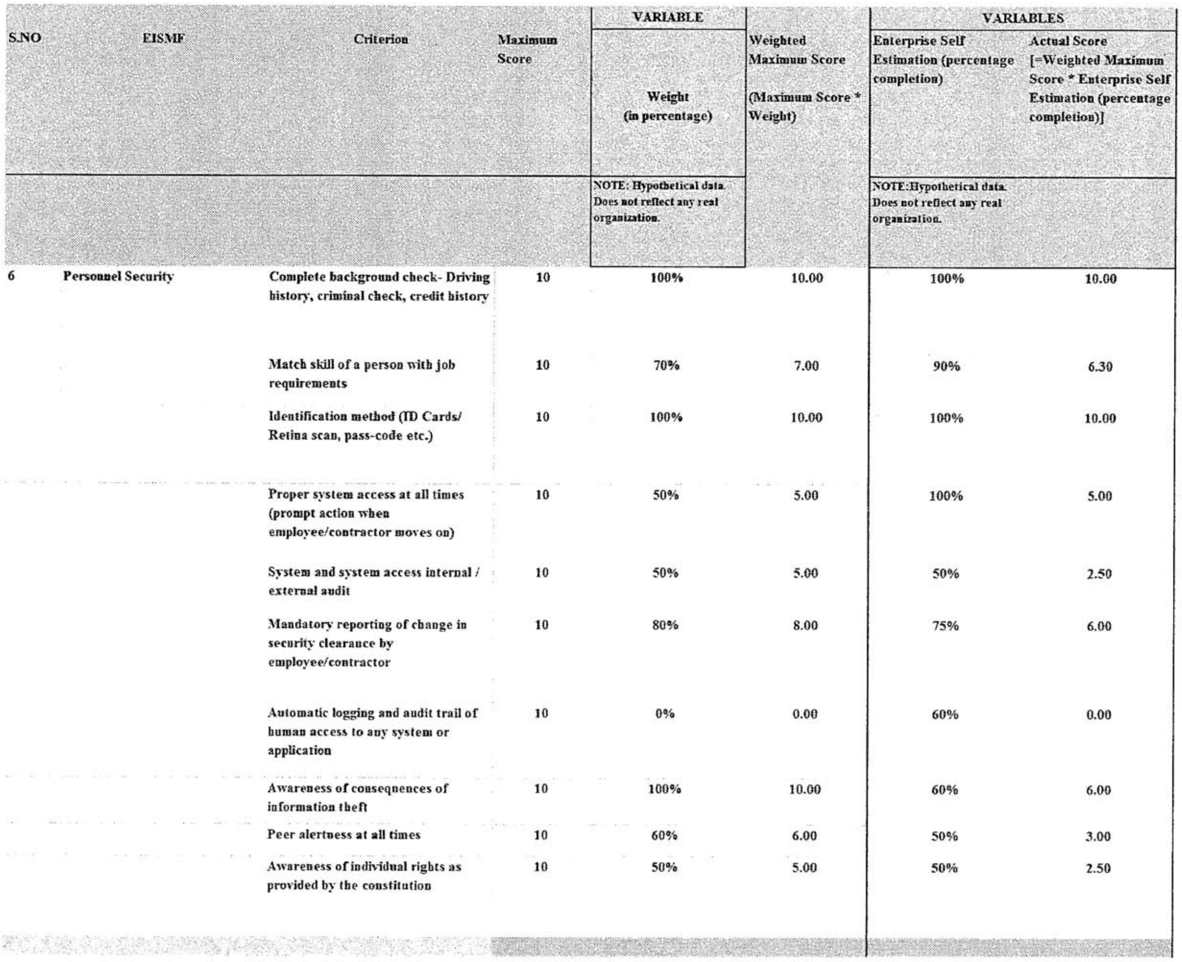
				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
1	Organizational Structure	CISO or equivalent dedicated information security person	100	100%	100.00	100%	100.00
2	House of Compliance	Laws/Regulations	25	100%	25.00	100%	25.00
		Standards	25	50%	12.50	75%	9.38
		Frameworks	25	50%	12.50	50%	6.25
		Best Practices	25	100%	25.00	75%	18.75
3	Policy and Procedures	Understand policy drivers	20	100%	20.00	50%	10.00
		Understand information threat landscape	20	60%	12.00	80%	9.60
		Create Enterprise Information Security Policy	20	100%	20.00	100%	20.00
		Develop procedures	20	100%	20.00	60%	12.00
		Procedure documentation	20	80%	16.00	100%	16.00
4	Risk Management	Clearly established risk assessment process	20	100%	20.00	75%	15.00
		List of information assets, asset classification, asset owner and information utilization details	20	80%	16.00	50%	8.00
		Asset impact/valuation, threat assessment, vulnerability assessment, current safety assessment, probabilistic estimates	20	100%	20.00	70%	14.00
		Clearly documented risk management process	20	70%	14.00	75%	10.50
		Documented risk management process implementation	20	90%	18.00	80%	14.40

Table is continued below:



