



**A HOLISTIC CYBER SECURITY STRATEGY IMPLEMENTATION  
FRAMEWORK**

**BY**

**ISSA ALI FALAH ATOUM**

**SUPERVISORS**

**DR. AMER ABU ALI**

**DR. AHMED OTOOM**

**This Thesis was Submitted in Partial Fulfillment of the  
Requirements for the Master`s Degree in Computer Science**

**Deanship of Academic Research and Graduate Studies**

**Philadelphia University**

**May 2012**

جامعة فيلادلفيا

نموذج التفويض

أنا عيسى علي فلاح عتوم، أفوض جامعة فيلادلفيا بتزويد نسخ من رسالتي للمكتبات أو المؤسسات أو الهيئات أو الاشخاص عند طلبها.

  
التوقيع:

التاريخ: 27/05/2012

Philadelphia University

Authorization Form

I am Issa Ali Falah Atoum , authorize Philadelphia University to supply  
copies of my Thesis to libraries or establishments or individuals upon request

Signature:

Date: 27/05/2012

**A HOLISTIC CYBER SECURITY STRATEGY IMPLEMENTATION  
FRAMEWORK**

**BY**

**ISSA ALI FALAH ATOUM**

**SUPERVISORS**

**DR. AMER ABU ALI**

**DR. AHMED OTOOM**

**This Thesis was Submitted in Partial Fulfillment of the  
Requirements for the Master`s Degree in Computer Science**

**Deanship of Academic Research and Graduate Studies**


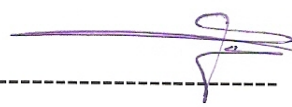


**Philadelphia University**

**May 2012**

(3B) نموذج رقم

قرار لجنة المناقشة

Successfully defended and approved on ---28/05/2012-----

Examination Committee	Signature
Dr. <u>Amer Abu Ali</u> ..., Chairman Academic Rank: <u>Associate prof.</u>	
Dr. <u>Prof. S. Ghoul</u> ..., member. Academic Rank: <u>Full prof.</u>	
Dr. <u>Hassan Al-Retai</u> ..., member. Academic Rank: <u>Assistant prof</u>	
Dr. <u>Mohammad Alhammouri</u> ..., External Member. Academic Rank: <u>Asst. Prof</u>	
( Name of University <u>JUST</u> )	

**DEDICATIONS**

I would like to dedicate this thesis to my parents (Ali and Moneera), wife Deema, brothers (Mohammed, Ahmed, Sultan, Sameer, and Samer), sisters (Mona, Manwa, Ibtisam, Amal, Samar, Sawsan, and Wafa), daughter Asma, sons (Khaled, Abd Alrahman, Ibrahim), and mother-in-law for their sincere love, confidence, and unselfish support, and to my fellow students at Philadelphia University.

**Issa Atoum**

## ACKNOWLEDGEMENTS

My sincerest appreciation and thanks go to my thesis advisors: Dr. Amer Abu Ali and Dr. Ahmed Ootom for their sincere patience, support, and guidance.

This work would not have been possible without the support of many people. Therefore, I would like to thank HE the Minister of ICT, the Secretary General of MoICT, and HE the President of Philadelphia University for giving me the opportunity to validate my research using the National Information Assurance & Cyber Security Strategy (NIACSS) as a case study. I would like also to thank the NITC employees who participated in the review of the case study: Dr. Ahmed Ootom, Eng. Mohammad Al-Fayoumi, Yousef M. Sarairah, Eng. Mohammad Al-Ja'afreh, Eng. Abdullah Zboun, Hiyam Alyousfy, Bashar Almajali, Mohammad Hijazi, and Mohammad Sarairah.

I would also like to thank the Examination Committee, the reviewers, Prof. Said Ghoul, Dr. Nameer El-Emam, Dr. Hasan Al-Refai, Prof. Mahmoud Qishtah, Dr. Khaldoun Batiha, Dr. Fadi Fayez, Dr. Wael Hadi, Dr. Murad Moache, Dr. Samer Hanna, and Dr. Moayad Al-Athami for their support, comments or feedback.

**Issa Atoum**

## Table of Contents

<b>Subject</b>	<b>Page</b>
Authorization form	i
Title	ii
Examination committee	iii
Dedications	iv
Acknowledgements	v
Table of contents	vi
List of tables	x
List of figures	ix
List of abbreviations	xii
Disclaimer	xvi
Abstract	xvii
Chapter One : Intorduction	1
1.1. Background	1
1.2. Research motivation	3
1.3. Problem statement	4
1.4. Research objectives	5
1.5. Contributions	6
1.6. Methodology	7
1.7. Limitations	7
1.8. Organization of thesis	8
Chapter Two : Literature Review	10
2.1. Introduction	10
2.2. Related Frameworks Or Models	11
2.2.1. Management and Governance Frameworks	11
2.2.2. Guidelines	12
2.2.3. Customized Frameworks	13
2.2.4. Security Maturity and Metrics Models	14

2.2.5. Generic Frameworks	16
2.2.6. Provider Specific Architectures and Frameworks	16
2.2.7. Open Architectures	17
2.3. Viewpoints	18
2.4. Performance Measurement	19
2.5. Belief Networks	20
2.6. Conclusion	20
Chapter Three : Holistic Cyber Security Strategy Implementation Framework (CSS-IF)	21
3.1 Introduction	21
3.2 Cyber Security Research Perspectives	22
3.3 Framework Development Process	22
3.4 The Implementation Framework(CSS-IF)	24
3.4.1. CSS-IF Block Diagram	25
3.4.2. Cyber Security Strategy (CSS)	28
3.4.3. Requirement Elicitation	29
3.4.3.1. Requirement Elicitation Formulation	30
3.4.4. Security Strategic Moves	35
3.4.5. Controls	39
3.4.5.1. Governance	40
3.4.5.2. Strategic Controls	41
3.4.5.3. Audit Controls	43
3.4.5.4. Framework Controls And Prototype	44
3.4.5.4.1. Framework Controls	44
3.4.5.4.2. Framework Prototype	50
3.4.6. Business Controls	51
3.4.7. Cyber Security Objectives	52
3.4.8. Implementation Framework Repository	53
3.5 Chapter Summary	53
Chapter Four : CSS-IF Performance Measurement	55



4.1. Introduction	55
4.2. ITsec-BSC As Related To CSS-IF	56
4.3. Proposed Performance Model	58
4.3.1. Holistic Performance Formulation	59
4.4. Chapter Summary	62
Chapter Five: Validation Of The CSS-IF	63
5.1. Introduction	63
5.2. Validation Using A Case Study	63
5.2.1. Background	63
5.2.2. Applying CSS-IF For NIACSS	65
5.2.3. NITC Practitioners	74
5.2.4. Case Study Summary	75
5.3. Validation Model Using Bayesian Belief Network	76
5.3.1. Introduction To Bayes Networks	76
5.3.2. Example On Belief Networks	77
5.3.3. Bayes Network For CSS-IF	79
5.4. Comparison With Other Frameworks	82
5.5. Chapter Summary	84
Chapter Six: Conclusions and Future Work	86
6.1. Conclusion	86
6.2. Future Work	88
Appendixes	90
A. References	90
B. Detailed Frameworks Comparison	99
C. Holistic Balanced Scorecard For NIACSS	103
D. Letter Of Cooperation With NITC	105
E. Applicability Of CSS-IF To Jordan NIACSS	106

### List of Tables

<b>Table Number</b>	<b>Table Title</b>	<b>Page</b>
Table (2-1)	List of International Enterprise Architecture related to Cyber Security.	17
Table (3-1)	Requirement Elicitation Matrix.	35
Table (3-2)	Example - Goal Weighting Technique.	37
Table (3-3)	Example-Independent Project Ordering.	38
Table (5-1)	Example – Requirements to Goals for NIACS	67
Table (5-2)	Example – Goal Prioritization (1/2).	68
Table (5-3)	Example – Goal Prioritization (2/2).	70
Table (5-4)	Summary of NITC's Practitioners Evaluation.	75
Table (5-5)	Cyber Security Frameworks (category) Comparison.	84
Table (5-6)	CSS-IF Validation Techniques Advantages and Disadvantages.	85

## List of Figures

<b>Figure Number</b>	<b>Figure Title</b>	<b>Page</b>
Figure ( 1-1 )	Strategy Processes.	2
Figure ( 3-1 )	Process for developing the CSSIF.	24
Figure ( 3-2 )	Conceptual View of Cyberspace Security Layers.	25
Figure ( 3-3 )	Detailed Cyber Security Strategy Implementation Framework (CSS-IF).	27
Figure ( 3-3)	Block Diagram View of CSS-IF	28
Figure ( 3-4 )	Requirement Elicitation Component.	30
Figure ( 3-5 )	Requirement Acceptance.	33
Figure ( 3-6)	Strategic Moves process.	36
Figure ( 3-7 )	Example Interdependent Projects Ordering.	38
Figure ( 3-8 )	The CSSIF Controls Interaction.	39
Figure ( 3-9 )	The CSSIF Conceptual CS Governance.	41
Figure ( 3-10)	The CSSIF Strategic Controls.	43
Figure ( 3-11)	The CSSIF Security Level and Gap Finder Processes.	44
Figure ( 3-12)	The CSSIF Framework Controls.	45
Figure ( 3-13)	An Example of a UML Diagram for high level classes of CSS-IF.	50
Figure ( 3-14)	Sample UML Requirements, Viewpoints and Security Goals Classes.	51
Figure ( 3-15)	The CSSIF Sample Business Controls.	52
Figure ( 4-1)	ITsec BSC Model, Herath et al., 2010.	58
Figure ( 4-2)	The CSSIF H-ITsec-BSC Conceptual Model.	60
Figure ( 4-3)	Example - Goal Performance Compared to Sub-goal Performance.	62
Figure ( 5-1 )	Example - “Viewpoints” applied to NIACSS.	67
Figure ( 5-2 )	Example – Master High Level Road Map for NIACS.	72
Figure ( 5-3 )	Example – Dashboard of H-ITsec-BSC for NIACS (BSC Designer).	73

Figure ( 5-4)	Example – Strategy Map of H-ITsec-BSC for NIACS (BSC Designer).	74
Figure ( 5-5)	Example –Mapping Security Moves to Security Objectives.	75
Figure ( 5-6 )	Belief Network Example Before an Evidence Is Set.	79
Figure ( 5-7 )	Belief Network Example After an Evidence Is Set (S=N).	79
Figure ( 5-8 )	List Of Probabilities Values For BN Example.	79
Figure ( 5-9)	Belief Network of CSS-IF.	81
Figure ( 5-10)	Sample Network of CSS-IF (Assigning Values By Experts.)	82
Figure ( 5-11)	Sample Network of CSS-IF (Assigning Evidence of Controls to False.)	82

### List of Abbreviations

<b>ACRONYM / SYNONYM</b>	<b>MEANING</b>
AICPA	Auditing Standards Board of the American Institute of Certified Public Accountants
ALE	Annual Loss Expectancy
ANSI	American National Standards Institute
BN	Bayesian Network
BSC	Balanced Scorecard
CAG	The Consensus Audit Guidelines
CASE	Computer-Aided Software Engineering
CC	The Common Criteria for Information Technology Security Evaluation
CCB	Change Control Board
CIO	Chief information officer
CMMI	Capability Maturity Model Integration
CNI	Critical National Infrastructure
COBIT	Control Objectives for Information and related Technology
COSO	The Committee of Sponsoring Organizations of the Treadway Commission
COTS	Commercial Off The Shelf
CS	Cyber Security
CS & IA	Cyber Security and Information Assurance
CSMF	Cyber Security Management Framework
CSS	Cyber Security Strategy

<b>ACRONYM / SYNONYM</b>	<b>MEANING</b>
CSS-IF	Cyber Security Strategy Implementation Framework
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAG	Directed Acyclic Graph
DoDAF	The U.S. Department of Defense Architecture Framework
E2AF	Extended Enterprise Architecture Framework
EISA	Enterprise Information Security Architecture
ENISA	European Network and Information Security Agency
FEA	Federal Enterprise Architecture of the United States Government
GDP	Gross Domestic Product
GGI	The Global Governance Institute
GRCiP	Open Interoperability Protocol
H-ITsec- BSC	Holistic Information Security Balanced Scorecard
HM Gov.	Her Majesty Government
IBM	International Business Machines, a leading U.S. computer manufacturer
ICT	Information and Communication Technology
iGRC	The Integrated Governance, Risk And Compliance Consortium
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum
ISG	Information Security Governance
ISMS	Information Security Management System

<b>ACRONYM / SYNONYM</b>	<b>MEANING</b>
ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
ISP	Internet Service Provider
ISPMG	Information Security Program Maturity Grid
ISSA	Information Systems Security Association
ISSEA	International Systems Security Engineering Association
ISST	The Fraunhofer Institute for Software and Systems Engineering
ITES	IT Enabled Services
ITIL	The Information Technology Infrastructure Library
ITSEC	The Information Technology Security Evaluation Criteria
ITSec-BSC	Information Security enabled BSC
ITSM	IT Service Management
ITU	International Telecommunication Union
JO-CERT	Jordan Computer Emergency Readiness Team
MoICT	Jordan's Ministry of Information and Communications Technology
NEC	National Encryption Center
NIACSS	National Information Assurance and Cyber Security Strategy
NITC	National Information Technology Center
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OMB	Office of Management and Budget
ORA	Oracle Reference Architecture
PERT	Program Evaluation and Review Technique

<b>ACRONYM / SYNONYM</b>	<b>MEANING</b>
PMM	Performance Measurement And Management
PMO	Project Management Office
PMS	Performance Management system
ROSI	Return on Security Investment
SABSA	Sherwood Applied Business Security Architecture
SFPBGS	Protecting Business, Government and Society
SLEPT	Social, Legal, Economic, Political, Technological
SMM	Security Maturity Model
SoGP	Standard of Good Practice
SSE-CMM	Security Engineering Capability Maturity Model
SWOT	Strengths, Weaknesses, opportunities and Threats
TCSEC	Trusted Computer System Evaluation Criteria
TOGAF	The Open Group Architecture Framework
UCF	Universal Compliance Framework
UML	Unified Modeling Language
U.S. DoD	United States Department of Defense



**DISCLAIMER**

This thesis does not represent the thoughts, intentions, plans or strategies of the National Information Technology Center (NITC), Jordan's Ministry of Information and Communications Technology (MoICT), or any other Governmental or nongovernmental entity; it is solely the opinion of the author. The NITC, MoICT, and/or any other entities are not responsible for the accuracy of any of the information supplied herein.

## ABSTRACT

Cyber Security Strategy (CSS) implementation is a problem for many countries. Cyberspace is insecure and is considered a challenging problem for many governments due to a set of factors such as: lack of holistic systematic cyber security strategy implementation frameworks, lack of comprehensive performance measures at the national level, and lack of cooperation with other governments in the field of cyber security. While several cyber security frameworks address the issue from a management perspective of cyber security, little research has been conducted on cyber security from engineering perspectives.

This thesis proposes an implementation framework for cyber security strategy that has the following benefits: 1) helps the international governments to take on a consolidated approach to enforce the implementation of CSS across their nations, 2) The CSS-IF provides an early detection of likely threats and mitigate risks related to government information systems and critical infrastructure, 3) enhances security by providing leading and lagging measures of cyber security at the national level, and 4) helps convert the CSS from the natural language to a set of business and security requirements.

The framework has been conceptually and practically validated to provide a proof of concept by using a case study and Bayes Belief Network. The case study shows that the CSS-IF is applicable to the Cyber Security Strategy of Jordan. The Bayesian network validation model shows the strong relevance of CSS-IF and its components to achieve the required security objectives. The CSS-IF outperforms other frameworks on six selected cyber security features. The framework is developed for CSS implementation; however a possible future research may show that it can be generalized or be applicable for other domains.

**Key words:** *Cyber Security, Security Performance, Requirements Elicitation, Strategy Implementation Framework, Information Assurance, and Strategic Controls.*

## **CHAPTER ONE**

### **INTRODUCTION**

## CHAPTER 1

### INTRODUCTION

#### 1.1. BACKGROUND

Cyberspace is a new term in computer security referring to a huge space of all electronic forms of activities such as the internet, the mobile phones, and the wire and wireless networks. Cyberspace is dynamically evolving in technology and is subject to human behaviours. Cyber security is the set of actions or plans taken to protect the cyberspace. According to Symantec® internet security report, security threats are costing the world more than 114 Billion U.S. Dollars (Fossi et al., 2011). Unfortunately, several information security threats are catastrophic; they might affect human lives directly or indirectly, such as Stuxnet attacks that targeted Iranian nuclear systems (Constantine, 2011).

Cyberspace is insecure (sometimes called cyber insecurity) and is considered a challenging problem for many governments due to a set of internal and external factors. The internal factors include: 1) lack of cyber security strategy implementation frameworks (e.g. Government of UK, (Nguyen, 2012)), 2) lack of an overall governance with performance measures at the national level (Bartol, Bates, Goertzl, & Winograde, 2009), 3) government sheepish response to threats: through the application of law and regulation, inefficient application of procedures and policies to protect underlying systems, bad capacity building or awareness programs, and lack or bad cyber security plans, and 4) vulnerabilities in hardware and software systems. The external factors are due to many reasons such as: 1) lack of cooperation with other governments in the field of cyber security (Broom, 2009; Hunker, 2010), 2) lack of research and development of global risk mitigations (e.g. U.S. (Maughan, 2010)), 3) lack of holistic cyber security strategies (Fielden, 2011), 4) attacks that target information or architectures for various reasons, and 5) threat enquired by the bad design of the internet. Iheagwara et. al. (2011) state that the current internet design is exploited to launch cyber-attacks and they suggest modifying internet design to allow better authentication (Iheagwara & Charless M. Iheagwara, 2011).

Cyber Security Strategies (CSSs) play a major role in combatting threats and identifying risks. Many governments have developed CSSs based on the reappraisal of information

security status in their corresponding countries (International Telecommunication Union(ITU), 2011a; The White House, 2011).These strategies usually comply with the organization missions and influence information security operations to achieve specific security objectives. CSSs recognize the threats imposed by the unprecedented revolutionary changes in Information Technology and the cyberspace environment. The CSSs are usually high level abstract documents that guide what has to be achieved and usually do not have implementation details. For example, Jordan has developed the National Information Assurance and Cyber Security Strategy (NIACSS). The NIACSS identifies strategic objectives and National priorities. The strategic objectives aim to: strengthen National security, minimize risks to critical National infrastructure, minimize damage and recovery time, enhance economy and National prosperity, and increase cyber security and information assurance awareness. The National priorities of NIACSS address the critical needs required to guide the implementation towards achieving the National objectives (MoICT, 2011). For more details and examples of international CSSs, refer to (Estonia Department of Defence, 2008; Government of Australia, 2009; HM Government, 2010; Phahlamohlaka, Jansen van Vuuren, & Coetzee, 2011; Suid-afrika, 2010; The White House, 2009; U.S. DoD, 2011).

Countries strive to protect their cyberspace by first formulating their CSSs. Generally, a strategy planning has three consecutive processes(David, 2011). These processes, as shown in Figure 1-1, are: Strategy Formulation, Strategy Implementation, and Strategy Evaluation. Our major concern in this research is the Strategy Implementation and precisely a holistic framework for cyber security strategy implementation. Strategy Formulation and Strategy Evaluation processes are outside the scope of this research.