S.NO	EISMF	Criterion	Maximum Score	VARIABLE		VARIABLES	
				Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
5	Employee awareness and training	Enterprise information security policy awareness	5	100%	5.00	30%	1.50
		Common knowledge procedures awareness	5	100%	5.00	30%	1.50
		Phishing and spyware	5	90%	4.50	20%	0.90
		Identity protection	5	100%	5.00	80%	4.00
		Responsibility	5	50%	2.50	75%	1.88
		Password choice	5	100%	5.00	75%	3.75
		Practice safe access	5	60%	3.00	80%	2.40
		Protect your work outside the office	5	50%	2.50	60%	1.50
		Reduce e-mail risks	4	100%	4.00	60%	2.40
		Suspect e-mail hoaxes	4	100%	4.00	60%	2.40
		Work wisely with the web	4	70%	2.80	60%	1.68
		Avoid internet dangers	4	80%	3.20	60%	1.92
		Master instant messaging	4	0%	0.00	30%	0.00
		Use firewalls and patches	4	100%	4.00	90%	3.60
		Use PDAs wisely	4	20%	0.80	75%	0.60
		Backup and secure data	4	100%	4.00	75%	3.00
		Manage data wisely	4	100%	4.00	60%	2.40
		Secure your workplace	4	100%	4.00	75%	3.00
		Beware of social engineers	4	80%	3.20	30%	0.96
		Use corporate resources only for work	4	90%	3.60	50%	1.80
		Call the experts when things go wrong	4	100%	4.00	60%	2.40
		Internet browser privacy settings	4	80%	3.20	100%	3.20
		Dangers from portable information stores such as pen drives, passport drive etc.	4	70%	2.80	50%	1.40

Table is continued below:

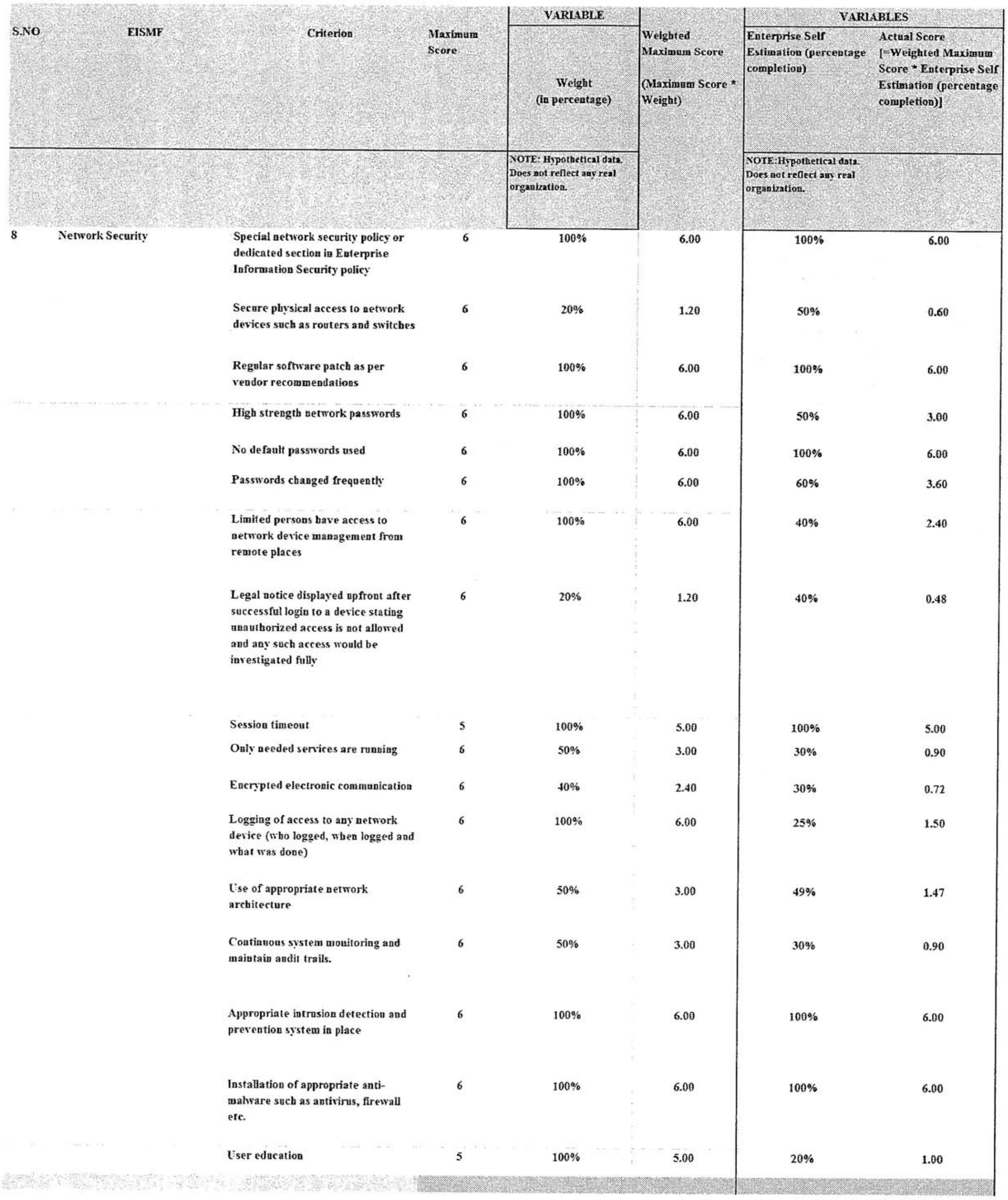


				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
6	Personnel Security	Complete background check- Driving history, criminal check, credit history	10	100%	10.00	100%	10.00
		Match skill of a person with job requirements	10	70%	7.00	90%	6.30
		Identification method (ID Cards/ Retina scan, pass-code etc.)	10	100%	10.00	100%	10.00
		Proper system access at all times (prompt action when employee/contractor moves on)	10	50%	5.00	100%	5.00
		System and system access internal / external audit	10	50%	5.00	50%	2.50
		Mandatory reporting of change in security clearance by employee/contractor	10	80%	8.00	75%	6.00
		Automatic logging and audit trail of human access to any system or application	10	0%	0.00	60%	0.00
		Awareness of conseqnences of information theft	10	100%	10.00	60%	6.00
		Peer alertness at all times	10	60%	6.00	50%	3.00
		Awareness of individual rights as provided by the constitution	10	50%	5.00	50%	2.50