Figure 1-1 Strategy Processes.

First, we discuss the motivations behind this research. Then we explore the problem and research objectives. After that, we list the contributions, methodology and limitations. Finally, we list the published and current works out of this research and the organization of the thesis, respectively.

## **1.2. RESEARCH MOTIVATION**

This research is motivated by three major factors. The first factor is lack of a holistic consolidated approach to enforce the implementation of CSS across a corresponding nation (Dasgupta & Rahman, 2011). This factor triggers the willingness of the international governments to take on a consolidated approach to enforce the implementation of CSSs across their nations (Broom, 2009; International Telecommunication Union(ITU), 2011a; Tagert, 2010). Enforcing information security policies at the national level is important for many reasons: 1) to ensure early detection of likely threats and mitigate risks related to government information systems and critical infrastructures, 2) to enable decision makers to take necessary actions once needed, and be able to implement security solutions that involve vast number of stakeholders including private ICT companies, government entities, and citizens, 3) to assist governments in creating a safe and trustworthy environment for business, and 4) to be able to implement a national awareness program.

The second factor is the lack of a global performance measures for cyber security strategy implementation at the national level (Bartol et al., 2009). According to Bartol et. al. (2009) , “While a number of Cyber Security/Information Assurance (CS/IA) strategies, methods, and tools exist for protecting IT assets, there are no universally recognized, reliable, and scalable methods to measure the ‘security’ of those assets” (Bartol, Bates, Goertzl, & Winograde,2009). This factor is supported by three sub factors which are: lack of cooperation with other governments (Broom, 2009; Hunker, 2010), lack of research and development on global risk mitigations (Maughan, 2010), and lack of holistic cyber security strategies (Fielden, 2011).

The third factor is the crucial need of international governments to protect citizens and investments in the sector of Information and Communication Technology (ICT) and IT Enabled Services (ITES) via achieving acceptable level of security given limited

resources. One third of the world's population is online and 45% of Internet users are below the age of 25 (International Telecommunication Union(ITU), 2011b). Telecommunications services revenue on a worldwide basis will grow from \$2.1 trillion in 2012 to \$2.7 trillion in 2017 at a combined average growth rate of 5.3% (The Insight Research Cooperation, 2012).

### **1.3. PROBLEM STATEMENT**

Cyber security strategy implementation is a problem for many countries (Hunker, 2010; International Telecommunication Union(ITU), 2009; Maughan, 2010). In USA, despite increasing attention from federal and state governments and international organizations, the defence against cyber-attacks has appeared to be generally fragmented and varying widely in effectiveness (Fischer, 2005). Different countries vary in the level of confronting cyber security threats (International Telecommunication Union(ITU), 2011a; Tagert, 2010). Where there are significant efforts that have been taken in the developed countries, several developing countries have taken little or no efforts in cyber security domain.

One of the major international challenges that is still valid, is the need to consolidate cyber security efforts at the national level(Broom, 2009). Cyber security efforts are not consolidated and implementation efforts are not overarching. 90% of mid-to-large enterprises in Europe are likely to undertake a network security consolidation initiatives (Fortinet, 2011). Jordan is not an exception in terms that cyber security efforts across government organizations and private sectors are not consolidated, have no security performance controls at the national level, and risks are not nationally addressed. Current cyber security solutions adopted by government of Jordan are subjective; usually performed on an ad hoc basis; and do not deal effectively with threats emerging from cyberspace (e.g. MoICT, 2011). CSSs are usually written in a natural language which adds additional complications to the aforementioned problems and limits understanding of specifications, makes specifications over-flexible, and there will be no easy way to modularize requirements (Nuseibeh, Kramer, & Finkelstein, 2003; Salem, 2010).

This thesis proposes an implementation framework that lays out the ground for a conceptual, coherent, systematic, holistic, and consolidated approach to implement CSSs.

The Cyber Security Strategy Implementation Framework (CSS-IF): 1) suggests a methodology to elicit requirements from the CSS, 2) illustrates how the CSS analysis can be utilized to design strategic moves, 3) proposes a holistic technique to measure the performance during strategy implementation, 4) proposes a set of adaptable security controls that govern the CSS implementation and allow achieving excellence, innovation, efficiency, and quality. The CSS-IF is validated to provide a proof of concept.

#### **1.4. RESEARCH OBJECTIVES**

The CSS-IF helps governments enforce the cyber security at the national information systems and critical information infrastructures; it helps governments consolidate the efforts of the citizens, private sector and government organizations and addresses the risks at the national level. The CSS-IF bridges the gap between strategy formulation and strategy implementation and guides the implementation process and guarantees the achievement of the national objectives identified in a security strategy. Moreover, it suggests a global conceptual security performance framework that enables decision makers at various levels to have full control on the implementation process and facilitates an efficient engagement of all involved parties at the national level.

The CSS-IF allows the description and measurement of its goals. The CSS-IF helps in aligning security and business goals to achieve the required goals. These goals –extracted from CSSs- must depend on results or states rather than protection or prevention of attacks. For example, the functional goals that target reducing system maintenance and recovery time are better than goals that target reducing number of attacks or preventing system attacks because attacks are different on level of damage that may result to information systems. For example, a single attack may result in devastating results whereas hundreds of attacks may be gracefully ended.



## 1.5. CONTRIBUTIONS

1. Holistic Cyber Security Strategy Implementation Framework, here in, we call it CSS-IF: the main contribution of this work is developing a conceptual holistic framework for strategic implementation of cyber security. The CSS-IF is explored in CHAPTER 3.
2. Holistic Performance Framework as an embedded component within the CSS-IF: the performance of the CSS-IF will be established by utilizing a modified version of Information Technology Security Balanced Score Card (ITsec-BSC) that we call the Holistic ITsec-BSC (H-ITsec-BSC). The term “Holistic”, in the context of the H-ITsec-BSC, is used to reflect that the H-ITsec-BSC measures the performance at a national level to best serve the CSS-IF. The ITsec-BSC was originally proposed by Herath (2010). The H-ITsec-BSC aggregates performance measures from various entities executing CSS sub-goals. In other words, the H-ITsec-BSC will be used in the upper level of the CSS-IF while each provider will have his/her choice of the BSC version or any other performance measurement technique as long as provider’s metrics is exposed to the H-ITsec-BSC. The H-ITsec-BSC is explored in CHAPTER 4.
3. Requirements Elicitation. The Requirements Elicitation component embedded within the CSS-IF helps convert the CSS from the natural language to a set of business and security requirements. The elicitation is important to break the CSS into manageable understandable requirements and identify Strategic Moves that will eventually enhance the overall security level. Requirements elicitation is explored in Section 3.4.3.
4. Integrate and consolidate different components to serve as a holistic CSS-IF: the CSS-IF integrates Viewpoints, a concept being used in Software Engineering, and an enhanced Holistic Information Security Balanced Score Card (H-ITsec-BSC) , Strategic Moves Component, Control Components, and other necessary components in various domains of security engineering to implement the CSS. These components and interaction among them are explored in CHAPTER 3 under the context of the CSS-IF.

5. A three-way validation technique: the CSS-IF is validated utilizing three different techniques: 1) a comparison with other related works, 2) through a case study, and 3) formally via a Bayes Belief Networks(BN). Validation is covered in CHAPTER 5.
6. A Configurable framework: the CSS-IF is a configurable framework where strategy implementers can decide on input components that target the required cyber security level. Configurability of the CSS-IF is covered and demonstrated in CHAPTER 3 and its validation is demonstrated in CHAPTER 5.

## 1.6. METHODOLOGY

In this research, we adopt the following methodology: (refer to Section 3.3 for details).

- Review literature of international cyber security strategy analysis and implementation, active frameworks, and security engineering approaches.
- Integrate Viewpoints and an enhanced information security BSC along with other necessary components utilizing information security best practices in order to develop a holistic conceptual framework for implementing cyber security strategies.
- Validate the framework by applying a case study on the National Information Assurance and Cyber Security Strategy of Jordan and via Belief Networks (BN).

## 1.7. LIMITATIONS

Domain specific framework: The CSS-IF explores cyber security from computer science point of view. Other related components such as law and regulations, awareness, cooperation and management of cyber security are only mentioned for completeness purposes. Details of such components are left outside the scope of this thesis to be thoroughly investigated by community researchers in the corresponding respective domains.

Assumptions: the CSS-IF assumes that cyber security strategy is already formulated. CSS formulation occurs during Strategy Formulation Process (Figure 1-1) which is out of scope. Although the CSS-IF can detect gaps in CSS to get better results, CSS should satisfy

holistic properties such as changing technologies, information security management, complexity and other properties suggested by Fielden(2011) (Section 3.4.2). Moreover, the framework assumes that a cyber security Governance Board is already in place to kick in the CSS-IF implementation.

Belief Network Limitations: the results indicated by the Belief Network, used to validate the CSS-IF in CHAPTER 5, are highly dependent on the generated data and its distribution. We were not able to get data to our model due to the fact that most available data sets are on the operational level of cyber security, and even if we were able to aggregate such data the semantic of the data will get lost. Thus, we suggest further research in order to find the best weight of each random variable and then generate a more representative data to validate the model.

## **1.8. ORGANIZATION OF THESIS**

- CHAPTER 1: Introduction. This chapter introduces research motivation, the problem, objectives, contributions, research methodology, and lists the basic structure of the thesis.
- CHAPTER 2: Literature Review. This chapter reviews the related literature including: Implementation Frameworks, Viewpoints, Performance Measures, and Belief Networks. Readers familiar with cyber security frameworks may skip this chapter and go directly to the CSS-IF illustrated in CHAPTER 3.
- CHAPTER 3: A Holistic Cyber Security Strategy Implementation Framework. This chapter lists cyber security research perspectives, illustrates the development process of the CSS-IF, and thoroughly discusses the proposed CSS-IF.
- CHAPTER 4: The CSS-IF Performance Measurement. This chapter illustrates how performance of the CSS-IF could be established by utilizing a modified version of ITsec-BSC.
- CHAPTER 5: Validation of the CSS-IF. This chapter validates the CSS-IF by applying a group of formal and informal approaches to provide a proof of concept.

- CHAPTER 6: Conclusion and Future Work. This chapter explores the benefits of the CSS-IF over current related frameworks and lists possible topics to help direct future research.

**CHAPTER TWO**  
**LITERATURE REVIEW**

## **CHAPTER 2**

### **LITERATURE REVIEW**

#### **2.1. INTRODUCTION**

This chapter reviews the related literature including: Implementation Frameworks, Viewpoints, Performance Measures, and Belief Networks. Readers familiar with cyber security frameworks may SKIP this chapter and go directly to the CSS-IF illustrated in CHAPTER 3.

Since cyber security domain is highly interdisciplinary, touching everything from pure mathematics to management science, we select related works that focus on scientific perspective of cyber security engineering supported with practitioners' experience, government publications, international security solutions providers, and related ISO security standards.

We select the period from 2005 till 2012 to search on cyber security strategy implementation frameworks except for several security standards, maturity models, and metrics that were selected beyond this period. The list of references contains articles in: IEEE, Direct Science, Elsevier, ProQuest DB, ACM, Springer, Taylor & Francis, government web sites (UK, U.S., Jordan, Estonia, South Africa, Morocco, and Austria), International Associations (ITU and ENSIA) or ISO standards web sites. The searching keywords were phrases related to : 'Framework', 'cyber security', 'Methodology', 'information security', 'strategy implementation', 'information assurance', 'security implementation', and more.

We need to confirm that the CSS-IF is not intended to replace other frameworks nor it can. We review the current literature so we identify the limitations of current solutions and develop a solution that overcomes these limitations. More details about literature review influence on the development of CSS-IF are given in Section 3.3. In fact, the CSS-IF is designed to exploit and embed other frameworks were appropriate. We will see in Section 3.4.5.4.1 that the CSS-IF has a built in configuration components that make the

integration with other frameworks possible. The CSS-IF achieves its major advantage mainly by being able to implement and oversee cyber security on a holistic level.

First, we review cyber security frameworks. Then, we review Viewpoints, Balanced Score Cards, and Belief Networks. Finally, we conclude this Chapter.

## **2.2. RELATED FRAMEWORKS OR MODELS**

The gathered related literature is grouped into the following logical categories to facilitate a structured reading and analysis; though these categories are highly interconnected:

### **2.2.1. MANAGEMENT AND GOVERNANCE FRAMEWORKS**

Information security frameworks usually target the management perspective of information security. For example, Nnolim (2007) has suggested a conceptual framework for information security management meta model composed of two major components: information security framework and the information security management program. Nnolim information security framework is a result of strategic planning and applying international standards. Nnolim work targets cyber security enterprise level, applies management approaches, very high level, and hence does not qualify to be modified as cyber security strategy implementation framework. Another similar management framework is suggested by Zuccato (2007) to manage security of an enterprise using a set of defined activities mapped with system security engineering maturity model. Zuccato's work has the same drawbacks of Nnolim's work to be used as CS implementation framework.

Many governments deploy Enterprise Architectures (EA) solutions to align between different IT projects (such as e-government projects) and government business, to ensure interoperability, avoid duplication, and identify Business-IT gaps. For example, Janssen & Hjort-Madsen (2007) suggested National EA framework composed of architectures, principles and standards to compare architecture of Denmark and the Netherlands. Janssen's research identifies the need of taking a broader governance perspective in enterprise architecture but does not address the needed components for Cyber Security Framework on the national level. Even though EA initiatives align business and security,

they face complicated governance and insufficient support for the development according to a case study by (Seppanen, Heikkila, & Liimatainen, 2009).

International Telecommunication Union (ITU) suggests a management framework for Organizing national cyber security that depends on five factors: national strategy, government industry collaboration, deterring cybercrime, incident management capabilities, and culture of cyber security (ITU, 2008). Each element of the ITU framework recommends a policy, a goal and a specific step. However, this framework is leaned towards management providing a matrix of management plan, and governance perspectives.

Neubauer et al. (2005) suggest a framework for valuation of IT security based on business process. The approach makes a trade-off comparison between the cost of losing business opportunity and the cost of ensuring security to a specific level. The decision maker will be able to decide which security level to select according to cost benefit analysis. Neubauer did not provide any implementation process.

In the same category, proper controlling is suggested to ensure security governance (Von Solms, Thomson, & Maninjwa, 2011), aligning the Taiwanese national policy with standards of ISO/IEC 27001 and BS 7799 (Ku, Chang, & Yen, 2009), and Information Security Management System evaluation (Jo, Kim, & Won, 2011) are being continually explored to their crucial importance to Cyber Security. To the same above reasons, these works do not qualify to be used as CS implementation framework.

### **2.2.2. GUIDELINES**

Fielden (2011) shed the light on a possible direction towards a cyber security domain. He has identified six factors that determine a good cyber security strategy which are: purpose and role of information security, societal trends, human elements, interaction and complexity, information security management and changing technologies. We believe that Fielden's research is very general because it does not suggest an implementation approach and further research will be needed to drill down and up to a structure level of an implementation framework.



According to a recommendation by the European Network and Information Security Agency (ENISA), ICT systems must be secured in Europe coherently across geographical borders and should be followed consistently over time (ENISA, 2011). The Agency helps in identification and analysis of threat trends over time, suggests policy implementation and infrastructure protection, but does not identify a specific framework.

Most of the international information security strategies include guidelines in order to facilitate their implementation (Government of Australia, 2009; HM Government, 2010; Suid-afrika, 2010; The White House, 2009; U.S. DoD, 2011). Phahlamohlaka et al. (2011) suggest an Awareness Toolkit as an approach to implement the strategy of South Africa. Estonia Department of Defense (2008) has suggested the implementation of strategy in phases to be executed by security implementation vendors coordinating with various related government organizations. Unfortunately, these strategies do not provide clear implementation or performance controls to holistically monitor the implementation.

### **2.2.3. CUSTOMIZED FRAMEWORKS**

A suggested implementation framework for Jordan CSS is presented in a local conference (Jordan University) by Otoom (2011). Otoom's framework is targeting Jordan only, needs a validation model, suggests a very high level organizational structure and does not widely address performance measures that monitor and control the implementation process.

The Integrated Governance, Risk and Compliance (iGRC) Consortium is doing an on-going research program to protect UK. iGRC is using their integrated Enterprise information security management system, extended with the open interoperability protocol (GRCiP) along with network sensor technologies from participant companies. The goal is to automatize threat level and control status changes in real-time so that critical information infrastructure is made more resilient and be able to withstand the increasing number of attacks. We consider this framework a mixed between management and technology however it is specialized for UK.(iGRC, 2011).The research on iGRC framework is still on-going and it does not address holistic performance controls.

An application of the ITU framework has been applied to some countries like Morocco (el Kettani & Debbagh, 2008). The ITU framework is step by step management plan and is very abstract in the sense that no security engineering components are identified.

#### **2.2.4. SECURITY MATURITY AND METRICS MODELS**

Security Maturity models are used to ensure that an organization has adopted a set of procedures or standards in the security domain including IT assets, humans, and legal aspects. Examples of these models are: Security Engineering Capability Maturity Model (SSE-CMM), ISO/IEC 21827, Capability Maturity Model Integration (CMMI®), Information Security Program Maturity Grid (ISPMG), Security Maturity Model (SMM), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®), and security metrics bodies. More about security maturity models can be found at (Wangenheim, Hauck, & Salviano, 2010).

The SSE-CMM is used to ensure that an organization apply in practice security engineering principles. It can evaluate security engineering practices; customers can evaluate providers' security engineering capability, and thus establish organization capability-based confidence (Carnegie Mellon University, 2010). In 2002, it has been approved as ISO/IEC 21827 International Standard and henceforth its certification is maintained by the International Systems Security Engineering Association (ISSEA). The ISO/IEC 21827 additionally covers areas of concurrent interaction within the organization and with other organizations, and project execution cycle (Tsohou, Kokolakis, Lambrinoudakis, & Gritzalis, 2010). The CMMI® is a five level process improvement approach whose goal is to help organizations improve their performance by focusing in improving their internal process and enhancing security related processes (Ahern, Clouse, & Turner, 2008). The ISPMG is a tool composed of five stages of security maturity and five measurement categories that may be used by management in evaluating an enterprise's maturity from the perspective of information security (Stacey, 1996). The Fraunhofer Institute for Software and Systems Engineering (ISST) has developed SMM to assess a company's IT security (Kurrek, 2002). OCTAVE® is risk-based information security strategic assessment and planning. In OCTAVE® model, the organization will set the security strategy based on current evaluation of organization risks. (Alberts & Dorofee, 2003).

Security metrics are often qualitative methods to measure how an organization is secured. There are many guiding standards and good experiments of security metrics such as: Federal Information Processing Standards Publication (FIPS PUB) 140-2, The Information Technology Security Evaluation Criteria (ITSEC), Trusted Computer System Evaluation Criteria (TCSEC), The Common Criteria for Information Technology Security Evaluation (CC or common criteria), the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) and NIST Special Publication 800 series. (Wang, 2005).

FIPS 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements for cryptographic module to protect sensitive information within computer and telecommunications systems (NIST, 2001). The ITSEC is a structured set of criteria for evaluating computer security within products and systems used in Europe. The ITSEC framework is originated from TCSEC, a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The ITSEC criterion is currently superseded with the CC which is an ISO/IEC 15408 standard. The ISO/IEC 15408 computer security certification standard is a framework to specify security functional and assurance requirements. The CTCPEC is a combination of TCSEC and ITSEC, a computer security standard published by the Communications Security Establishment to provide evaluation criteria on IT products. The Special Publications of the 800 series present documents of general interest to the computer security community and is based on ITIL's research, and governmental organizations.