Table is continued below:

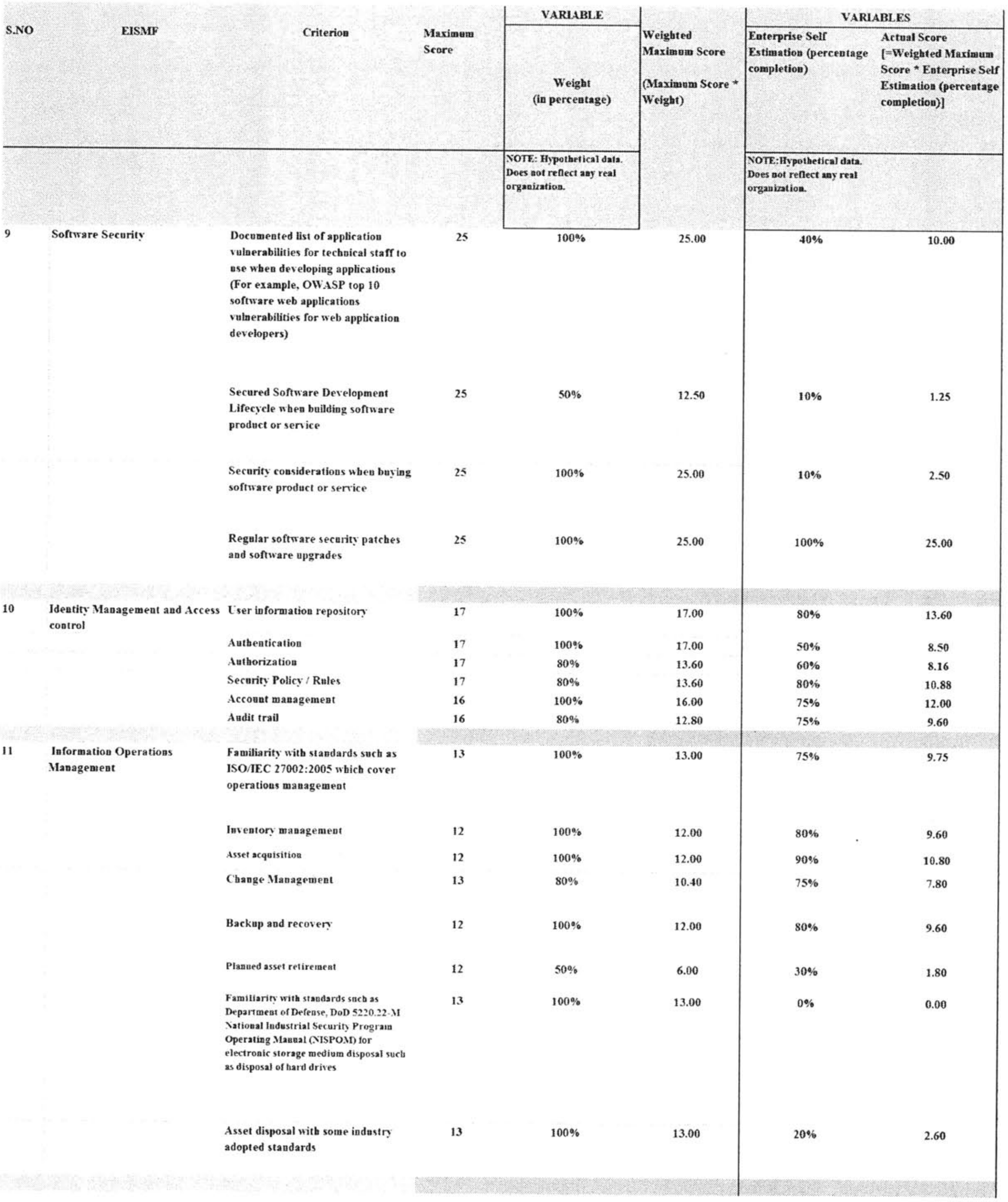
S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score	VARIABLES	
				Weight (in percentage)	(Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
7	Physical Security	Documented plan for protection against natural disaster (For example, earthquake, lightening, flood, and storms)	7	100%	7.00	60%	4.20
		A checklist for regular physical security checks	7	80%	5.60	0%	0.00
		Protection against earthquake considered	7	20%	1.40	0%	0.00
		Protection against lightening	7	50%	3.50	100%	3.50
		Secured keys areas of building for protection against flood and storm	7	40%	2.80	50%	1.40
		Documented plan for protection against human factors (For example, Mistakes, Theft, Vandalism, and Actual physical attack)	7	100%	7.00	0%	0.00
		Electronic monitoring of complete facility	7	100%	7.00	50%	3.50
		Guards at all key areas of the facility such as entrance, location of key physical devices or storage area, etc.	7	40%	2.80	100%	2.80
		Display for appropriate legal messages at various location. For example, message stating - secured area, authorized personnel only	7	30%	2.10	50%	1.05
		Documented plan for protection against other threats (For example, building fire, building water damage, power outage, and strutural failure)	7	50%	3.50	0%	0.00
		Regular fire drills	6	100%	6.00	100%	6.00
		Fire protection mechanism in place	6	100%	6.00	75%	4.50
		Backup power supply	6	20%	1.20	0%	0.00
		Secured all inlet to the facility such as water system, air conditioning, power cable chambers etc.	6	50%	3.00	60%	1.80
		Regular inspection of building structure	6	100%	6.00	100%	6.00

Table is continued below:



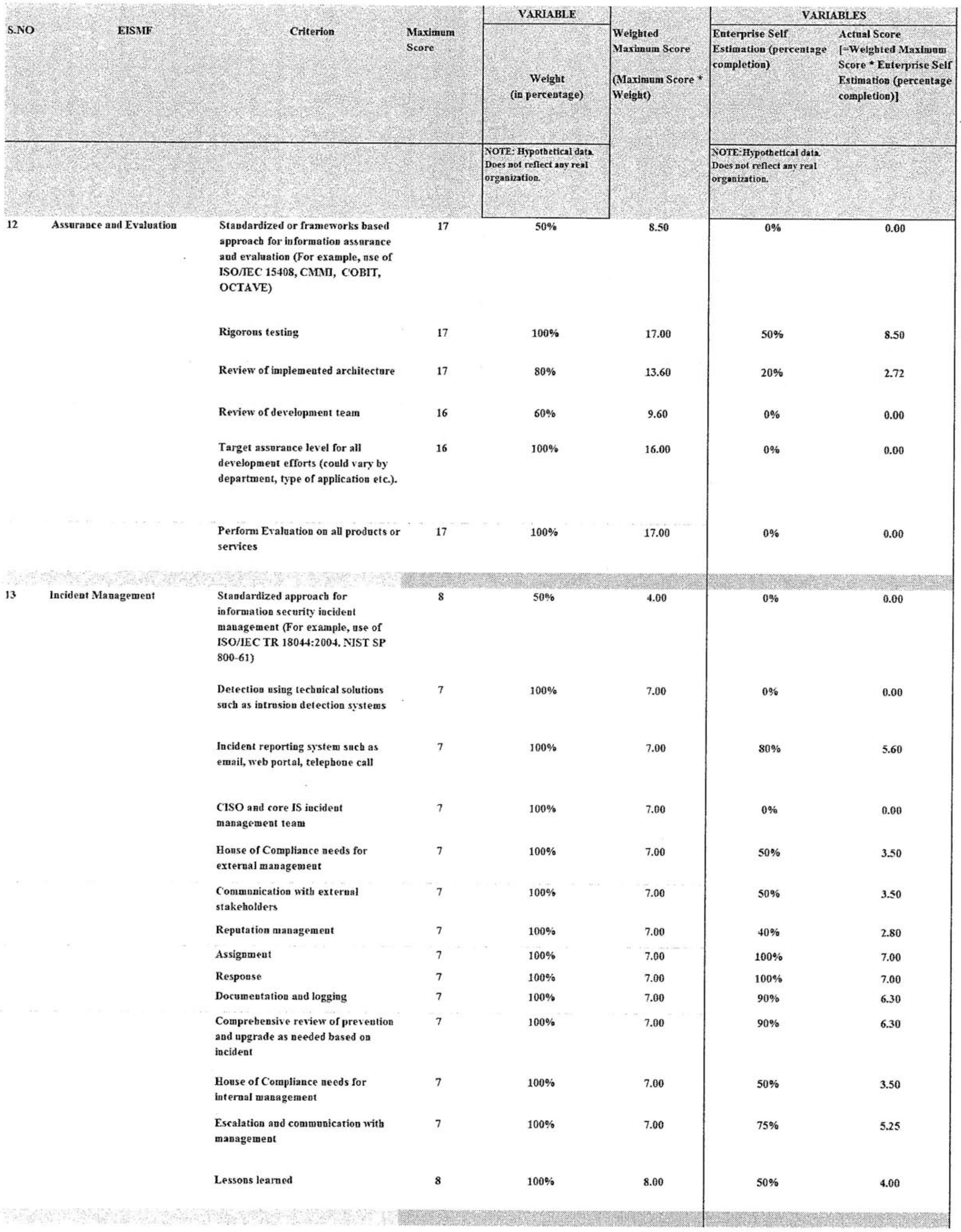
S.NO	EISMF	Criterion	Maximum Score	VARIABLE	Weighted Maximum Score	VARIABLES	
				Weight (in percentage)	(Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
8	Network Security	Special network security policy or dedicated section in Enterprise Information Security policy	6	100%	6.00	100%	6.00
		Secure physical access to network devices such as routers and switches	6	20%	1.20	50%	0.60
		Regular software patch as per vendor recommendations	6	100%	6.00	100%	6.00
		High strength network passwords	6	100%	6.00	50%	3.00
		No default passwords used	6	100%	6.00	100%	6.00
		Passwords changed frequently	6	100%	6.00	60%	3.60
		Limited persons have access to network device management from remote places	6	100%	6.00	40%	2.40
		Legal notice displayed upfront after successful login to a device stating unauthorized access is not allowed and any such access would be investigated fully	6	20%	1.20	40%	0.48
		Session timeout	5	100%	5.00	100%	5.00
		Only needed services are running	6	50%	3.00	30%	0.90
		Encrypted electronic communication	6	40%	2.40	30%	0.72
		Logging of access to any network device (who logged, when logged and what was done)	6	100%	6.00	25%	1.50
		Use of appropriate network architecture	6	50%	3.00	49%	1.47
		Continuous system monitoring and maintain audit trails.	6	50%	3.00	30%	0.90
		Appropriate intrusion detection and prevention system in place	6	100%	6.00	100%	6.00
		Installation of appropriate anti-malware such as antivirus, firewall etc.	6	100%	6.00	100%	6.00
		User education	5	100%	5.00	20%	1.00