In the same category, the German IT protection Manual is a collection of huge documents (more than 3000 pages) from the German Federal Office for Security in Information Technology (BSI) that provide useful information for detecting weaknesses and combating attacks in IT environment (Henze, 2000).

All of the studied work in this section cannot be generalized to cyber security strategy implementation framework because most of them are very specific to one aspect of cyber security (maturity or metrics). Moreover, none of them has identified any implementation framework for cyber security.

### **2.2.5. GENERIC FRAMEWORKS**

A generic framework for strategy implementation is suggested in Barnat(2005) online book “strategy management” which includes these components: devising rewards and incentives, shaping the corporate culture, and strategic leadership. We believe this framework is very high level and is more suitable to business strategy rather than cyber security strategy implementation.

Trim & Lee (2010) suggest a generic cyber security Framework consisting of a cyber security Management Framework (CSMF) overseen by a Security Framework for Protecting Business, Government and Society (SFPBGS). The CSMF provides a linkage between outputs of SLEPT (Social, Legal, Economic, Political, Technological) analysis and SWOT (Strengths, Weaknesses, Opportunities and Threats). The main goal of Trim’s work is to allow managers to incorporate counter intelligence and places risk in a manageable context. Unfortunately this model, do not have a performance measure and does not target strategy implementation.

### **2.2.6. PROVIDER SPECIFIC ARCHITECTURES AND FRAMEWORKS**

The IBM Center for the Business of Government reports that there is a need of CIO at the state level (Goodyear, Goerdel, Portillo, & Williams, 2010) . The IBM security framework consists of five components: data, people, network, infrastructure, and process. This framework influence governance, risk management and compliance through complete IBM solutions. A more detailed technical framework is the IBM blueprint which shows the components of IT security management and IT security infrastructure capabilities. The IBM Framework and IBM blueprint suggest a secure-by-design approach which means that implementation of this framework will need to use IBM software and hardware solutions which finally limits the user needs in terms of costs and needed customization at the national level (Buecker, Borrett, Lorenz, & Powers, 2010).

Oracle® has a set of library guidelines and reference architectures called Oracle Reference Architecture (ORA) that can be used by organizations to plan and execute their IT initiatives. They suggest a conceptual architecture to show how architectural concepts are

associated with information security within the ORA.(Toal, Herron, Rees, McLaughlin, & Young, 2011)

### 2.2.7. OPEN ARCHITECTURES

These frameworks are developed for external consumption by other than the framework developer. There are various available Enterprise Architecture (EA) frameworks that vary in: completeness, visual aspects, simplification, and representation. Table 2-1 lists a sample of international frameworks. Readers may refer to other frameworks and their relationship with security from frameworks websites, or research works such as Jalaliniya thesis (Jalaliniya, 2011, pp43)

Table 2-1 List of International Enterprise Architecture related to Cyber Security.

Framework	Description
Zachman	Define a matrix of stakeholders' viewpoints, and six main abstractions in describing information security. It does not consider explicitly security concerns.(Zachman International®, 2012)
FEAF	Federal Enterprise Architecture Framework. A structure for organizing Federal resources. Security standards are part of FEAF components.(office of Management and Budget, 2012)
DoDAF	Department of Defense Architecture Framework. The focus is to understand complex EA models to facilitate decision making. Does not have any specific viewpoint for security.(U.S. DoD, 2009).

Framework	Description
TOGAF	Open Group Architecture Forum. Describe guidelines, models and methods of developing EA. Addressed security architecture explicitly in the Architecture Development Method, but not Security Methodology.(The Open Group, 2012)

Although there are industry accepted Enterprise Information Security Architecture (EISA) frameworks such as: Those in Table 2-1, Sherwood Applied Business Security Architecture (SABSA), and Gartner EISA framework, EA frameworks helps to answer ‘what’ questions not ‘how’ questions as indicated by EA consultant company (EAdirections, 2007). Moreover, most of the EA frameworks are used in financial and insurance sectors and to our knowledge they have been never used specifically for cyber security on a national level which might deliberate there usage in our context (Oda, Fu, & Zhu, 2009). Our research is not intended to replace such frameworks, but utilize and build on such frameworks.

### 2.3. VIEWPOINTS

The Viewpoints-oriented approach is used in software engineering to structure requirements. It is particularly useful when vast number of stakeholders is involved. Usually, different stakeholders will have different views for a system requirement which makes exploiting this approach towards CSS implementation appealing. During CSS implementation a multidisciplinary stakeholders of possible divergent interests will involve in the implementation. With the application of the viewpoints, conflicts can be confronted and requirements are conciliated. More information about the viewpoint usage refer to (Nuseibeh et al., 2003; Salem, 2010).

## 2.4. PERFORMANCE MEASUREMENT

Performance indicators can support management of complex systems. One dimensional performance measures cannot give the full picture of performance due to its being favoured toward one performance aspect such as financial aspect while not considering other aspects such as customer, or risk aspects. Nowadays financial and non-financial performance measures are available. According to Neely (1999) more than 3600 articles in performance measures have been published between 1994 to 1996, which then was described as a revolution. Taticchi (2008) has indicated that Performance Measurement and Management (PMM) has notably increased in the last 20 years. For more information about performance measures models and framework in various domains, readers might refer to (Nudurupati, Bititci, Kumar, & Chan, 2011; Paolo Taticchi, Tonelli, & Cagnazzo, 2010).

Good measurement techniques or frameworks should balance between financial and non-financial measures, and they should allow measurement of the security achievements at the national level (Nudurupati et al., 2011; Paolo Taticchi et al., 2010). Cyber security strategy implementation should also have a performance measurement to control the performance during implementation. There are several frameworks and techniques that can be used for performance measurement. The BSC is a strategic planning and management system used widely by commercial companies, governments, and non-profit organizations worldwide to align business activities to strategy. According to Bain & Company reports, the Balanced Scorecard (BSC) is being used internationally in more than 63% of worldwide entities (Rigby & Bilodeau, 2011). In its first version by Norton and Kaplan (1992), the BSC has four perspectives: Financial, Customer, Internal Business Process, and Growth perspectives. These perspectives are integrated together, with each assigned a list of performance measures, to assist in calculating the cumulative performance of a strategy during implementation.

There have been many modifications to the BSC to make it suitable for specific domains. Herath et al (2010) has modified the Kaplan version of BSC to measure security of an organization. Other works in BSC with IT, service management and BSC integrations can be found in (Goldman & Ahuja, 2011; Györy, 2012; Heavey & Murphy, 2012; Marcos &

Rouyet, 2012; Wu & Kuo, 2012). In CHAPTER 4, we will demonstrate how our proposed performance model builds upon available BSC solutions.

## **2.5. BELIEF NETWORKS**

Belief Network (BN) has been used in many application areas and mostly in threat assessment and security prediction. Kondakci (2010) has used BN to analyse and quantify information security risks caused by various threat sources. According to Kondakci, BN can be applied for various IT aspects such as information security evaluation. Al-Salloum et al. (2011) applied BN to analyse and quantify threats. Shin et al. (2012) propose a way to model the risk propagation using BN. Houmb et al (2010) have used BN to model trust based system to measure security level. BN is also used for cyber threat assessment of cyber-attacks and prediction in (Gonsalves, Call, Ho, & Lapsley, 2011). A Large engineering project risk management using a Bayesian belief network, is suggested in (Lee, Park, & Shin, 2009). More about BN concept can be found in (Pearl, 2011).

## **2.6. CONCLUSION**

Security frameworks have been adopted to secure cyberspace. Most of them target a specific domain or developed for specific entities. To our knowledge, there is no complete CSS implementation framework at the national level except for few ones illustrated in Sections (2.2.2, 2.2.3, 2.2.5) that have major drawbacks.

These drawbacks indicate that the defence against cyber-attacks has appeared to be generally fragmented and varying widely in effectiveness. Where there are significant efforts that have been taken in the developed countries, several developing countries have taken little or no efforts in cyber security domain. One of the major international challenges that are still valid is the need to consolidate cyber security efforts on the national level.

Moreover, aggregating performance of cyber security strategy implementations across national level has not been thoroughly considered in literature. In the next two chapters, we present a holistic framework and a performance measurement approach that can both work together to overcome the shortcomings of the current solutions.



## **CHAPTER THREE**

### **HOLISTIC CYBER SECURITY STRATEGY IMPLEMENTATION FRAMEWORK (CSS-IF)**

## **CHAPTER 3**

### **HOLISTIC CYBER SECURITY STRATEGY IMPLEMENTATION FRAMEWORK (CSS-IF)**

#### **3.1 INTRODUCTION**

Security frameworks have been adopted to secure cyberspace. From the literature review (CHAPTER 2), we found that most of these frameworks target a specific domain or developed for specific entities. While several cyber security frameworks look on management perspective of cyber security, little research has been conducted on cyber security from engineering perspectives. Current solutions has major drawbacks: lack of holistic view of cyber security strategy implementation frameworks (e.g. UK government; Nguyen, 2012), lack of holistic performance measures for holistic implementation frameworks (e.g. Bartol et al.; 2009), lack of cooperation between governments and related entities in the cyberspace (e.g., Schjolberg & Ghernaouti-Helie, 2011), and lack of research on global risk mitigations(e.g. U.S. Gov; Maughan, 2010).

These drawbacks indicate that the defence against cyber-attacks has appeared to be generally fragmented and varying widely in effectiveness. One of the major international challenges that are still valid is the need to consolidate cyber security efforts at the national level. Moreover, aggregating performance of cyber security strategy implementations across national level has not been thoroughly considered in literature. This chapter presents a holistic framework that overcomes the shortcomings of the current solutions and resolve the issues presented in the problem statement Section 1.3.

To justify the importance of cyber security strategy implementation framework below we quote from the governments of UK, U.S. and Thailand. In UK, the cyber security strategy implementation is ‘too slow ‘. UK government states that “The government's lack of a framework for its cyber security strategy implementation has been previously highlighted .....” (Nguyen, 2012) . In the U.S., “The current public private partnerships are inadequate for taking R&D results and deploying them across the global infrastructure” (Maughan, 2010). Thailand is now in a process of creating national cyber security policy. Thailand

government states that: “The Information and Communications Technology Ministry will draw up a national cyber security policy framework to fight online crime and fraud.”(Pattaya Today, 2012).

First, we summarize current cyber security research perspectives. Then, we discuss the framework development methodology. After that, we illustrate the framework. Finally, we summarize the chapter.

### **3.2 CYBER SECURITY RESEARCH PERSPECTIVES**

Cyber security research space is very sparse; subsequently researchers see security from different perspectives. Below is a sample from these perspectives. More details about such perspectives can be found in Cole Network Security Bible Book (Cole, 2011).

- Management perspective: usually researchers in this area concentrate on the actions or plans that should be adopted to manage and achieve current and future goals. Some organizations believe that it is just only managing risk and risk assessment to ensure security. Examples on this perspective can be found in Section 2.2.1.
- Standard and policy perspective: adopting out of the box security standards to protect, detect, and recover from security failures. For example, ISO27000 series provide best practice on information security management, risks and controls within the context of global information security management system.
- Security architecture perspective: Many organizations use COTS solutions to secure their information such as Cisco, IBM, or Oracle. Examples on this perspective can be found in Section 2.2.6.

### **3.3 FRAMEWORK DEVELOPMENT PROCESS**

To develop a holistic cyber security strategy implementation framework, a holistic cyber security strategy is assumed to be already in place (Fielden, 2011). Generally developing a framework for security implementation might be seen as: 1) an art: there is no manual for implementing security in interconnected systems, 2) security as a science: faults are resulted from interconnected hardware and software, 3) social

security: individual actions are major players in security, and 4) engineering or pattern based approach. For more details about these approaches, readers might refer to (Haley, Moffett, & Laney, 2006; Whitman & Mattord, 2011). Unfortunately, these approaches alone have some troubles: they may not form a complete or holistic solution to cyber security strategy implementation and due to the complexity of the problem; these approaches cannot be generalized as a national CSS implementation framework. Figure 3-1 shows the methodology used to develop the CSS-IF. This methodology consists of the following steps:

1. Study and analyze a set of current international cyber security strategies and its supporting implementation frameworks at the national and the organization level. In a nutshell, we collect as much as possible of related research documents in the last seven years. Since the implementation of cyber security covers many domains and perspectives, we select only the researches that are related to security engineering including: cyber security strategy guidelines, international security standards, and general security frameworks. Although, for completeness, we have touched other important areas such as management, awareness and capability building, the main core of these areas is left out of scope for future research. During this step, we got more than 200 works that are filtered out except those illustrated in CHAPTER 2.
2. Elicit common security features or components: by keeping an eye on the overall objectives of cyber security, we extract from implemented strategies the common cyber security components. In other words, we concentrate on the presented security features rather than the algorithm or domain of study. Then, we list these features as candidate features for our framework.
3. Eliminate all customized implementations and remove duplication, i.e., generalize components. The collected components or features are again filtered, combined if needed and generalized into new abstract components. For example, security features such as flexibility and agility are combined into one component named resilience component. For cleanness and readability of this research, we will not present this long list, however they are available per request.

4. Develop the framework to achieve security objectives. The CSS-IF is logically designed by applying security engineering concepts on the collected components resulted in step three above. The CSS-IF: 1) incorporates and integrates a selection of various components, and 2) tweaks and enhances components when necessary and 3) introduces new components necessary to make the CSS-IF a holistic framework. The developed CSS-IF is explored in CHAPTER 3.
5. Validate the framework using a comparison with other frameworks, a case study on Jordan CSS, and Bayesian Belief Networks. We will illustrate the validation in CHAPTER 5.

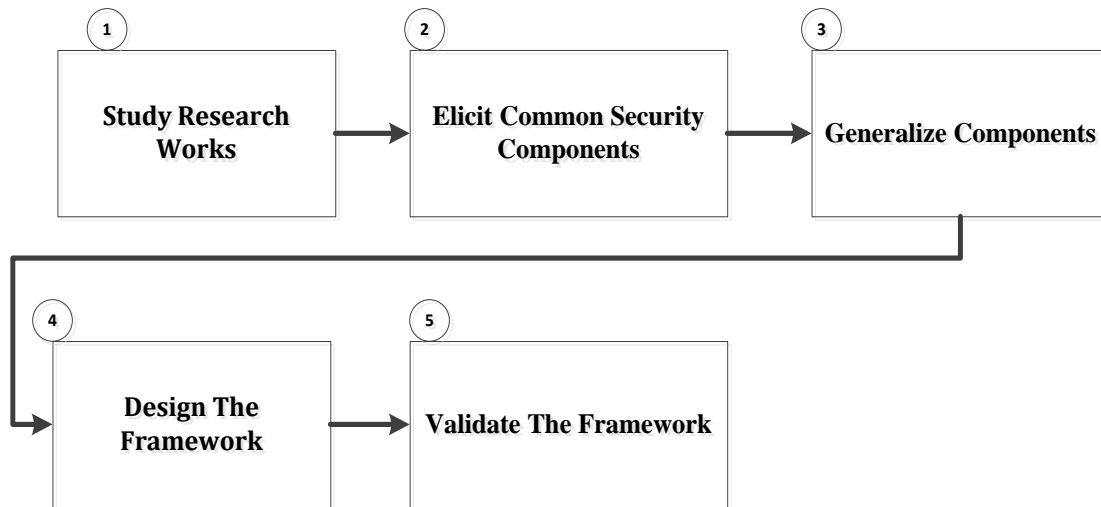


Figure 3-1 Process for developing the CSS-IF.

### 3.4 THE IMPLEMENTATION FRAMEWORK(CSS-IF)

The implementation framework is a set of security components that are interconnected to transform CSS into a security implementation objectives and thus enhancing the security level on the national level. In the context of our research, a holistic cyber security strategy implementation framework develops and/or integrates a set of high level conceptual security components, solutions, entities, tools, techniques, or mechanisms to collectively collaborate in order to implement cyber security strategies and thus enhances the security level on the national level. A component, in the context of this research, is a constituent part of the CSS-IF; the component may integrate one or more necessary functions or

solutions to help in the implementation of cyber security strategy towards achieving the overall cyber security objectives.

The CSS-IF takes a cyber security strategy written in natural language as an input and transforms it to security objectives that are measured against chosen security principles. The framework perceives cyber security in a top down approach. Figure 3-2 shows the conceptual view of the CSS-IF framework. The CSS-IF provides an overarching layer over available and intended cyber security solutions. The CSS-IF allows monitoring cyber security on a national level and at the same time it allows each entity to have its own technical and managerial details as long as this entity adheres to Nation-wide cyber security policies and regulations.

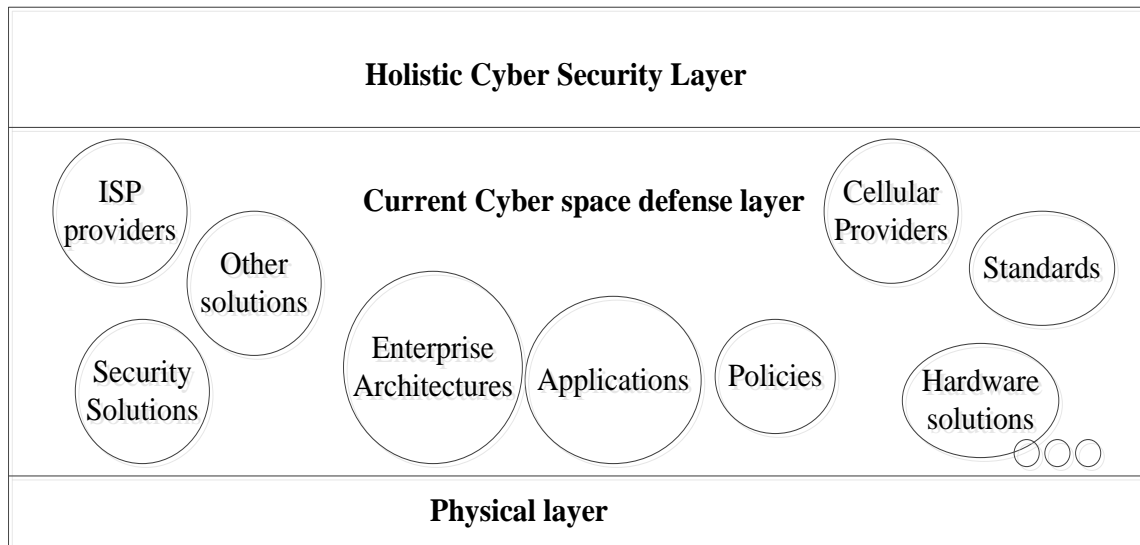


Figure 3-2 Conceptual View of Cyberspace Security Layers.

Figure 3-4 shows the detailed framework, however for simplicity we illustrate the framework step by step using the block diagram as illustrated in section 3.4.1.