Table is continued below:



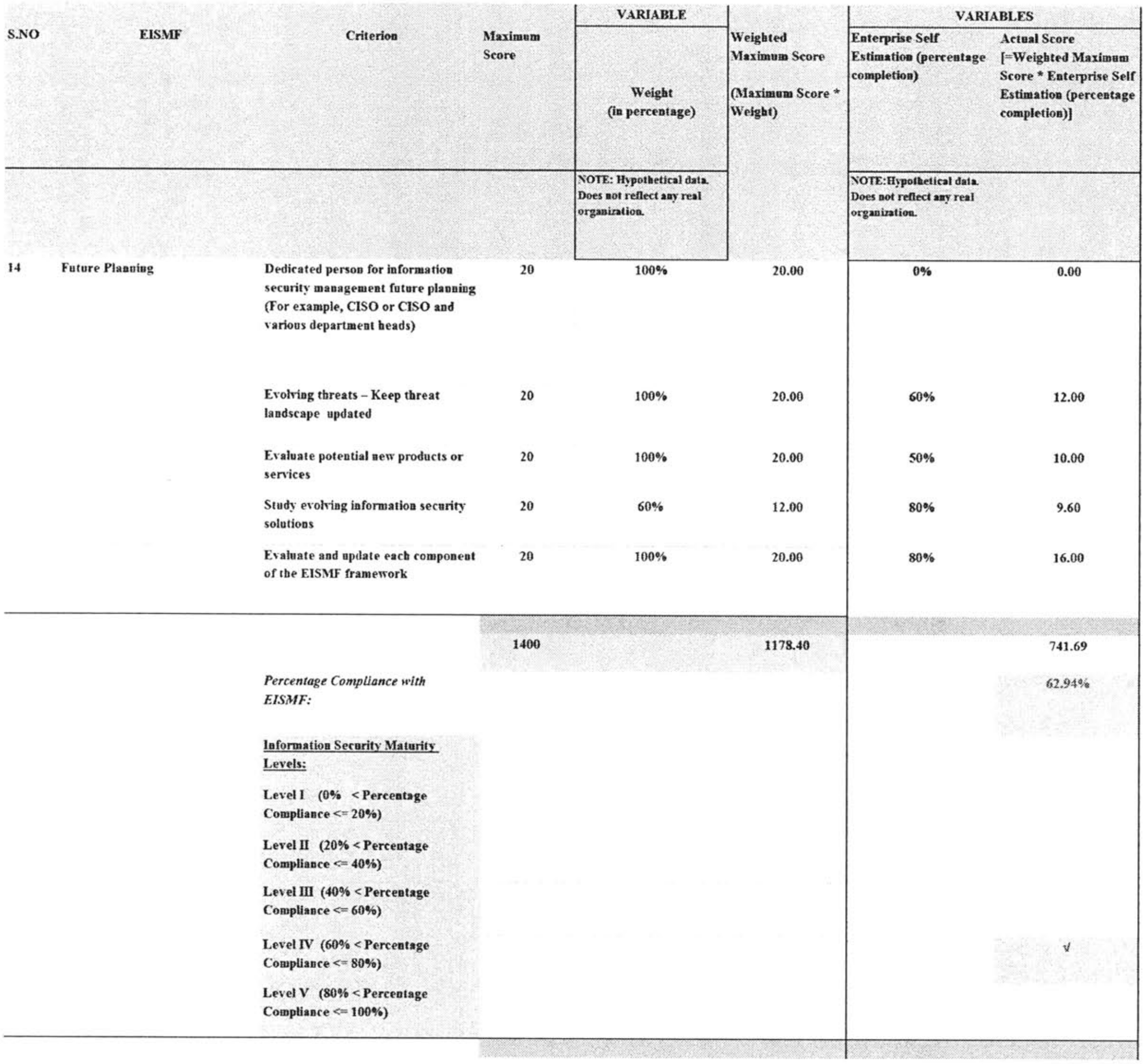
				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
9	Software Security	Documented list of application vulnerabilities for technical staff to use when developing applications (For example, OWASP top 10 software web applications vulnerabilities for web application developers)	25	100%	25.00	40%	10.00
		Secured Software Development Lifecycle when building software product or service	25	50%	12.50	10%	1.25
		Security considerations when buying software product or service	25	100%	25.00	10%	2.50
		Regular software security patches and software upgrades	25	100%	25.00	100%	25.00
10	Identity Management and Access control	User information repository	17	100%	17.00	80%	13.60
		Authentication	17	100%	17.00	50%	8.50
		Authorization	17	80%	13.60	60%	8.16
		Security Policy / Rules	17	80%	13.60	80%	10.88
		Account management	16	100%	16.00	75%	12.00
		Audit trail	16	80%	12.80	75%	9.60
11	Information Operations Management	Familiarity with standards such as ISO/IEC 27002:2005 which cover operations management	13	100%	13.00	75%	9.75
		Inventory management	12	100%	12.00	80%	9.60
		Asset acquisition	12	100%	12.00	90%	10.80
		Change Management	13	80%	10.40	75%	7.80
		Backup and recovery	12	100%	12.00	80%	9.60
		Planned asset retirement	12	50%	6.00	30%	1.80
		Familiarity with standards such as Department of Defense, DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) for electronic storage medium disposal such as disposal of hard drives	13	100%	13.00	0%	0.00
		Asset disposal with some industry adopted standards	13	100%	13.00	20%	2.60

Table is continued below:



				VARIABLE		VARIABLES	
S.NO	EISMF	Criterion	Maximum Score	Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
12	Assurance and Evaluation	Standardized or frameworks based approach for information assurance and evaluation (For example, use of ISO/IEC 15408, CMMI, COBIT, OCTAVE)	17	50%	8.50	0%	0.00
		Rigorous testing	17	100%	17.00	50%	8.50
		Review of implemented architecture	17	80%	13.60	20%	2.72
		Review of development team	16	60%	9.60	0%	0.00
		Target assurance level for all development efforts (could vary by department, type of application etc.).	16	100%	16.00	0%	0.00
		Perform Evaluation on all products or services	17	100%	17.00	0%	0.00
13	Incident Management	Standardized approach for information security incident management (For example, use of ISO/IEC TR 18044:2004. NIST SP 800-61)	8	50%	4.00	0%	0.00
		Detection using technical solutions such as intrusion detection systems	7	100%	7.00	0%	0.00
		Incident reporting system such as email, web portal, telephone call	7	100%	7.00	80%	5.60
		CISO and core IS incident management team	7	100%	7.00	0%	0.00
		House of Compliance needs for external management	7	100%	7.00	50%	3.50
		Communication with external stakeholders	7	100%	7.00	50%	3.50
		Reputation management	7	100%	7.00	40%	2.80
		Assignment	7	100%	7.00	100%	7.00
		Response	7	100%	7.00	100%	7.00
		Documentation and logging	7	100%	7.00	90%	6.30
		Comprehensive review of prevention and upgrade as needed based on incident	7	100%	7.00	90%	6.30
		House of Compliance needs for internal management	7	100%	7.00	50%	3.50
		Escalation and communication with management	7	100%	7.00	75%	5.25
		Lessons learned	8	100%	8.00	50%	4.00

Table is continued below:



S.NO	EISMF	Criterion	Maximum Score	VARIABLE		VARIABLES	
				Weight (in percentage)	Weighted Maximum Score (Maximum Score * Weight)	Enterprise Self Estimation (percentage completion)	Actual Score [=Weighted Maximum Score * Enterprise Self Estimation (percentage completion)]
				NOTE: Hypothetical data. Does not reflect any real organization.		NOTE:Hypothetical data. Does not reflect any real organization.	
14	Future Planning	Dedicated person for information security management future planning (For example, CISO or CISO and various department heads)	20	100%	20.00	0%	0.00
		Evolving threats – Keep threat landscape updated	20	100%	20.00	60%	12.00
		Evaluate potential new products or services	20	100%	20.00	50%	10.00
		Study evolving information security solutions	20	60%	12.00	80%	9.60
		Evaluate and update each component of the EISMF framework	20	100%	20.00	80%	16.00
			1400		1178.40		741.69
		Percentage Compliance with EISMF:					62.94%
		<u>**Information Security Maturity Levels:**</u>					
		Level I (0% < Percentage Compliance <= 20%)					
		Level II (20% < Percentage Compliance <= 40%)					
		Level III (40% < Percentage Compliance <= 60%)					
		Level IV (60% < Percentage Compliance <= 80%)					√
		Level V (80% < Percentage Compliance <= 100%)					

Table 20: Information Security Management Maturity Level Calculations – ***All Criteria***

Note: It is recommended that organizations should start with self assessment using the EISMF. As changes are made to the percent completion of each criterion, updates should be made to the spreadsheet as shown in the example above. This way management and information security personnel would have a way to track progress. Note that self assessment is not a one-time exercise. It should be done at regular intervals.

Bibliography

Allen, Thomas (2009), slide 6, Lecture 4 –Dated April 09, 2009, 15.980 Organizing For Innovative Product Development

Anderson, Ross (2008), Security Engineering, Second Edition, Wiley [ISBN: 978-0-470-06852-6], page 866

British Standards Institute, BS 7799: Part 1: 1995, World Wide Web, Retrieved from http://shop.bsigroup.com/en/ProductDetail/?pid=000000000001324657 on August 05, 2010

California State Government, —SB 1386, Retrieved on October 13, 2010 from http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Carnegie Mellon University Computer Emergency Response Team.(CERT), "OCTAVE(Operationally Critical Threat, Asset, and Vulnerability Evaluation)" World Wide Web, Retrieved October 11,2010 from http://www.cert.org/octave/

Coremetrics, Press Releases, 2009 Press Release, World Wide Web, Retrieved on August 01, 2010 from http://www.coremetrics.com/company/2009/pr12-21-09-online_retail_sales.php

Cusumao, Michael, Selby, Richard W Selby, 1995, Microsoft Secrets: How the World's Most Powerful Software Company Creates Technology, Shapes Markets, and Manages People, Publisher: Free Press (A division of Simon & Shuster, Inc.), New York

Cusumao, Michael, 2004, The Business of Software: What Every Manager, Programmer, and Entrepreneur Must Know to Thrive and Survive in Good Times and Bad, ISBN 0-7432-1580-X, Publisher: Free Press (A division of Simon & Shuster, Inc.), New York

Cusumao, Michael, 2010, Staying Power – Six enduring principles for managing Strategy & Innovation in an uncertain world, ISBN 978-0-19-921896-7, Publisher: Oxford University Press

Damianou N., et al (2001)., "The Ponder Policy Specification Language". In Workshop on Policies for Distributed Systems and Networks, Springer-Verlag (LNCS 1995), 2001,pp. 18-39. R