### 3.4.1. CSS-IF BLOCK DIAGRAM

Figure 3-4 shows the major core components of the CSS-IF: CSS, Requirement Elicitation, Strategic Moves, Controls, Security Objectives and Implementation Framework Repository. The CSS-IF essentially facilitates transforming the cyber security level from the current state to the future state. Both current and future states related to cyber security

should be already documented directly or indirectly in the CSS document. Further analysis is required to make knowledge about these states more valuable and understandable which

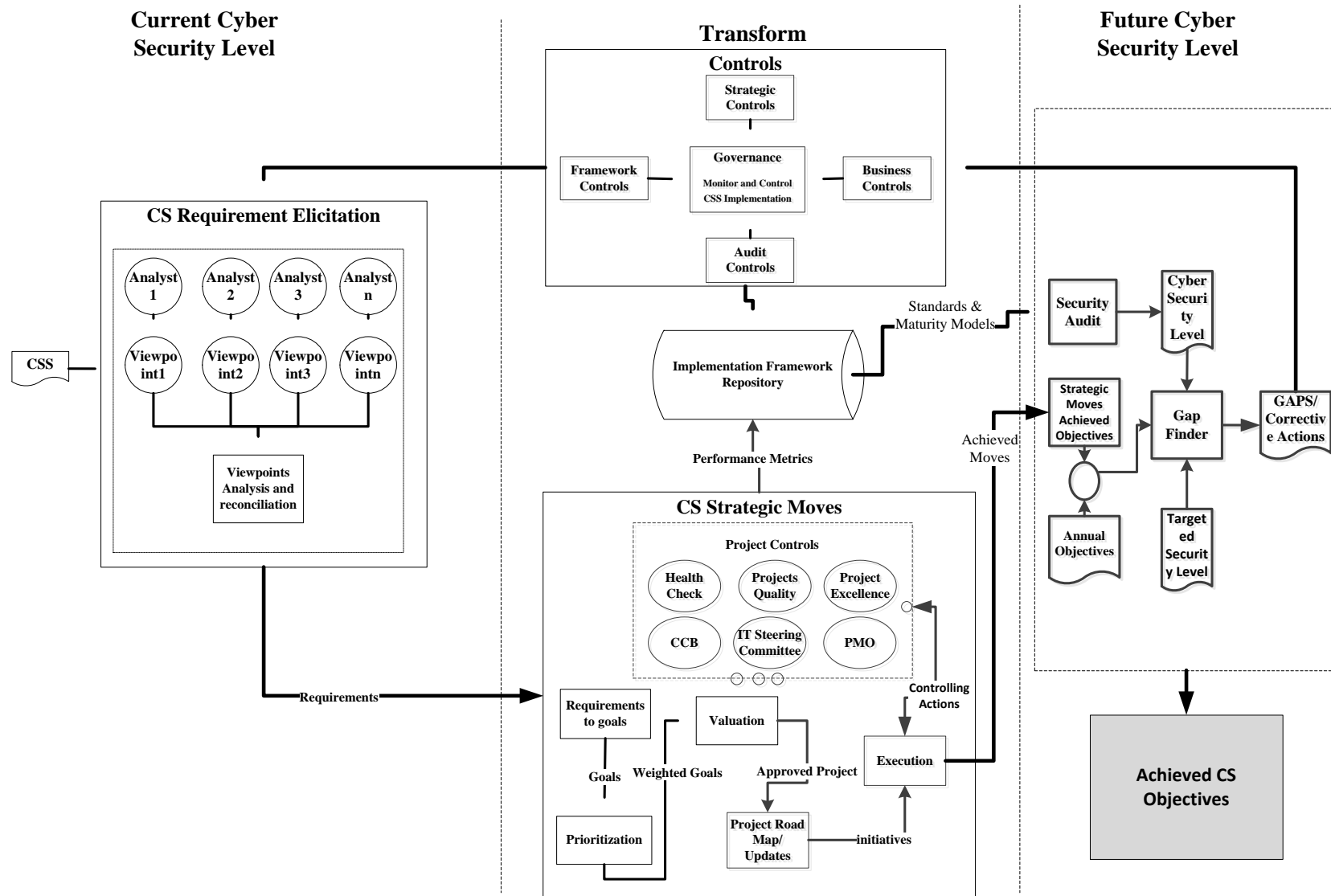


Figure 3-3 Detailed Cyber Security Strategy Implementation Framework(CSS-IF).



will be covered in the upcoming Sections. The CSS-IF proposes a methodology to analyze the CSS and break it down into well-defined requirements that will be eventually transformed into Strategic Moves. These Strategic Moves are executed under the defined framework controls in order to achieve the required security objectives. The implementation is guided and managed via the help of a focal implementation framework repository.

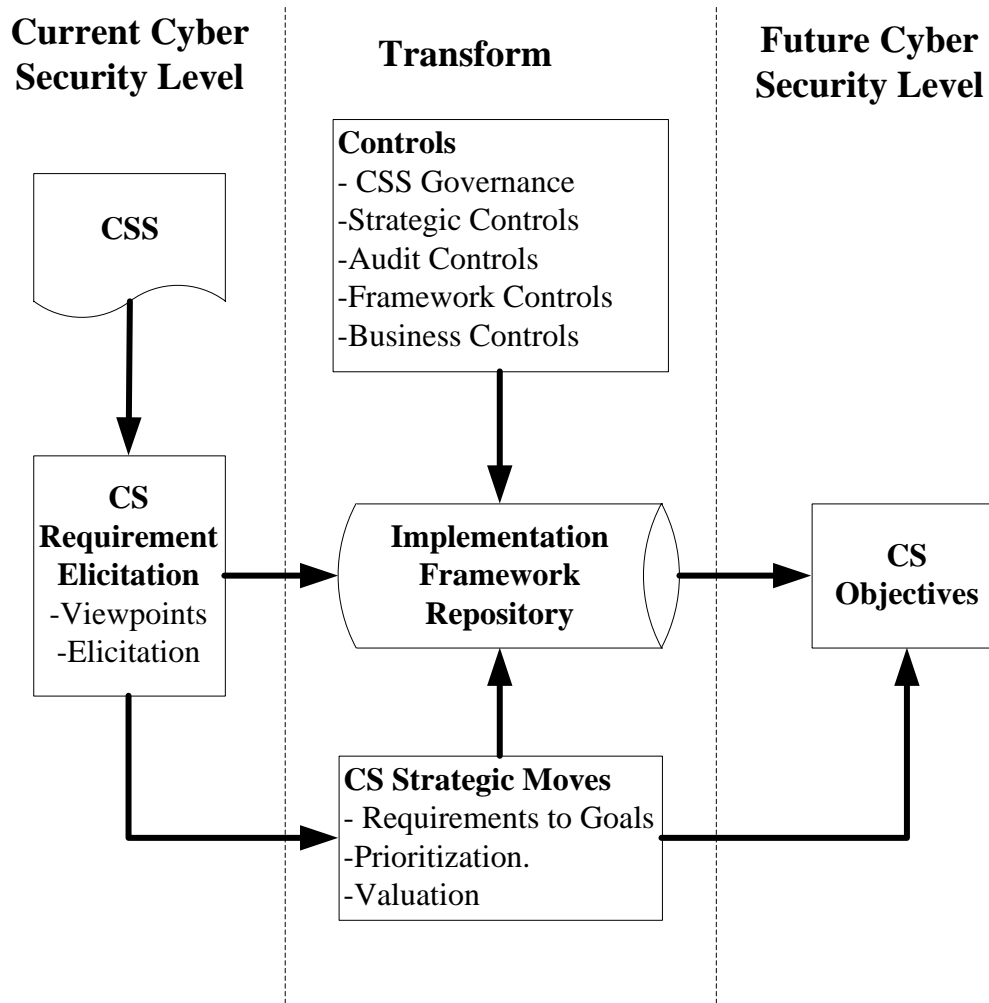


Figure 3-4 Block Diagram View of CSS-IF

### 3.4.2. CYBER SECURITY STRATEGY (CSS)

The cyber security strategy is a document that has guidelines on how to secure cyberspace. Many governments have developed CSS based on the reappraisal of information security

status in their corresponding countries (Estonia Department of Defence, 2008; Government of Australia, 2009; HM Government, 2010; International Telecommunication Union (ITU), 2011a; MoICT, 2011; Suid-afrika, 2010; The White House, 2011). These strategies recognize the threats imposed by the unprecedented revolutionary changes in Information Technology and the cyberspace environment. Usually, each country has its own cyber security strategy. As an example of these strategies, Jordan has developed the National Information Assurance and Cyber Security Strategy (NIACSS). The NIACSS identifies strategic objectives and national priorities. Refer to Section 5.2.1 for more details about the NIACSS.

According to Fielden (2011), a good CSS should include various clusters to ensure every aspect of cyber security into consideration. Fielden suggests the following clusters: purpose and role of information security, societal trends, human elements, changing technologies, information security management, and complexity and interactions.

### **3.4.3. REQUIREMENT ELICITATION**

The Requirement Elicitation converts the CSS from the natural language to a set of business and security requirements. Although the business requirement supports the security requirements, our concern in this research is the security requirements. The elicitation is important to break the CSS into manageable understandable requirements and identify Strategic Moves. We propose to carry out the elicitation using the concept of “viewpoints”, a concept that is being used in software engineering to elicit software requirements. Usually, different stakeholders will have different views for a system requirement which makes exploiting this approach towards CSS implementation appealing as we will have multidisciplinary stakeholders of possible divergent interests. The process for the elicitation is detailed in (Figure 3-5). For more information about viewpoints, refer to Section 2.3.

The CSS is taken as an input to the analysis process. The Analysis Team should include members with related expertise in the related domains. The more professional and diverse the team, the more successful the analysis output will be. The “viewpoints” of the team are gathered, incorporated, and summarized. The Analysis Team must resolve conflict,

generate a reconciled understanding, and make sure that analysis is complete. For an example on a “viewpoints” technique applied to a case study, refer to Section 5.2.2.

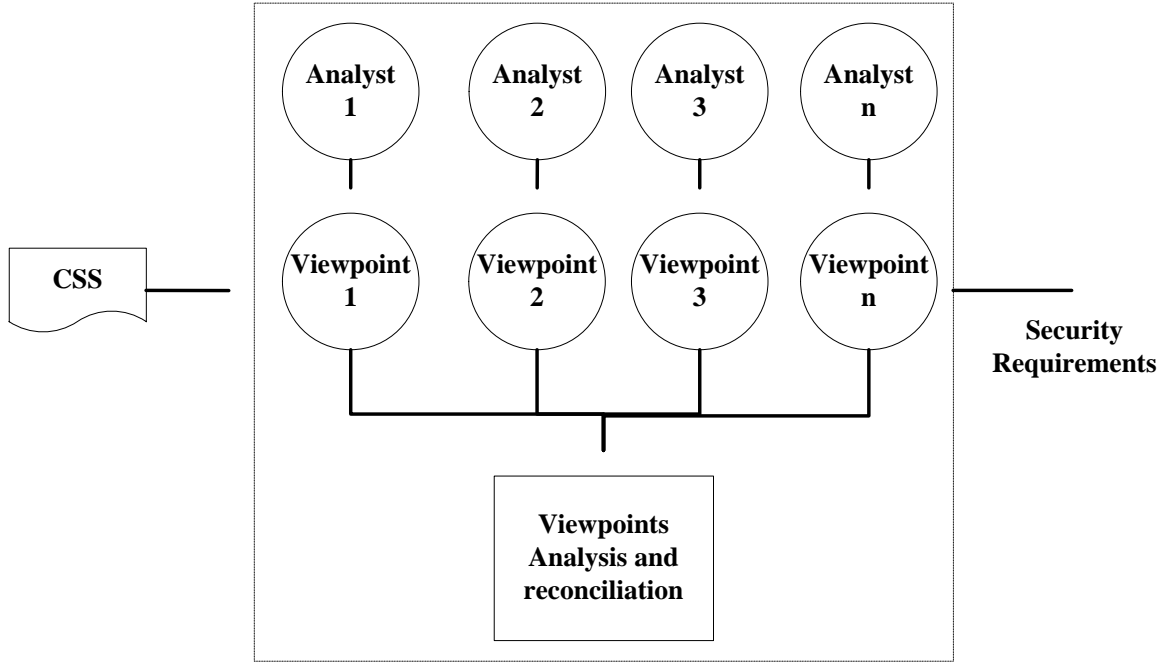


Figure 3-5 Requirement Elicitation Component.

### 3.4.3.1. REQUIREMENT ELICITATION FORMULATION

We formally define Requirement Elicitation process as follows: given a set of analysts,  $\mathbf{A} = \{a_1, a_2, a_3, \dots, a_n\}$  and the set of all domains of all analysts  $\mathbf{D} = \{d_1, d_2, d_3, \dots, d_h\}$  and  $\mathbf{WD}$  is the set of the corresponding weights of domains  $\mathbf{WD} = \{wd_1, wd_2, wd_3, \dots, wd_h\}$ . Each analyst has an experience in years  $e_i$  in any domain  $d_i$ . In practice, selecting analysts is subjective however the team should be diverse enough with proper expertise. We define the Expertise of an analyst as in formula ( 3-1 ):

$$Expertise(A_k) = \sum_{i=1}^h e_i wd_i \quad (3-1)$$

Where:

$A_k$  is any analyst  $\in A$ .

$h$  is number of all domains in  $D$

$e_i$  is experience of analyst  $A_k$  measured in years or months in domain  $d_i$ .

$wd_i$  is the weight of domain  $d_i$ .

This formula will help us in forming the analysis team to select those having maximum expertise. Each analyst will ultimately have an effect on the holistic security implementation, specifically on each requirement identified directly or indirectly by his/her viewpoint.

Let  $R$  be the set of all possible requirements in the CSS document=  $\{r_1, r_2, \dots, r_m\}$ . Let an effect factor ( $F$ ) be defined as the ability to identify a requirement in  $R$ . This function shows whether an analyst can identify a requirement or not. The effect factor  $F$  can be defined as function of analysts and requirements as in formula ( 3-2 ):

$$F(A_k, R_s) = x, \quad x \in \{0, 1\} \quad (3-2)$$

Where:

$A_k$  is any analyst  $\in A$

$R_s$  is any requirement  $\in R$

$x$  any value in the set  $\{0, 1\}$ (i.e., the range of the effect factor).

In the set  $\{0, 1\}$ , zero means the analyst has failed to identify the requirement and one means the analyst has fully identified the requirement. In theory, an analyst may partially identify a requirement which means the effect factor will take a value between 0 and 1

exclusive. However, for simplicity we neglect this case and consider a partially identified requirement as if it is identified. For example,  $F(a_1, r_1) = 1$  and  $F(a_1, r_5) = 0$  means analyst ( $a_1$ ) has identified requirement ( $r_1$ ), yet failed to identify requirement ( $r_5$ ). The Strength of any requirement  $R_s$  is defined in formula ( 3-3 ).

$$\textbf{Strength}(R_s) = \frac{\sum_{i=1}^n F(A_i, R_s) \cdot \textbf{Expertise}(A_i)}{\sum_{j=1}^m \sum_{i=1}^n F(A_i, R_j) \cdot \textbf{Expertise}(A_i)} \quad ( 3-3 )$$

Where:

$R_s$  is any requirement  $\in R$

$n$  is number of all analysts.

$m$  is number of requirements in the CSS document .

$F(A_i, R_j)$  is as defined by formula ( 3-2 )

The stronger the requirement, the more consensus the team has made on. Requirements with low strength values mean that these requirements were identified by few or less expertized team members. These requirements should go through a reconciliation process to decide if these requirements are valid, or they were identified by mistake and should be removed. Formula ( 3-4 ) illustrates the Requirements Acceptance Criterion.

$$\textbf{Requirment Acceptance}(R_s) = \begin{cases} \textbf{valid} & \textbf{strength}(R_s) \geq \theta \\ \textbf{need reconciliation} & \textbf{otherwise} \end{cases} \quad ( 3-4 )$$

Where:

$\textbf{strength}(R_s)$  is as defined in formula ( 3-3 ).

$\theta$  is the requirement acceptance threshold value.

***valid*** , requirements above threshold are accepted by the team.

***need reconciliation***, requirements below threshold need further refinement by the team and need to go through reconciliation process.

Figure 3-6 illustrates an example on applying formula ( 3-4 ) by showing list of requirement ordered by strength given a threshold value= 0.5. Requirements (r<sub>5</sub>, r<sub>1</sub>, r<sub>4</sub>, r<sub>7</sub>, r<sub>2</sub>, r<sub>3</sub>) are considered valid whereas requirements (r<sub>6</sub>, r<sub>8</sub>) should be considered further by the analysis team who will either accept or reject them depending on the reconciliation process.

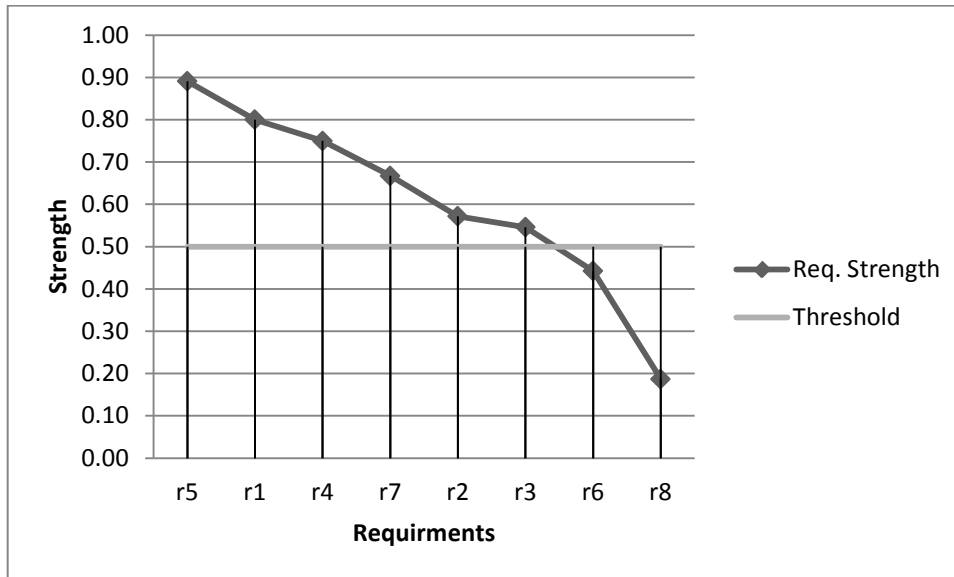


Figure 3-6 Requirement Acceptance.

We define Analyst Effectiveness shown in formula ( 3-5 ). This function rates the effectiveness of an analyst who is participating in the requirement elicitation

**Effectiveness ( $A_k$ )**

**( 3-5 )**

$$= \frac{Expertise(A_k) \cdot \sum_{i=1}^m F(A_k, R_i)}{\sum_{j=1}^m \sum_{i=1}^n F(A_i, R_j) \cdot Expertise(A_i)}$$

Where:

$A_k$  is an analyst  $\in A$

$n$  is number of analysts.

$m$  is number of requirements .

$F(A_k, R_i)$  is as in formula ( 3-2 ).

This formula will be useful to rate the effectiveness of analysis team. Such rating will serve as a feedback to select team members to engage in possible future cyber security requirement analysis.

Refer to Table 3-1 Requirement Elicitation Matrix. as an example to illustrate formulas ( 3-1 ) to ( 3-5 ). The table is filled using the formula ( 3-2 ). The higher the summation value across columns the more consensus on the identified requirement, whereas the higher the summation values across rows reflects the experience and the effectiveness of an analyst in identifying requirements. The above formulation opens a research direction towards formulating requirement elicitation as identified in Section 6.2 .

Table 3-1 Requirement Elicitation Matrix.

Analysis/Requirement	R <sub>1</sub>	R <sub>2</sub>	...	R <sub>m</sub>	Sum
A <sub>1</sub>	1	1	...	1	3
A <sub>2</sub>	0	1	...	1	2
...	...	...	...	...	...
A <sub>n</sub>	1	1	...	...	2
Sum	2	3	...	2	...

### 3.4.4. SECURITY STRATEGIC MOVES

Security Strategic Moves (we refer to it shortly as Strategic Moves) are actions taken to achieve one or more cyber security objectives. Strategic Moves are prescriptive and purposeful; they identify exactly what is to be done and directly act to achieve their objectives. Strategic Moves must not contradict each other; rather, they should complement. The Strategic Moves component has these processes 1) convert requirements to goals, 2) prioritize goals 3), security valuation, 4) build/update the project road map, and 5) place project road map into the execution process. See Figure 3-7.

Convert requirements to goals. Goals often identify measurable achievements on a yearly basis in the direction of achieving cyber security strategy implementation. The difference between requirements and goals is that requirements will possibly take long time to complete which complicates the measurement of security levels and audits. Usually governments have annual budgets that can be utilized rather than open budgets. To improve security level yearly, it is better to slice each requirement at the goal level and assign milestones in yearly plans accordingly. This process is a subjective process that takes input from many aspects such as: management, lessons learned, commitment plans, risk plans and professional expert judgment..



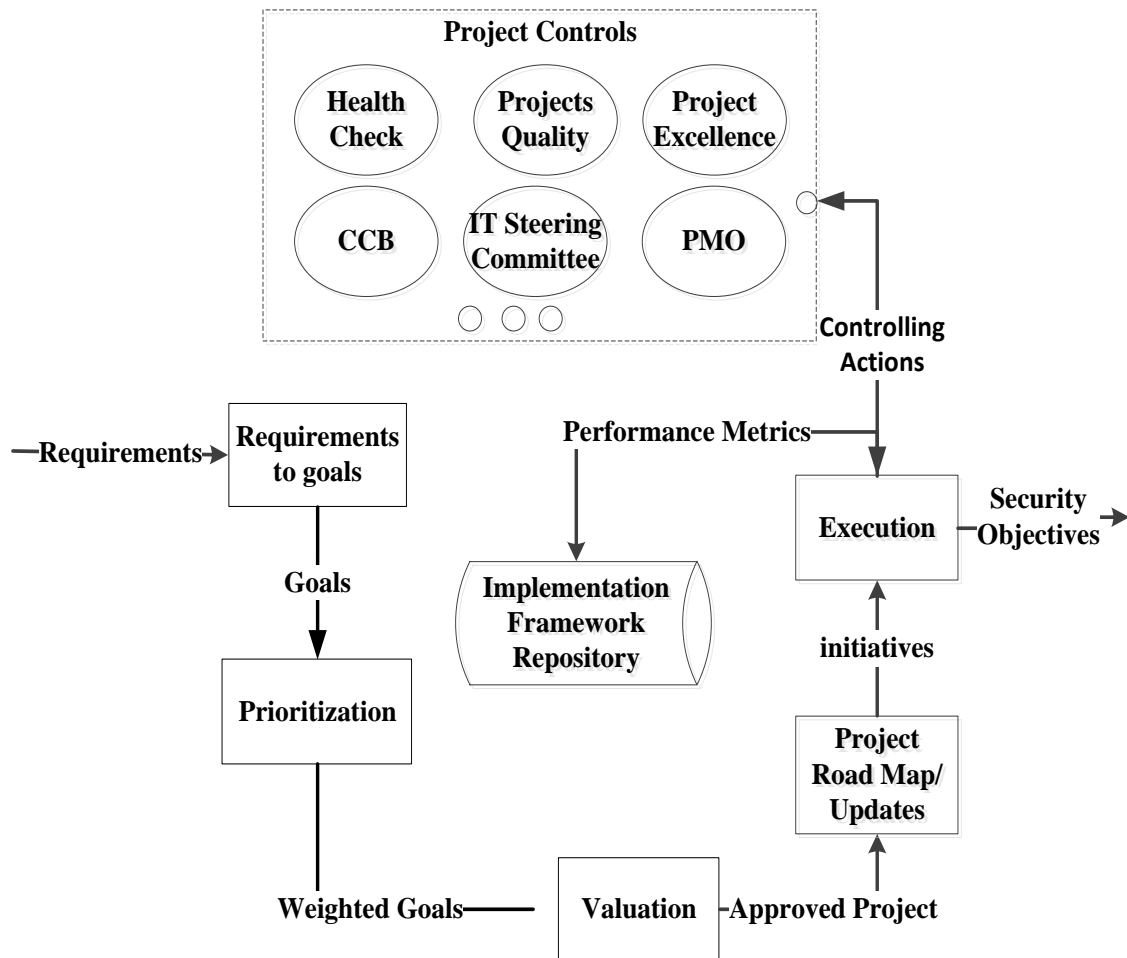


Figure 3-7 Strategic Moves process.

Prioritize goals. Prioritization orders the list of goals to be kicked in the Strategic Moves process based on goal importance. Prioritization is affected by many factors such as: timeline, budget, requirement dependency, management preference and many other factors. To do the prioritization, we suggest listing all Strategic Controls (Section 3.4.5.2) and weighting each goal against that Strategic Control. Though several factors can be added if needed by CSS-IF users. Other approaches might be adopted by the governance entity responsible for CSS implementation, if needed; Table 3-2 shows a goal weighting prioritization technique. The goal weighting is calculated using formula ( 3-6 ).

$$\overline{G}_k = \frac{Risk(G_k) \sum_{i=1}^n w_i v_i}{\sum_{i=1}^n w_i} \quad (3-6)$$

Where:

$G_k$  is the goal being weighted.

$n$  is number of controls.

$w_i$  is the weight of control  $i$ .

$v_i$  is the goal value with respect to control  $i$ .

$Risk(G_k)$  is the risk if goal  $G_k$  is not implemented,  $Risk(G_k) \in (0,1)$ ; subjectively determined by risk management team.

This Formula will calculate a weighted mean according to goal importance. The more value the weighted mean indicates a more important goal. In Table 3-2 Reduce Risk and Improve quality Controls has a weight of 50, 20 respectively. Using formula ( 3-6 ), and assuming we have only these two controls, we get the weighted mean of (Goal<sub>1</sub>, Goal<sub>2</sub>) values (2400/70, 1500/70), respectively. It indicates that although Goal<sub>2</sub> has a higher value in improving quality control, Goal<sub>1</sub> is more important than Goal<sub>2</sub> because it has higher weighted mean.

Table 3-2 Example - Goal Weighting Technique.

Strategic Control	Weight	Goal <sub>1</sub>	Goal <sub>2</sub>	...	Goal <sub>m</sub>
Reduce Risk	50	40	10	...	...
Improve Quality	20	20	50	...	...
...	...	...	...	...	...
Weighted Mean		...	...	...	...

Security Valuation. The Security Valuation process is used to approve the initiation of a new project or even a program. A business case is usually presented to Cyber Security steering committee showing analysis of requested budget and threat analysis as two important input factors. Then a decision is taken to approve or disapprove the initiation. The output of this process will only have projects that management is willing to implement in a specific year.

Build/update the project road map. The Project road map building process is triggered to place projects together in the optimum possible order. When projects are independent, we suggest using a tool such as the matrix shown in Table 3-3. However, for interdependent projects, we suggest using PERT charts such as the one shown in Figure 3-8. Many entities use PERT or Gantt charts. Refer to (Schwalbe, 2010) for details.

Table 3-3 Example-Independent Project Ordering.

<b>Cost</b>	High	4	5	6
	Medium	2	3	5
	Low	1	2	2
		High	Medium	Low
	<b>Priority (Pay Off)</b>			

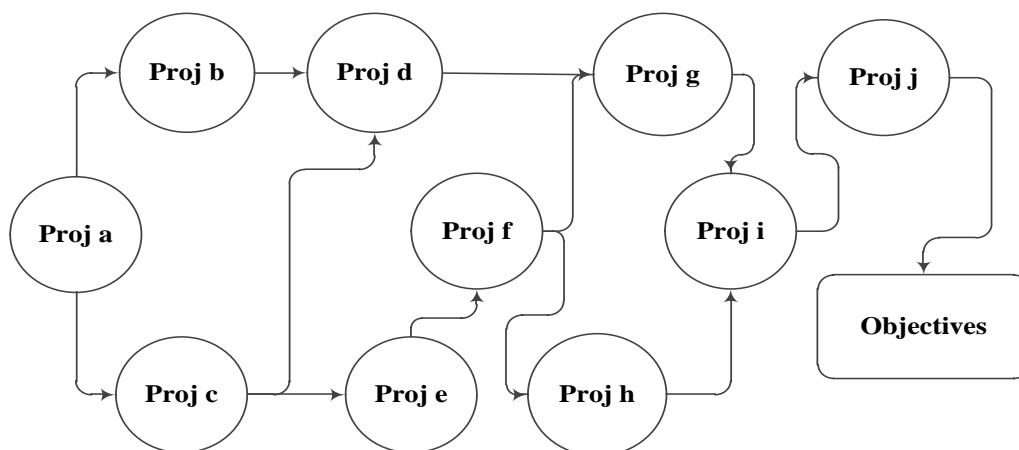


Figure 3-8 Example-Interdependent Projects Ordering.

Place project road map into the execution process. When projects start execution, they produce deliverables and record metrics in the CSS-IF Implementation Repository (see Section 3.4.5.4.1) for the purpose of managing, monitoring, and controlling the implementation. Related data is also recorded to help in corrective actions including request for change and request for proposal. Execution will be communicated to other entities such as Change Control Board (CCB), Security projects steering committee, Project Management Office (PMO), Projects Quality assurance, Project Excellence, etc. We mention project management controls for completeness, however we leave details out of scope since they are highly related to project management domain.

### 3.4.5. CONTROLS

Controls are used to monitor the CSS-IF by taking corrective or proactive actions to control the implementation. The Controls are governed by a governance entity that oversees the execution. See Figure 3-9.

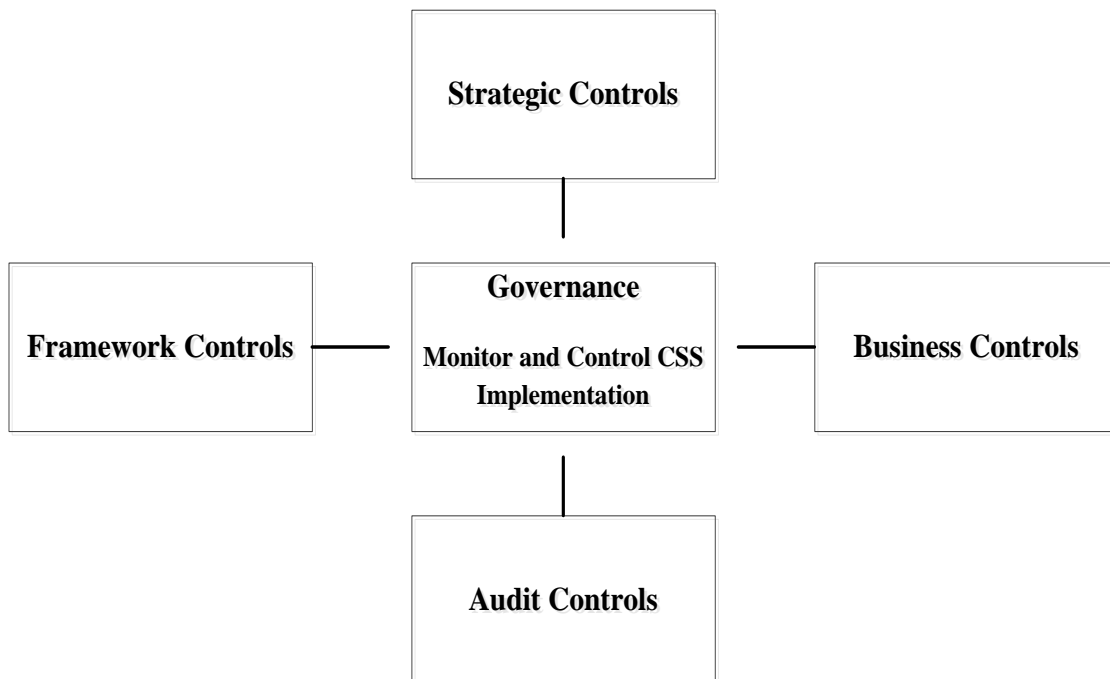


Figure 3-9 The CSS-IF Controls Interaction.

### **3.4.5.1. GOVERNANCE**

Implementing a CSS requires the existence of a governance entity, herein called Cyber Security Agency (CSA). The CSA is the entity accountable for executing, managing and monitoring the implementation. The Governance entity will make sure a proper chain of command is ensured between related entities. To sustain a proper implementation, the governance should be global governance, beyond the corporate governance. Global governance is generally defined as: “The complex of formal and informal institutions, mechanisms, relationships, and processes between and among states, markets, citizens and organizations, both inter- and nongovernmental, through which collective interests on the global plane are articulated, rights and obligations are established, and differences are mediated”.(Hewson & Sinclair, 1999; Rosenau, 1999).

The Information security governance is a tool to lower costs, increase overall productivity and produce value for relevant stakeholders. Figure 3-10 shows the relationship between the Global Governance, the Cyber Security Governance and Strategic Moves Governance. The subcomponents are samples and not intended to be complete. The governance provides strategic alignment, risk management, resource management, performance measurement and value delivery. More about information governance can be found in (Abu-Musa, 2010; Fitzgerald, 2011).

Governance has many components such as: CS Performance Management Control, Regulation Regime Control, and International Cooperation Control. The CS Performance Management Control is responsible for maintaining the proper chain of command between participating entities. It also can suggest changes on how the performance should be calculated in terms of goal weights or performance measures. While the Strategic Moves (Section 3.4.4) are collecting or updating performance data, the CS performance management control provides a holistic global view of all performance data and consequently applies any needed monitoring and controlling actions. In other words, the CS holistic performance control is implemented in Strategic Moves and controlled holistically in CS governance component. The Regulation Regime Control is very important in the sense that it will allow enforcing policies and applying law on crimes if needed. The International Cooperation Control will allow tracking threats and alert of new threats in

case neighbouring countries are facing cyber-attacks. Thus, cooperation is required to follow cybercrime internationally.

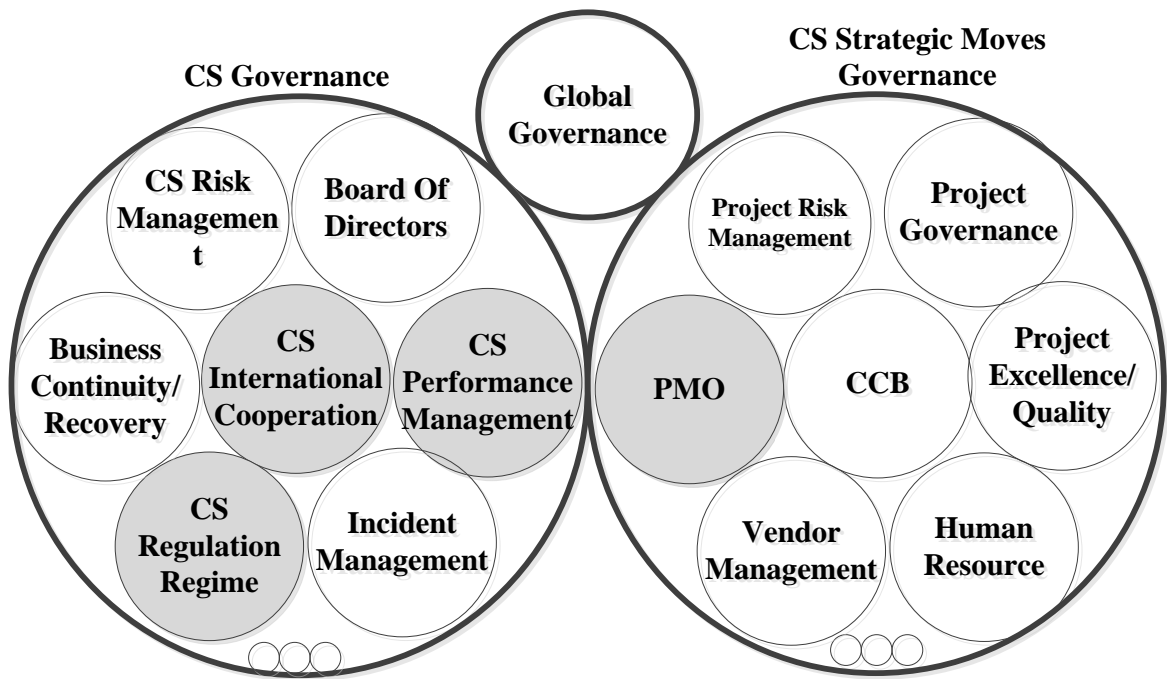


Figure 3-10 The CSS-IF Conceptual CS Governance.

We leave details for global CSA structure and governance for researchers in organization theory.

#### 3.4.5.2. STRATEGIC CONTROLS

The CSA, an entity responsible for CSS implementation, should deploy a set of applicable Strategic Controls that are considered, from CSS-IF's point of view, very significant to the success of the CSS implementation. The Strategic Controls should allow decision makers determine whether the CSA is achieving innovation, efficiency, and quality. Moreover, they will enable decision makers make any necessary adjustments and improvements as early as possible in the implementation process. These Controls should be adaptable to the culture and they should evolve with the CSA. i.e., the CSA should be able to add, enhance, or delete controls as needed. The set of Strategic Controls shown in Figure 3-11 may include, but not limited to:

- **Holistic Performance Control:** is used to make sure that the execution of any CS strategic move is performed within specified thresholds specified by each CS strategic move and according to the CS Performance Management Control (Section 3.4.5.1). The PMO should consolidate all performance data and aggregate it up to CS Performance Management Control. The implementation of holistic performance control of the CSS-IF is illustrated in CHAPTER 4.
- **Quality:** Quality controls will be applied throughout the whole implementation process to make sure plans are complete, correct, and best possible for the CSA. The quality metrics are inserted in the implementation framework repository.
- **Risk:** the CSA will identify risks, mitigate them and change the cyber security threat risk level according to the situation. If mitigation plans are not executed then it is possible that the execution of the implementation may be subject to failures.
- **Human Resources Incentives:** Since human resources are a major factor in any security solution, they must be encouraged to detect, monitor and repair possible damages. Some organizations give a percentage of profit on each successful project suggested by an employee. The human resources are managed using Human Resource Management Sub-Control in Section 3.4.6.
- **Evaluation and Correctness:** To check if the strategy is doing what is supposed to. Is the strategy fit for the country? Do we need to alter the strategy? The evaluation of the stage is outside the scope of this work.
- **Vigilance:** Vigilance will enable the CSA to proactively scan the environment in order to deal with unanticipated events of strategic value. These new or unforeseen events may make it necessary to change on-going plans.
- **Global Schedule Monitoring:** Although there is a schedule for the security roadmap, there is a critical need to monitor the overall schedule for both business and security projects along with other on-going activities.

The bottom line is that the CSA should deploy all necessary Strategic Controls that enable it to efficiently manage and control the implementation of the CSS towards achieving the required objectives within specified timeframes.