Department of Defense, DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) January 1995, Department of Defense - Department of Energy - Nuclear Regulatory Commission - Central Intelligence Agency U.S. Government Printing Office ISBN 0-16-045560-X, World Wide Web, Retrieved on October 11, 2010 from www.usaid.gov/policy/ads/500/d522022m.pdf

Distributed Management Task Force, Inc.(DMTF), Common Information Model (CIM) Standards, Retrieved on August 06,2010 from http://www.dmtf.org/standards/cim/

eMarketer, Data Security Breaches Worlwide, by industry, 2009, World Wide Web, Retrieved on August 08, 2010 from http://totalaccess.emarketer.com.libproxy.mit.edu/Chart.aspx?R=93231&Ntt=Data+Security+Breaches+Worldwide&No=-1&xsrc=chart_head_sitesearchx&N=0&Ntk=basic

FEI Survey, Financial Executives International (FEI), World Wide Web, Retrieved on September 22, 2010 from http://fei.mediaroom.com/index.php?s=43&item=204

Forrester, The State Of Enterprise IT Security And Emerging Trends:2009 To 2010, Dated January 25, 2010, by Jonathan Penn for Vendor Strategy Professionals

Helokunnas, T., Kuusisto, R.(2003), Information Security Culture in a Value Net, IEEE Digital Object Identifier: 10.1109/IEMC.2003.1252258

Information Systems Audit and Control Association (ISACA), New Report Shows Benefits of CISOs, Retrieved on August 11, 2010 from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/New-Report-Shows-Benefits-of-CISOs.aspx

Information Systems Audit and Control Association (ISACA) ."COBIT" World Wide Web, Retrieved October 11, 2010 from http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Information Systems Audit and Control Association (ISACA), New Report Shows Benefits of CISOs, Retrieved on August 11, 2010 from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/New-Report-Shows-Benefits-of-CISOs.aspx

Information Systems Audit and Control Association (ISACA) ."COBIT" World Wide Web, Retrieved October 11, 2010 from http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

International Organization of Standardization (ISO), World Wide Web, Retrieved on July 30, 2010 from http://www.iso.org/iso/iso_cafe_management_systems.htm

International Organization for Standardization (ISO), ISO/IEC 27002:2005—Information technology -- Security techniques -- Code of practice for information security management, World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/catalogue_detail?csnumber=50297

International Organization for Standardization (ISO), "ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341

International Organization for Standardization (ISO), "ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414

International Organization for Standardization (ISO), "ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46413

International Telecommunication Union, Identity Management Global Standards Initiative, World Wide Web, Retrieved on October 06, 2010 from http://www.itu.int/en/ITU-T/gsi/idm/Pages/default.aspx

International Organization for Standardization (ISO), ISO/IEC 27002:2005— Information technology -- Security techniques -- Code of practice for information security management , World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/catalogue_detail?csnumber=50297

International Organization for Standardization (ISO), "ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341

International Organization for Standardization (ISO), "ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46414

International Organization for Standardization (ISO), "ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components" World Wide Web, Retrieved October 11, 2010 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46413

ISecT Ltd., World Wide Web, Retrieved on September 22, 2010 from http://www.isect.com/

ISO 27001 Security, World Wide Web, Retrieved on September 22, 2010 from www.iso27001security.com/**ISO27k**_The_**business**_value_of_**ISO27k**_case_study.pdf

Johnson, E (2009), Managing Information Risk and the Economics of Security, Springer (ISBN: 978-0-387-09761-9)

Landoll, D. (2006), The Security Risk Assessment Handbook – A complete Guide for Performing Security Risk Assessments, Auerbach Publications (Taylor and Francis Group), ISBN: 0-8493-2998-1

MACTECH, Key findings of the 8th Annual 2010 BSI Computer Theft Survey, World Wide Web, Retrieved on October, 04 2010 from http://www.mactech.com/2010/08/03/key-findings-8th-annual-2010-bsi-computer-theft-survey

McGraw, G. (2004), Software Security, IEEE Security & Privacy, IEEE Digital Object Identifier : 10.1109/MSECP.2004.1281254 , page 3

McMillan, R., Computerworld, Boeing laptop theft puts U.S. data breach tally over 100M, World Wide Web, Retrieved on October, 04 2010 from http://www.computerworld.com/s/article/9006140/Boeing_laptop_theft_puts_U.S._data_breach_tally_over_100M

Microsoft, Security Risk Management Guide , World Wide Web, Retrieved on September 28, 2010 from http://technet.microsoft.com/en-us/library/cc163143.aspx

National Institute of Standards and Technology (NIST), NIST 800 series, World Wide Web, Retrieved June 12, 2010 from http://csrc.nist.gov/publications/PubsSPs.html

National Institute of Standards and Technology, NIST Special Publication 800-30, World Wide Web, Retrieved on August 14,2010 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

National Institute of Standards and Technology (NIST), SP 800-61 Rev. 1(Computer Security Incident Handling Guide), World Wide Web, Retrieved on October 11, 2010 from http://csrc.nist.gov/publications/PubsSPs.html

Open Security Foundation, Data Loss Database, Retrieved on August 08, 2010 from http://datalossdb.org/reports

Open Web Application Security Project (OWASP), CLASP Best Practice, World Wide Web, Retrieved on August 18, 2010 from http://www.owasp.org/index.php/Category:CLASP_Best_Practice