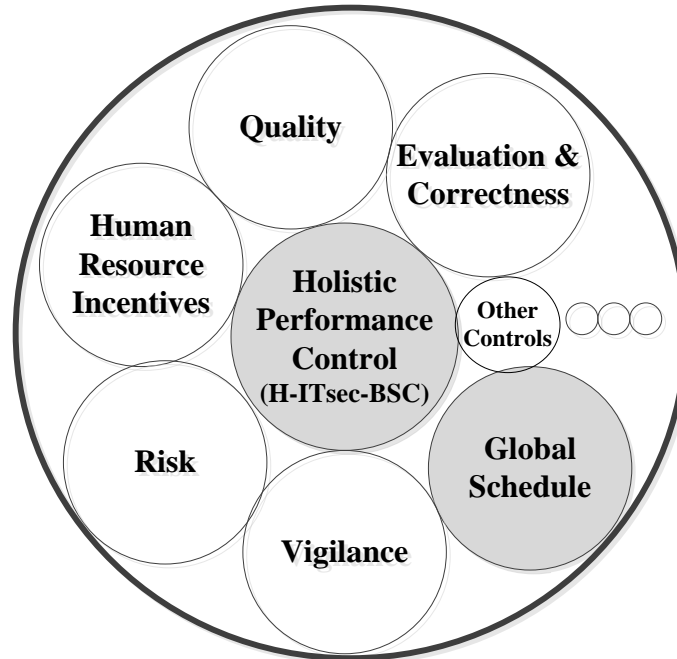


Figure 3-11 The CSS-IF Strategic Controls.

### 3.4.5.3. AUDIT CONTROLS

Audit Controls perform two major functions: 1) Check Security Maturity Level, and 2) Find gaps in the original CSS document or in the implementation process.. These two functions depend on the Maturity Models (Section 2.2.4), International Standards, Strategic Moves achieved objectives(Section 3.4.4) , Current Security Level, Targeted Security Level, and Annual Objectives(Section 3.4.7). Figure 3-12 shows the Security Maturity Level Check and Gap Finder processes. In order to achieve the first function, the current CSS implementation efforts are audited according to a set of chosen Security Standards and Security Maturity Models. The output of this functionality will be a report on the current cyber security level. To achieve the second function, the Gap Finder compares the Current Maturity Level to the Targeted Maturity Level using Strategic Moves and Annual Objectives as inputs. The Gap Finder reports if the current on-going implementation using



the Strategic Moves, is not able to achieve the Targeted Security Level which indicates that either the CSS has got an original flaws or the implementation process is not being executed as planned. The Gap report suggest corrective actions to global project roadmap by adding/updating Strategic Moves or further review on the current CSS document.

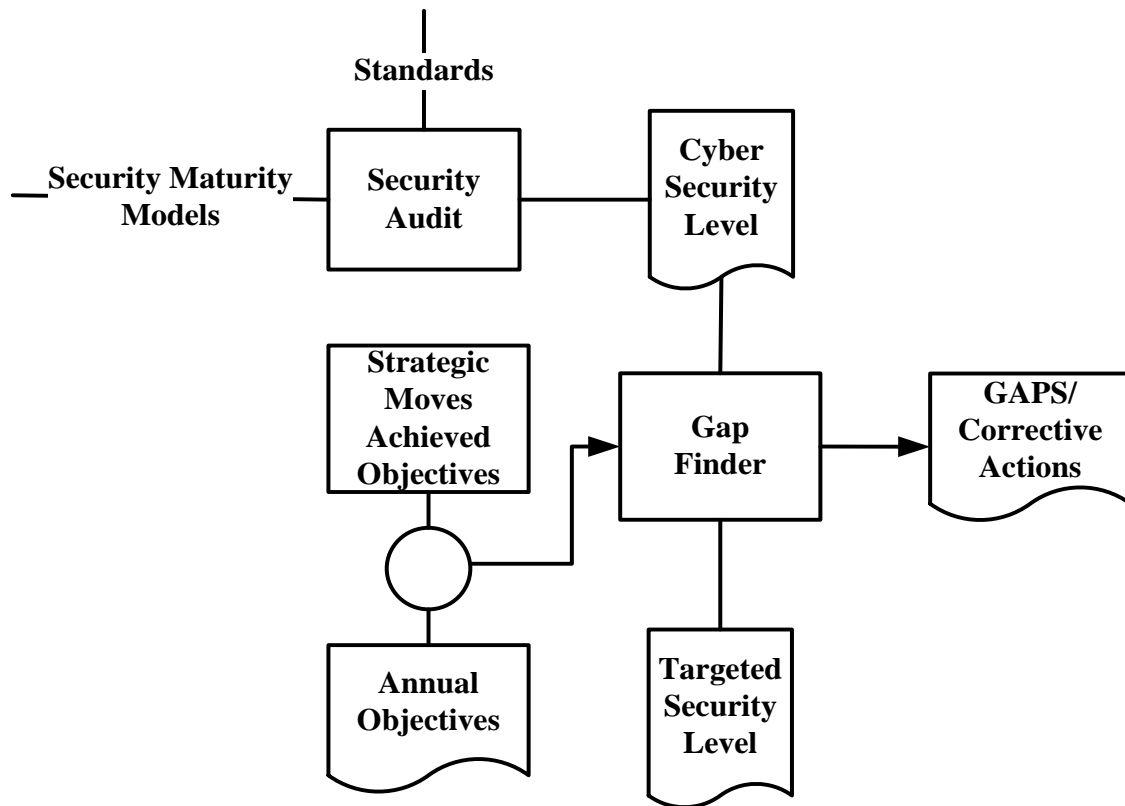


Figure 3-12 The CSS-IF Security Level and Gap Finder Processes.

#### 3.4.5.4. FRAMEWORK CONTROLS AND PROTOTYPE

First, we discuss the framework controls. Then, we illustrate the CSS-IF prototype.

##### 3.4.5.4.1. FRAMEWORK CONTROLS

The CSS-IF controls (Figure 3-13) are used to manage the framework itself and it includes these controls: Configuration, Framework Repository, Version Control, Universal Compliance Framework (UCF) database as implemented by UCF company (Unified Compliance Framework™ (UCF), 2012), Resilience, Access Control and Recovery Control.

The framework Configuration Control sets initial values to the framework properties, such as using a specific risk management standard, using a specific auditing standard, and so on. We will see more enhanced features in Section 5.3 that makes this framework not only configurable but it also has a configurable validation model. By using this control, the CSS-IF can reuse or integrate with other frameworks and/or standards if necessary. The Framework Repository is used to track and log monitoring activities during execution of the CSS-IF.

The Version Control can be used to track the version of the framework a government is implementing. It might be useful to track which version of the framework is being implemented especially if the framework is customized. The UCF aligns various standards and documents and maps them from one to another. This will be helpful if the implementers of the CSS-IF want to ensure compliance with national and international organizations that are possibly implementing different approaches and standards. The Resilience Control manages the unknowns while implementing the CSS. Risk management and change management play a major effect on this control. The Access Control component can be used to give rights for users, network access, etc., to access the framework components, reports, etc. The Recovery Control enables to recover the framework and it's supporting tools in case of a failure.

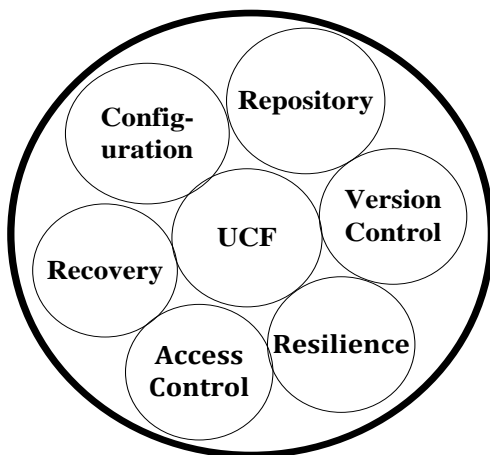


Figure 3-13 The CSS-IF Framework Controls.

Below we illustrates framework Settings, Configuration, Concurrency, Recovery, and Instantiation.

**// General Settings for any framework.**

Settings (Framework frm)

```
{
....
Frm.Name =Name; //assign a name to the framework
Frm.Domain =D; //choose the domain of the framework
Frm.Version=Version; //version of the framework
```

//Configuration for the framework.

Frm.Configuration= Configuration;

...

};

**//Configuring any framework**

Configuration (Framework frm)

```
{
```

Frm.Recovery= Recovery\_Technique; //chosen recovery technique.

//ensure correct results for concurrent operations

//chosen concurrency control technique.

Frm. Concurrency\_Control= Concurrency\_Control;

```
}
```

### **//Save State of any framework**

```
Save_State(Framework frm, Recovery_Technique)
```

```
{
```

```
...
```

```
Frm.Recovery= Recovery_Technique;
```

```
Frm.Save(Repository); //save the state of the framework in the framework repository
```

```
Frm.State=Current_State;
```

```
};
```

### **//Recover any framework**

```
Recover_Framework(Framework frm , Recovery_Technique);
```

```
{
```

```
Frm.Recovery= Recovery_Technique;
```

```
Frm.New_State= Frm.old_state; //recover the framework to its old state.
```

```
};
```

### **//Design pattern for implementation framework**

```
Framework_DP (Framework Frm, Domain D)
```

```

Throws exception Recover_Framework on failure;

{

....

//keep saving new states of the framework during execution
{ ....}

Frm.Settings = Settings(frm); //setup the framework

Frm.Configuration= Configuration(frm); //configure the framework

...

Frm.Run();// run the framework.

} //end framework Design Pattern.


//Instantiate Cyber Security Strategy Implementation Framework.

Framework_CSS_IF (Parameters,..)

{

String Name, Domain, ...

....

//set up the framework initialization parameters.

With Frm.Settings

{

. Name =CSS-IF; //assign a name to the framework

.Domain =CSS; //cyber security strategy domain

.Version=1.0; //version 1


//choose concurrency control technique.

.Concurrency_Control= ACID; // Atomicity,Consistency,Isolation,Durability

```

```
.Performance_Measure=H-ITsec-BSC; //holistic information security balanced score card
.Compliance_Standard= UCF; // universal compliance framework
.Governance= CSA; //cyber security agency
.Annual_Objectives=Annual_Objectives;
.Strategy=CSS_NAME;// name of strategy document.
}
```

### **//Configure Framework.**

With Frm.Configuration

```
{
.Risk= Project Institute Standard;// can use also other standards
.Quality= ISO 9001;// can use other quality standards
.Security_Standard= ISO27000; //can use any standard;
.Audit = ITAF; //IT Assurance Framework
.Maturity_Model =SSE-CMM; //Security Engineering Capability Maturity Model
....
}
Frm.Run(); //run the framework.
} //end framework Instantiation of CSS-IF.
```

### 3.4.5.4.2. FRAMEWORK PROTOTYPE

Figure 3-14 and Figure 3-15 show an example of a UML prototype diagram of the CSS-IF's main components. This example is not intended to be complete; it is only meant to illustrate the concept. As shown in the Figures (Figure 3-14 , Figure 3-15), the CSS-IF is transformed to a set of classes including, but not limited to: Viewpoint, Requirements, Goal Valuation, Strategic Controls, Business Management, Framework Repository, and the Security Strategic Moves –Objectives Mapper. This Section suggests that a complete CASE tool can be built to adopt and execute the methodology suggested by the CSS-IF.

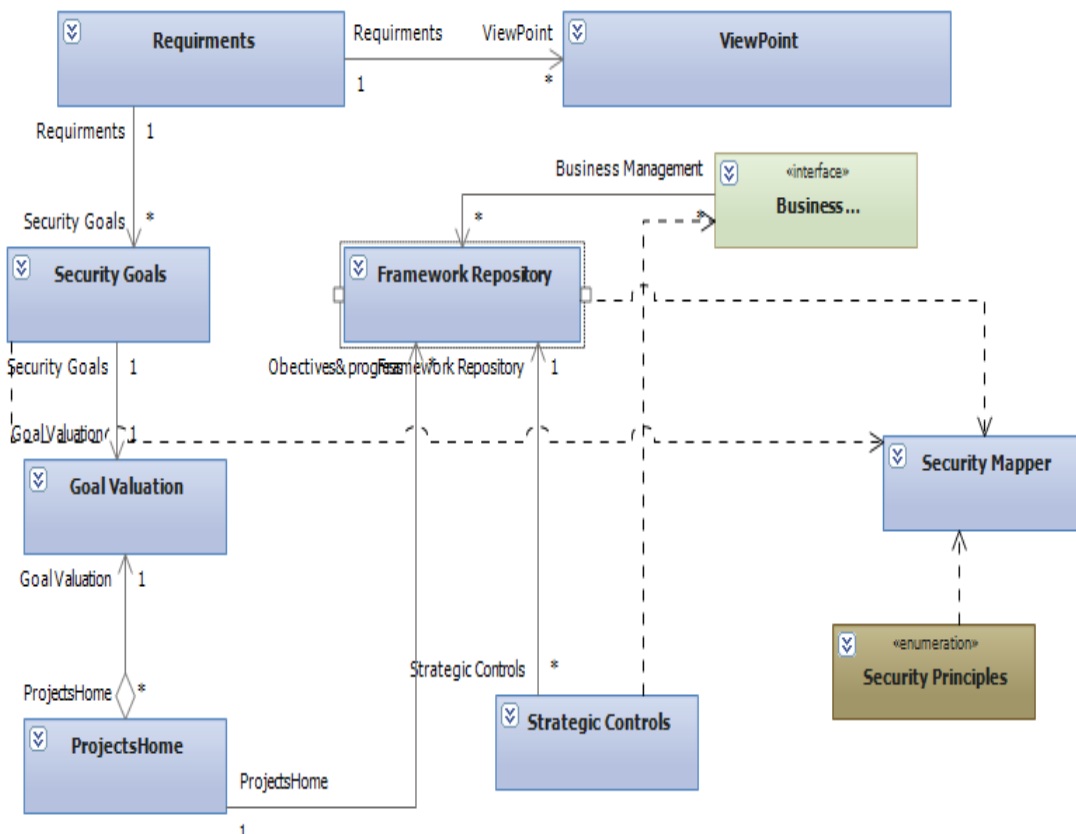


Figure 3-14 An Example of a UML Diagram for high level classes of CSS-IF.

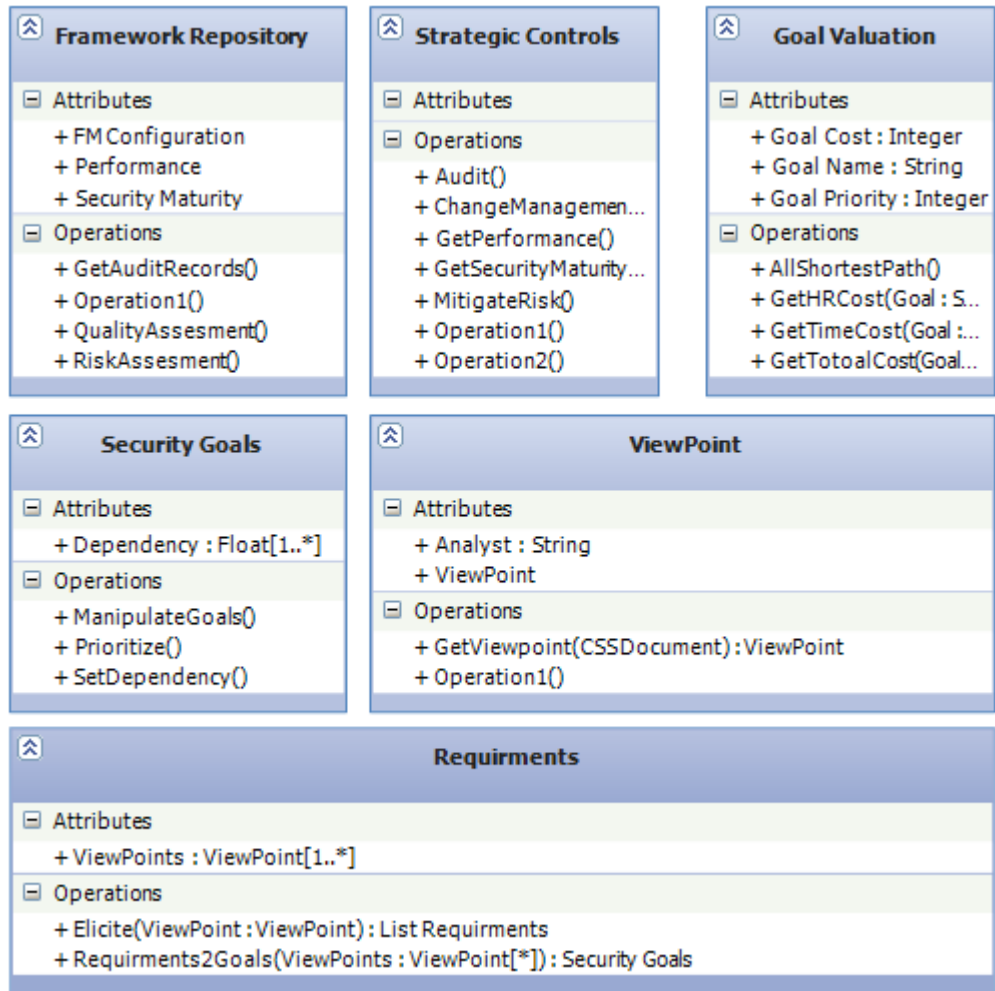


Figure 3-15 Sample UML Requirements, Viewpoints and Security Goals Classes.

### 3.4.6. BUSINESS CONTROLS

The business component controls (Figure 3-16) include but not limited to: Regulation Management, International Cooperation Management, Recovery Management, Incident Management, Human Resource Management, Vendor Management, Commitment Plan, Change Plans, Awareness and Capability Building, etc. Business component controls span many other components with an overall objective to ensure operational activities execution.

These components are outside the scope of this research and mentioned here for completeness and thus researchers in relative domains can do further research to enhance the CSS-IF from business perspective. Here, we mention Commitment Plan, Vendor



Management, and Change Plan as a few examples on business controls. The Commitment Plan is important to ensure budget, people, and technology are available when needed. The Vendor Management ensures proper contracting formulation and monitors activities executed by parties that are executing cyber security goals from contracting perspective. The Change Plan will bring different entities to cooperate and engage in a consolidated effort towards achieving the required Cyber Security objectives.



Figure 3-16 The CSS-IF Sample Business Controls.

### 3.4.7. CYBER SECURITY OBJECTIVES

As discussed in Section 3.4.5.1, the CSA must deploy all necessary Controls to achieve the cyber security objectives identified in the CSS (Long Term Objectives). Throughout this thesis, objectives are meant to refer to cyber security objectives. Annual Objectives help measure performance of CSS-IF on a yearly basis. The Annual Objectives will guide the planning, expose priorities, and form a basis for organization, collaboration and evaluation. We want to highlight two major issues: long term objectives should be broken down into

annual objectives and there is a need to come up with more accurate measures to these objectives so that implementation progress can be assessed and controlled. During the execution of Strategic Moves, achieved objectives are compared with Annual Objectives using Audit Controls illustrated in Section 3.4.5.3.

#### **3.4.8. IMPLEMENTATION FRAMEWORK REPOSITORY**

The Implementation Framework Repository is a focal component that helps manage, monitor, track, and control the implementation process. This component can contain but not limited to: project management tools, strategic planning tools, PMO required tools and dashboards. The need for such repository along with the need to have a configurable framework (Section 3.4.5.4.1) calls for a need to develop a CASE tool to facilitate adopting and executing the CSS-IF.

### **3.5 CHAPTER SUMMARY**

In this chapter, we have proposed a holistic, coherent, and systematic cyber security strategy implementation framework (CSS-IF) that essentially facilitates transforming the cyber security from the current state to the required future state. The CSS-IF major core components are: CSS, Requirement Elicitation, Strategic Moves, Controls, Security Objectives and the Framework Repository. Controls includes: Governance Controls, Strategic Controls, Audit Controls, Framework Controls, and Business Controls.

The CSS-IF proposes a methodology to analyze the CSS and break it down into well-defined requirements. We exploited and enhanced a “Viewpoints” approach to elicit requirements and developed a set of formulas necessary to help accepting requirement and selecting analysis team members. Requirements will eventually be prioritized, evaluated, and executed as a set of Strategic Moves under the control of 1) project controls (Section 3.4.5.1) such as PMO, CCB, steering committee, project excellence, and 2) framework controls. These Strategic Moves are executed in order to achieve the required security objectives. During execution, Strategic Moves metrics are recorded in the CSS-IF’s Repository so proactive and reactive changes could be taken during the holistic performance measurement (CHAPTER 4). The achieved objectives are measured and

compared with the planned objectives through the Gap Finder to make sure that cyber security goals are satisfied.

The CSS-IF is enabled with all the necessary components that help translating the abstract high level requirements into actions that are implemented towards achieving the required security objectives. A CASE tool is suggested to implement the components and the methodology proposed by the CSS-IF. This tool is expected to manage, guide, monitor, and control a CSS implementation on a holistic level.

## **CHAPTER FOUR**

### **CSS-IF PERFORMANCE MEASUREMENT**

## CHAPTER 4

### CSS-IF PERFORMANCE MEASUREMENT

#### 4.1. INTRODUCTION

Performance measurement is the process that identifies if current actions being taken during the implementation process are within acceptable thresholds and if corrective actions are required. Good measurement techniques or frameworks should balance between financial and non-financial measures, and it should allow measurement of the security achievements at the national level (Nudurupati et al., 2011; Paolo Taticchi et al., 2010). There are several frameworks and techniques that can be used for performance measurement. A literature review of state of the art performance measurement can be found in (Nudurupati et al., 2011) and more details in Section 2.4. Traditional approaches such Return on Security Investment (ROSI) and Annual Loss Expectancy (ALE) do not suite security due to struggling in determining the value of security investment versus returns. It is known that a security incident can affect reputation or even be catastrophic such as Stuxnet worm (Constantine, 2011).

Performance was listed as one of the Strategic Controls in (Section 3.4.53.4.5.1) however this control was deferred to be discussed in this chapter. To implement this component, we suggest exploiting an approach based on Balanced Scorecard (BSC). The BSC is a strategic planning and performance measurement technique used widely by commercial companies, government, and non-profit organizations worldwide to align business activities to strategy during implementation. Norton and Kaplan model the BSC with four perspectives: Financial, Customer, Internal Business Process and Growth perspectives (Kaplan & Norton, 1996, 2004; Kaplan, Norton, & others, 1992; Klein, Kaplan, Chemical Bank (New York, & Corporation, 1999). These perspectives are integrated and linked together. Each perspective is assigned a list of performance measures to assist in calculating the cumulative performance of a strategy during implementation.

The BSC is a good choice for framework performance management due to many reasons: 1) the high usage of such a framework worldwide. According to Bain & Company reports, BSC is being used internationally in more than 63% of worldwide entities (Rigby & Bilodeau, 2011). Sawalqa et al. (2011) reports that 35.1% of Jordanian entities employ BSC, 2) the BSC balance the use of financial and non-financial measures with leading and lagging indicators, 3) the BSC provides a holistic view of organization performance by monitoring goals that are linked to an organization strategy , and 4) “It is distinct from other strategic measurement systems in that it contains outcome measures and the performance drivers of outcomes, linked together in cause-and-effect relationships” (Norreklit, 2000, p.67) .

First, we illustrate the Information Security Balanced Score Card (ITsec-BSC) suggested by Herath(2010). Then, we propose and enhancement to ITsec-BSC to make it fit for the CSS-IF needs. Finally, we conclude this chapter.

#### **4.2. ITSEC-BSC AS RELATD TO CSS-IF**

Although the BSC was used originally for Business it has been modified for IT (Györy, 2012). Herath et al. (2010) has modified it to be used for information security frameworks which makes it a useful enabler that serves as a performance component in the CSS-IF. Herath’s BSC is named (ITsec BSC); it consists of four components as follows:

- The Business Value Perspective: The major concern of information security is ensuring protection of information against loss, disclosure, damage or disruption. This perspective covers the security principles such as Confidentiality, Integrity and Availability. So this perspective fully aligns with CSS-IF goals.
- Stakeholder Orientation Perspective: Ensuring that desperately stakeholder needs, behaviours, actions are taken into consideration of information security. Our proposed CSS-IF incorporates communications with various stakeholders ranging from workers, users, managers, customers and even third party entities.

- **Internal Process Perspective:** The set of actions, and procedures that are followed in the organization to ensure security. The CSS-IF has a set of policies, processes and other components that need to be carried out towards achieving cyber security. So this perspective aligns with CSS-IF.
- **Future Readiness Perspective:** Threats are constantly evolving and thus there should be a future thinking of expected threats and planning and acting against them. This could be achieved through the acquirement of new technology, tools, and preparing security professionals for new challenges. The CSS-IF has a set of controls including: Awareness, Vigilance, Capability Building, Risk Management, Quality and other controls that align with this perspective.

Figure 4-1 shows that the ITsec-BSC: 1) concentrates on business value rather than the financial perspective. All other perspectives are also mapped to new meanings compared to Kaplan BSC. Refer to (Herath et al., 2010, pp 75) for a comparison between ITsec-BSc and BSC of Kaplan, 2) is built for a level of an organization and below, and to our knowledge it has not been used for cyber security at the national level. Since the cyberspace strategy is at the national level then it is more likely that the execution of such a strategy will take several years and so each goal may take long time to get results of lagging indicators. In other words, the strategy map/dashboard will be idle for long time and decision makers cannot take actions with no available information, 3) many problems may arise from the points 1,2; the BSC can point out problems not how to reveal them (Self, 2004), and the BSC is “seen as myopic and ignores the activities and initiatives that goes beyond the original targets” (Othman, 2008). Consequently, the CSS-IF will not be able to track the cause of the degraded performance, so decision makers will not be able to take necessary actions unless a suitable holistic performance measure is enabled.

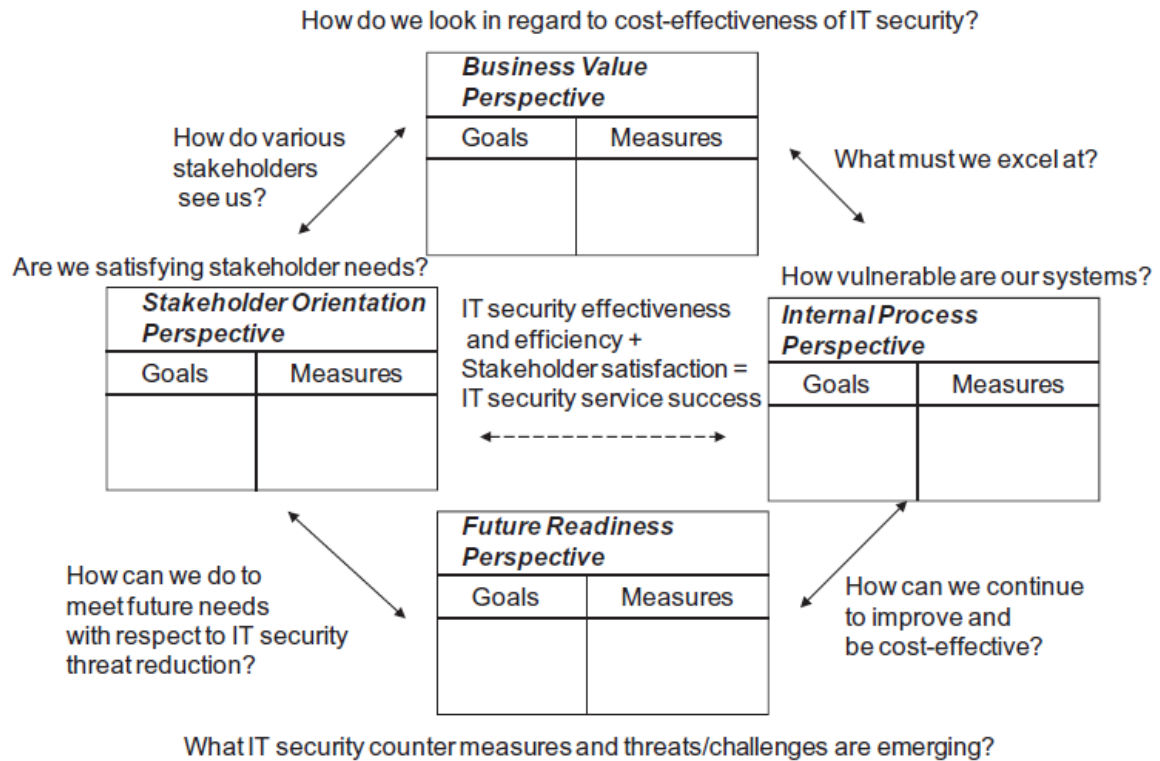


Figure 4-1 ITsec BSC Model, Herath et al., 2010.

#### 4.3. PROPOSED PERFORMANCE MODEL

We propose an enhancement to Herth's ITsec-BSC to make it fit for the CSS-IF needs. We call the new enhanced BSC a holistic IT Security Balanced Scorecard (H-ITsec-BSC). The H-ITsec-BSC enables the CSS-IF to manage, monitor, and control performance on a national level; it aggregates the performance state from all involved entities executing cyber security initiatives. The CSS implementation involves government entities, private sector and even the citizens. While the ITsec-BSC will not be used on citizen's level, it will be used for various organizations and private sector companies. Many organizations will hide details of their BSC and only expose a small portion of their BSC to related entities for privacy reasons, unless the relevance of these details is mandated by law and or regulations. Moreover, each organization has its own goals which may be subset or parallel to the CSS implementation goals. For example, an Internet Service Provider(ISP) might have



initiatives to enhance customer services, and at the same time have a mandatory role to execute one of the national CSS objectives such as protecting national internet gateways.

The H-ITsec-BSC is linked to entities to be able to provide the required overarching view or holistic performance. This link can be implemented by exploiting the primary/foreign key concepts used in the relational data models. A primary goal on the holistic level may be satisfied via achieving one or more than one sub-goals by the participating entities. With this link to the involved entities, we can track who is doing what, and therefore managers will be able to take corrective actions. In other words, if a goal leading indicator is degraded then managers, can know who is responsible for such low performance and actions can be taken holistically.

Figure 4-2 shows the conceptual proposed enhancement. Each participating entity is running its own version of BSC, and possibly other performance measurement techniques. Each entity performs its own part in implementing CSS goals. The H-ITsec-BSC enables measurement at the national level. It aggregates results from various participating entities and links the sub-goals to the CSS major goals. The aggregation can be a weighted average, summation, or any other suitable algorithm selected by the CSA as deemed necessary. The aggregation process must be configurable and allows using different algorithms to aggregate data for different goals. For example the awareness and capability building goal identified in a CSS might have several sub-goals being executed by different entities; national TV will run an awareness campaign for citizens, a security company will train professionals on how to prevent email attacks, another campaign will be conducted online to get e-commerce users be aware on how to prevent credit card frauds, etc. Our proposed Holistic BSC help in solving the problems pointed out by (Self, 2004) and (Othman, 2008) discussed in previous Section.

#### 4.3.1. HOLISTIC PERFORMANCE FORMULATION

We formally define Holistic performance measurement process as follows: given a set of goals in the CSS document  $\mathbf{G} = \{ g_1, g_2, \dots, g_n \}$ . A set of Entities  $\mathbf{ENT} = \{ ent_1, ent_2, \dots, ent_h \}$ . Each Entity has a performance measure  $\mathbf{PM} = \{ pm_1, pm_2, pm_3, \dots, pm_x \}$  for each sub-goal. Then we define the following formulas:

List of sub-goals for a goal :

$$\text{sub\_goals}(G_k) = \{G_k Sg_i\}, \forall i = 1, m \quad (4-1)$$

Where:

$G_k$  is any goal  $\in G$ .

$Sg_i$  is any sub-goal  $i$  of goal  $G_k$

$m$  is number of sub-goals of goal  $G_k$

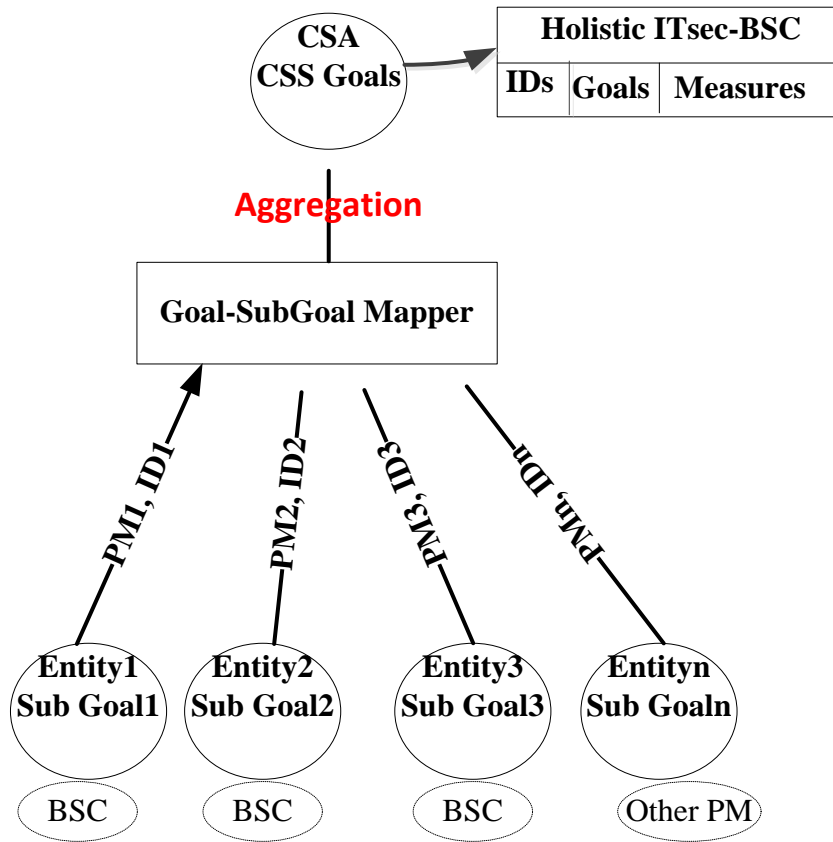


Figure 4-2 The CSS-IF H-ITsec-BSC Conceptual Model.

Formula ( 4-1 ) links all goals with their respective sub-goals, such that all performance metrics related to one goal will be linked with all its sub-goals.

Performance measures of any sub-goal are defined using:

$$\mathbf{Sub\_goal\_performance}(ENT_j, Sg_i) = PM_i \quad (4-2)$$

Where:

$ENT_j$  is any entity  $\in ENT$

$Sg_i$  is any sub-goal  $i$  as in formula (4-1)

$PM_i$  is the performance of any entity  $j$  on sub-goal  $i$

$$\begin{aligned} \mathbf{Holistic\_performance}(G_k) = \\ \mathbf{aggregate}(\mathbf{Sub\_goal\_performance}( \\ ENT_j, \mathbf{subogals}(G_k)) \end{aligned} \quad (4-3)$$

Where:

$G_k$  is any goal,  $\forall G_k \in G$

$ENT_j$  is any entity  $\in ENT$ , and is performing any sub-goal of  $G_k$

Figure 4-3 illustrates a possible dashboard for the H-ITsec-BSC for a specific goal. Assume that we have two goals Goal<sub>1</sub> and Goal<sub>2</sub> with the same weight for each sub-goal. Goal<sub>1</sub> has sub-goals (G<sub>1</sub>Sg<sub>1</sub>, G<sub>1</sub>Sg<sub>2</sub>, G<sub>1</sub>Sg<sub>3</sub>) and Goal<sub>2</sub> has sub-goals (G<sub>2</sub>Sg<sub>1</sub>, G<sub>2</sub>Sg<sub>2</sub>) with the performance values (90, 95, 25) and (70, 40) respectively. The holistic performance for (Goal<sub>1</sub>, Goal<sub>2</sub>) are (70, 55) respectively. Although (G<sub>1</sub>Sg<sub>1</sub>, G<sub>1</sub>Sg<sub>2</sub>) are achieving better than G<sub>2</sub>Sg<sub>3</sub>, the holistic performance is degraded to 70 because of G<sub>1</sub>Sg<sub>3</sub> associated with Entity (Ent<sub>2</sub>). In this case, managers can take correction actions if needed. Other dashboards and examples linked to CSS are shown when we apply CSS-IF on the NIACSS in Section 5.2.2.

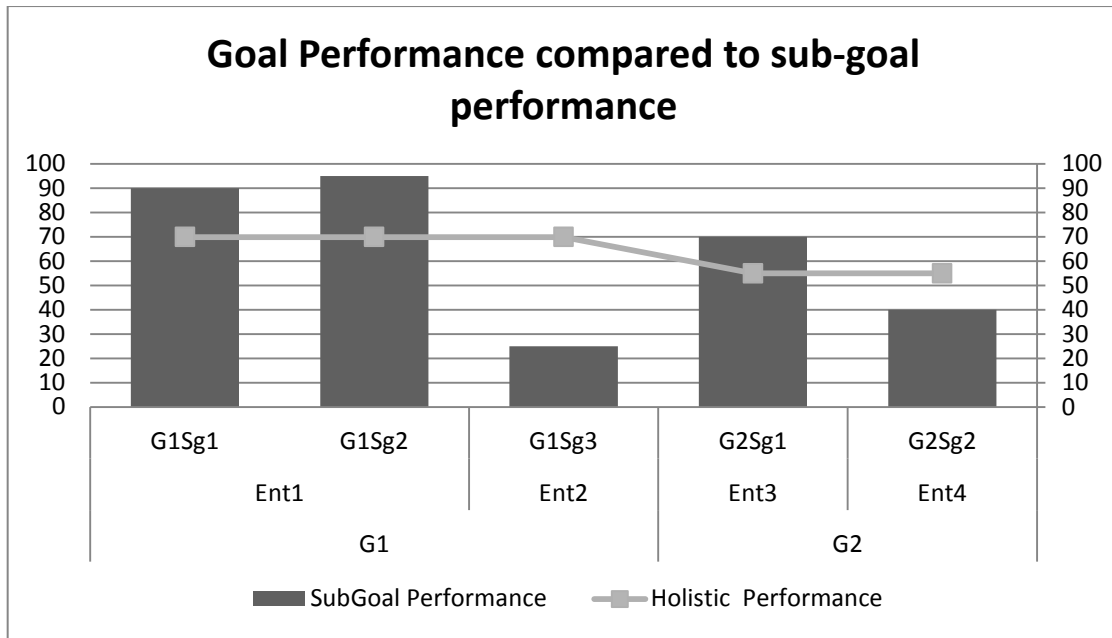


Figure 4-3 Example - Goal Performance Compared to Sub-goal Performance.