Pishva, D., Kitamura, N., Tsugawa, S.,Takeda, K. (2007), Corroborative Intersection of the Information Security Standards and the Legal Framework on Data Management, IEEE Digital Object Identifier: 10.1109/CCST.2007.4373461

Ponemon Institute, Fifth Annual US Cost of Data Breach, January 2010 - 2009 Annual Study: Cost of a Data Breach, Page 25, Retrieved on August 11, 2010 from http://www.ponemon.org/data-security

Privacy Rights Clearinghouse, Chronology of Data Breaches, Security Breaches 2005-Present, World Wide Web, Retrieved on July 28, 2010 from http://www.privacyrights.org/data-breach

Roberts, P., InfoWorld, IT security gets physical, World Wide Web, Retrieved on October, 04 2010 from http://www.infoworld.com/d/security-central/it-security-gets-physical-876

Rothke, Ben (2005), Computer Security: 20 Things Every Employee Should Know (Paperback), McGraw-Hill Professional Education (ISBN-10: 0072262826, ISBN-13: 978-0072262827)

SANS (SysAdmin, Audit, Network, Security) Institute , Information Security Policy Templates, World Wide Web, Retrieved on September 26, 2010 from http://www.sans.org/security-resources/policies/

SANS Institute, World Wide Web, Retrieved on September 29, 2010 from http://www.sans.org/

Sarbanes Oxley Act of 2002, The Library of Congress (Thomas), World Wide Web, Retrieved on September 22, 2010 from http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107Tl2MyO:e0:

Sarbanes Oxley Act of 2002, Section 404, The Library of Congress (Thomas), World Wide Web, Retrieved on September 22, 2010 from http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107Tl2MyO:e0:

SC Magazine, Roundup 2006: Do CISOs matter?, Retrieved on August 11,2010 from http://www.scmagazineus.com/roundup-2006-do-cisos-matter/article/34254/

SEI Carnegie Mellon, World Wide Web, Retrieved on September 29, 2010 from http://www.sei.cmu.edu/training/

Solms, v Basie (2000), Information Security — The Third Wave?,0167-4048/00$20.00 © 2000 Elsevier Science Ltd., World Wide Web, Retrieved on August 04, 2010 from www.tut.fi/units/tuta/tita/2006-2007/TITA-5300/the_third_wave.pdf

Sowa, S., Tsinas, L., Gabriel, R. (2008), BORIS –Business ORiented management of Information Security, Managing Information Risk and Economics of Security by M Eric Johnson, Springer, ISBN:978-0-387-09761-9

Symantec Corp. (2010), Symantec Global Internet Security Threat Report, Trends for 2009, Volume XV, Published April 2010, World Wide Web, Retrieved on July 28, 2010 from http://www.symantec.com/business/theme.jsp?themeid=threatreport

The Official Website of the Commonwealth of Massachusetts, Information Security Risk Assessment Guidelines, World Wide Web, Retrieved on September 28, 2010 from http://www.mass.gov/?pageID=afterminal&L=4&L0=Home&L1=Research+%26+Technology&L2=IT+Policies%2C+Standards+%26+Guidance&L3=Technical+Guidance&sid=Eoaf&b=terminalcontent&f=itd_policies_standards_it_security_risk_assessment_guidelines&csid=Eoaf

The Open Group, Identity Management Forum, World Wide Web, Retrieved on October 06, 2010 from http://www.opengroup.org/tech/idm/

Tsoumas, B., Gritzalis, D. (2006), Towards an Ontology-based Security Management, IEEE Digital Object Identifier: 10.1109/AINA.2006.329

United States Department of Justice, Computer Crime & Intellectual Property Section, World Wide Web, Retrieved on July 28, 2010 from http://www.justice.gov/criminal/cybercrime/ccpolicy.html

U.S Department of Homeland Security, Idaho National Engineering and Environmental Laboratory , Personnel Security Guidelines, World Wide Web, Retrieved on October 1, 2010 from www.us-cert.gov/control_systems/pdf/**personnel**_guide0904.pdf

U.S Department of Homeland Security, Office of Inspector General , The DHS Personnel Security Process, World Wide Web, Retrieved on October 1, 2010 from www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-65_May09.pdf

U.S Department of Navy, The Secretary of Navy, Personnel Security Program, Published By Chief of Naval Operations (N09N) Special Assistant for Naval Investigative Matters and Security, World Wide Web, Retrieved on October 01, 2010 from http://www.ncis.navy.mil/securitypolicy/Personnel/SECNAVINST/SECNAV%20M-5510.30%20-%20Complete%20Manual.pdf

VerizonBusiness, 2010 Data Breach Investigations Report, Retrieved on August 08, 2010 from www.verizonbusiness.com

Virginia Information Technology Agency (VITA), IT Risk Management Guideline, World Wide Web, Retrieved on September 28, 2010 from http://www.vita.virginia.gov/library/default.aspx?id=537

Wall Street Journal, Arrest in Epic Cyber Swindle (dated August 18, 2009), Retrieved on August 08, 2010 from http://online.wsj.com/article/NA_WSJ_PUB:SB125053669921337753.html

Washington Post, "Data Theft Common By Departing Employees", World Wide Web, Retrieved on June 26, 2010 from http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html

W3C, OWL Web Ontology Language, Retrieved on August 06, 2010 from http://www.w3.org/TR/owl-features/

Zulhuda, Sonny (2009), Corroborative Intersection of the Information Security Standards and the Legal Framework on Data Management, 2009 Second International Conference on Computer and Electrical Engineering, IEEE Digital Object Identifier: 10.1109/ICCEE.2009.174