#### 4.4. CHAPTER SUMMARY

In this chapter, we illustrate how performance of the CSS-IF could be established by utilizing a modified version of ITsec-BSC called a Holistic ITsec-BSC (H-ITsec-BSC). The ITsec-BSC was originally proposed by Herath(2010). The H-ITsec-BSC allows performance measurement at the national level. It aggregates performance measure values from various entities executing CSS sub-goals. Aggregation is alleviated by proposing an approach that links and maps holistic goals with entities' sub-goals. The aggregation can be performed using a weighted average, summation, or any other suitable algorithm selected by the CSA as deemed necessary. The aggregation process must be configurable and allows using different algorithms to aggregate data for different goals.

The proposed H-ITsec-BSC allows the governance body of the CSS-IF including steering committees and Board of Directors to be able to track who is responsible for a variation between expected and current performance indicators. The H-ITsec-BSC manages, monitors, and controls the performance holistically, leaving each provider with its choice of the BSC version or any performance measurement technique as long as its metrics are exposed to the H-ITsec-BSC.

## **CHAPTER FIVE**

### **VALIDATION OF THE CSS-IF**

## **CHAPTER 5**

### **VALIDATION OF THE CSS-IF**

#### **5.1. INTRODUCTION**

In this Chapter, we validate the CSS-IF model proposed in CHAPTER 3. The enhanced ITsec-BSC (H-ITsec-BSC) illustrated in CHAPTER 4 is included in the validation process by default since it is already a component within the CSS-IF. We validate the CSS-IF by 1), validate CSS-IF through a case study, and 2) validate CSS-IF using Bayesian Belief Networks. Each of the validation techniques has its own strengths and weaknesses, however using they provide an acceptable proof of concept for the CSS-IF's validity. We believe that validation using surveys is also possible, though we leave this option for future research.

First, we validate the CSS-IF using a case study on CSS of Jordan. After that, we validate CSS-IF using Belief networks. Then, we compare our framework with other frameworks. Finally, we conclude with chapter summary.

#### **5.2. VALIDATION USING A CASE STUDY**

In the following subsections we apply the CSS-IF on the CSS of Jordan.

##### **5.2.1. BACKGROUND**

Jordan government has assigned the National Information Assurance and Cyber Security Strategy (NIACSS) formulation and implementation to the National Information Technology Center (NITC) which is a sub unit of the Ministry of Information and Communications Technology (MoICT). The NIACSS was motivated by the fact that current approaches to Cyber Security and Information Assurance (Cyber Security & IA) adopted by Jordanian Government organizations and private sector: are generally basic; not systematic; subjective; have no clear definition or boundaries, are not thorough; do not meet international standards; and do not deal effectively with threats emerging from cyberspace. Moreover, cyber security efforts in Jordan are not consolidated and risks are not addressed at the national level. The weaknesses in the current approaches, coupled with

rapid advancements in technology place the National networks and the Critical National Infrastructure (CNI) at risk.

There is a critical need to secure the national information infrastructures of Jordan to be resilient to malicious attacks or arbitrary disruption to maintain a high level of trust in these infrastructures across government, with the private sector, and within the citizenry. In Jordan, ICT sector contributes to 14.1% Gross Domestic Product (GDP) and the government is committed to maintain its growth (Int@j, 2011) . More information about the importance of ICT and ITES to Jordan economy can be found in:(Arab Advisor Group, 2010; Central Intelligence Agency/US, 2011; DOS & MoICT, 2010; Int@j & MoICT, 2010; Schwab, 2011).

The NIACSS identifies strategic objectives, national priorities, and an implementation road map. The strategic objectives aims to: strengthen National security, minimize risks to CNI, minimize damage and recovery time, enhance economy and National prosperity, and increase Cyber Security & IA awareness. National priorities address the critical needs required to guide the implementation towards achieving the National objectives. The National priorities cover the following areas: Risk Management, JO-CERT, Awareness, Standards and Policies, International Cooperation, Securing National Information Systems/NWs, CNI protection, NEC, and Legal Regulatory Regime. The implementation road map guides the implementation of the NIACSS. Successful implementation will demand collaboration within Government, with international partners, with the private sector, and with the citizenry of Jordan.

The NIACSS calls for establishing a well-defined organization called National Information Assurance and Cyber Security Agency (NIACSA) that oversees the efforts required to implement the NIACSS. The NIACSA is foreseen as a central national entity for governmental and non-governmental organizations regarding all information assurance and cyber security related issues.

We take the National Information Assurance and Cyber Security Strategy (NIACSS) as a case study to demonstrate the validity of the CSS-IF. For clarity, we go through CSS-IF's major components. This process is intended to show a proof of concept and is not meant to

be thorough nor comprehensive; complete analysis may take several hundreds of pages. For privacy reasons, in some cases real data is concealed and presented anonymously such as organization A, B, etc., or Incident1, 2, etc.

### **5.2.2. APPLYING CSS-IF FOR NIACSS**

To make our analysis readable, we demonstrate the case study by following a step by step approach. Note that monitoring, controlling, and other controls detailed in Section 3.4.5 are on-going activities that span over all the illustrated process.

#### **STEP1: REQUIREMENT ELICITATION & NIACSS GOVERNANCE**

**VIEWPOINTS:** The NIACSS is taken as an input to the analysis process (Figure 3-4). The Analysis Team may include, but is not limited to, members from: MoICT, National Information Technology Center (NITC), Internet Service Providers (ISPs), Health Sector, IT Business Experts, and Security Departments. It may also be useful to include team members from people who participated in the NIACSS development. The more professional and diverse the team, the more successful the analysis output will be. This team is not officially formed; therefore we formed a team that consists of researchers who already have a member from the NITC. The “viewpoints” of the team are gathered, incorporated, and summarized. The Analysis Team worked to resolve conflict, generate a reconciled understanding, and make sure that analysis is complete at least for the purpose of this research. An example on a “viewpoints” technique applied to the NIACSS is shown in Figure 5-1; it is given to illustrate the point and it is not meant to be thorough nor comprehensive.

We have also tested the validity of formulas ( ( 3-2 )to ( 3-6 ) ) however we think the illustrated example in Section 3.4.4 is enough to illustrate the point.



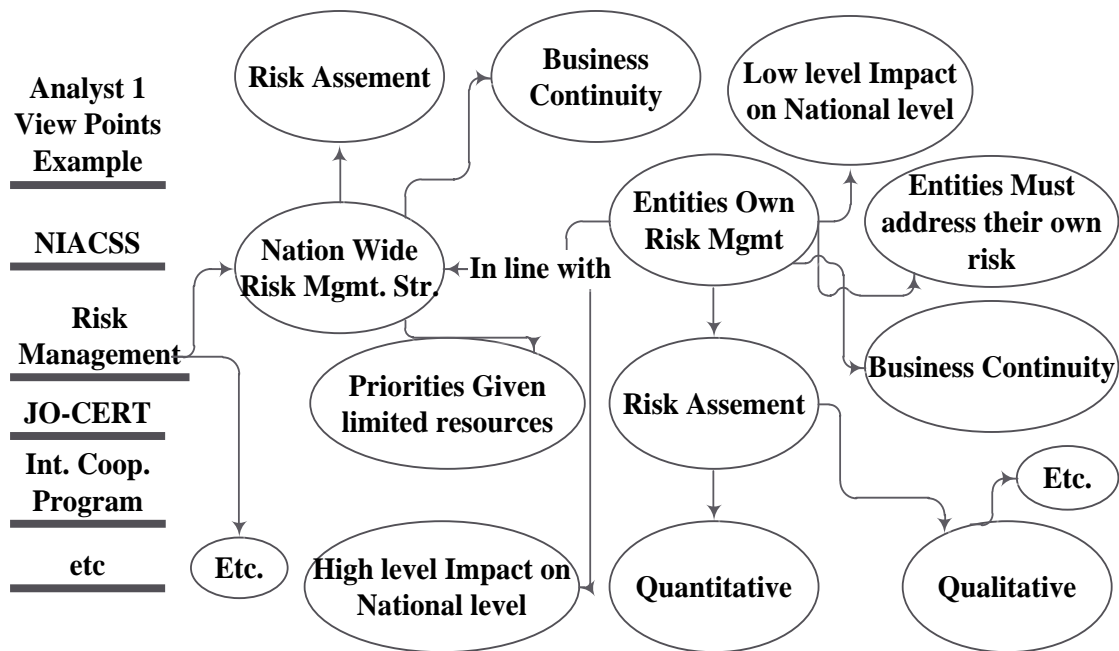


Figure 5-1 Example - “Viewpoints” applied to NIACSS.

**GOVERNANCE:** The NIACSA will be the major entity responsible for the implementation of the NIACSS. This entity does not exist yet and it has to be established. The NIACSA is foreseen as a central national entity for governmental and non-governmental organizations regarding all information assurance and cyber security related issues. The NIACSS has already anticipated the need to establish the NIACSA, but no implementation details about this entity were given. We suggest that structure of NIACSA should empower the employees and engage them into a collaborative environment. It must be adaptable to help the NIACSA be effective and able to provide cyber security products and services in an efficient manner. The organization structure should enable the NIACSA to allocate the required resources in order to achieve the NIACSS objectives. The organizational structure should be as a function of strategy; not the reverse. While organizational structure must enable strategy, it must also take into account the pragmatic issues of culture, management style, reward systems, administrative and Strategic Controls. It might also be useful to look into some similar international organizations to reuse, customize or build upon existing experience. We mention Governance for completeness, however we leave exploring this important field for future research.

## STEP2: SECURITY STRATEGIC MOVES

**REQUIREMENTS TO GOALS:** Requirements must be converted to goals to make it easy to measure. Refer to Section 3.4.4 for details. Table 5-1 shows an example on mapping requirements to goals. The “Nation Wide Risk Management” is a requirement identified by the analysis team. It is broken down into specific described goals.

Table 5-1 Example – Requirements to Goals for NIACS

Requirement	Goal	Description
Nationwide Risk Management	Establish Risk Governance Team	Risk Should be communicated from top to low level HR structures and vice versa. Risk should be a part of the global governance. Refer to Section 3.4.5.1.
	Establish Risk Management Model Nationwide	There should be global risk management for CS. Government might utilize the use of international standards of risk management
	Identify Assets, Systems, and Networks	All assets should be inventoried to track and identify possible risk to each of them.
	Set Security Goals and Objectives	Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective risk management posture.
	Assess Risks	etc.

Requirement	Goal	Description
etc.	etc.	

**GOALS PRIORITIZATION:** goals must be prioritized and aligned with available budget; threat trends and management concerns (see Sample in Table 5-2 and Table 5-3 respectively). Refer to Section 3.4.4 for details.

Table 5-2 Example – Goal Prioritization (1/2).

Measure (Strategic Control)	Importance / Weight	Establish Risk Governance	Establish Risk Management Model Nationwide	Identify Assets, Systems, and Networks	Assess Risks	etc.
Reduce Risk	160	40	160	35	30	
Improve Quality	50	5	5	10	10	
Increase performance	20	20	15	5	20	
Employ Regulations	20	0	20	4	1	

<b>Measure (Strategic Control)</b>	<b>Importance / Weight</b>	<b>Establish Risk Governance</b>	<b>Establish Risk Management Model Nationwide</b>	<b>Identify Assets, Systems, and Networks</b>	<b>Assess Risks</b>	<b>etc.</b>
Acquire Resources(Money)	40	20	10	0	0	
Acquire Resources(HR )	20	10	20	10	20	
Acquire Resources(Technology)	40	10	30	5	5	
Enhance International Cooperation	20	5	20	5	0	
Asset management	30	2	20	2	0	
etc.	...	...	...	...	...	
<b>Weights</b>	<b>400</b>	<b>21.525</b>	<b>73.875</b>	<b>17.1</b>	<b>15.8</b>	

Table 5-3 Example – Goal Prioritization (2/2).

Weighted Goals	Weight
Establish Risk Management Model Nationwide	73.875
Establish Risk Governance	21.525
Identify Assets, Systems, and Networks	17.1
Assess Risks	15.8

In the Sample in Table 5-2 and Table 5-3, the governance agency can prioritize goals according to goals importance given available budgets. The Tables shows that “Establish Risk Management Model Nationwide” is relatively more important that the reset of goals. These weighted goals figures are calculated using formula ( 3-6 ) on Section 3.4.3.1, however values of each goal could be calculated using different approaches, such as input lessons learned DB, management preferences and expert judgments.

### **STEP3: STRATEGIC MOVES ROADMAP CREATION/UPDATING**

A road map is created and continually monitored and controlled by board of directors, PMO and Project Steering Committee. This roadmap is the master plan for all plans. Figure 5-2 illustrates a sample high level roadmap using Microsoft Project 2010. See Section 3.4.4 for details.

Task Name	Duration	Start	Finish	Predecessors
<b>[-] CSS-IF Master Plan for NIACSS</b>	<b>364 days</b>	<b>Sun 1/1/12</b>	<b>Thu 5/23/13</b>	
<b>[-] Risk Management Program</b>	<b>90 days</b>	<b>Thu 4/12/12</b>	<b>Thu 8/16/12</b>	
Establish Risk Management Model nationwide	2 mons	Thu 4/12/12	Wed 6/6/12	
Establish Risk Governance	1 mon	Thu 4/12/12	Wed 5/9/12	
Identify Assets, Systems, and Networks	3 mons	Thu 5/10/12	Wed 8/1/12	4
Assess Risks	2 wks	Thu 8/2/12	Wed 8/15/12	5
Risk Program Milestone1	0 days	Thu 8/16/12	Thu 8/16/12	3,4,5,6
<b>[-] National Encryption program</b>	<b>195 days</b>	<b>Thu 6/7/12</b>	<b>Thu 3/7/13</b>	
Email Encryption	45 days	Thu 6/7/12	Wed 8/8/12	
e-services encryption	60 days	Thu 8/9/12	Wed 10/31/12	9
Cisco Hardware acquisition	90 days	Thu 11/1/12	Wed 3/6/13	10
Encryption completed	0 days	Thu 3/7/13	Thu 3/7/13	9,10,11
<b>[-] Awareness Program</b>	<b>364 days</b>	<b>Sun 1/1/12</b>	<b>Thu 5/23/13</b>	<b>11</b>
TV Program	365 days	Sun 1/1/12	Thu 5/23/13	
Online Services Program	120 days	Sun 1/1/12	Thu 6/14/12	
JO-CERT Activities	1 day?	Thu 4/12/12	Thu 4/12/12	
Awareness Program	1 day?	Thu 4/12/12	Thu 4/12/12	
<b>+ JO-CERT Activities</b>	<b>4216 days</b>	<b>Mon 4/16/12</b>	<b>Mon 6/12/28</b>	
etc.				

Figure 5-2 Example – Master High Level Road Map for NIACS.

#### STEP4: STRATEGIC MOVES EXECUTION

Once the security projects are kicked off, several metrics are got updated including project metrics, such as time and quality, or the performance metric of the whole implementation process. Figure 5-3 and Figure 5-4 show a sample Performance Metrics for CSS Implementation for Jordan and a sample dashboard for the H-ITsec-BSC, respectively. Refer Section 3.4.4 for details about Strategic Moves controls and CHAPTER 4 for details about H-ITsec-BSC.

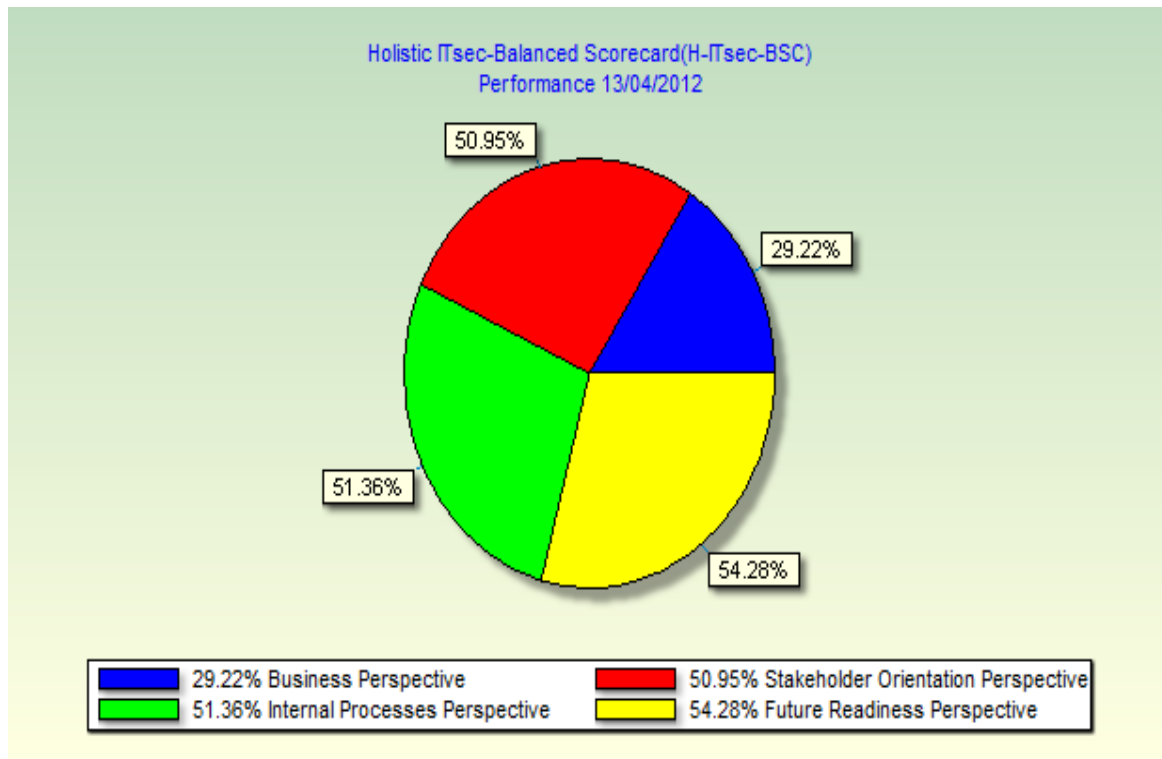


Figure 5-3 Example – Dashboard of H-ITsec-BSC for NIACS (BSC Designer).

Figure 5-3 shows that the (Business Perspective, Internal Process Perspective, Stakeholders Orientation Perspective, Future Readiness) perspectives are achieving approximately (29%,51%,50%,54%) respectively, which means that management may need to look deeply in reasons behind the low performance of business perspective compared to the other three perspectives. Details on Herath's perspectives are already given in Section 4.2. Note that the Balance Score card balances between these perspectives and the numbers will not sum to 100%, but each perspective will. Note that each indicator should reach 100%, at the end of each year, once related goals are completed.

Figure 5-4 shows the strategy map of CSS of Jordan at a particular point of time. Managers can know the percentage of achievement at the goal level and at the strategy level. This will be a very important tool in terms it will link goals and there leading and lagging indicators with the CSS, which ultimately allow instant view of the CSS implementation detailed status any time and thus taking appropriate actions when needed. A detailed H-ITsec-BSC applied to NIACSS is shown in Appendix CHAPTER 1 C.

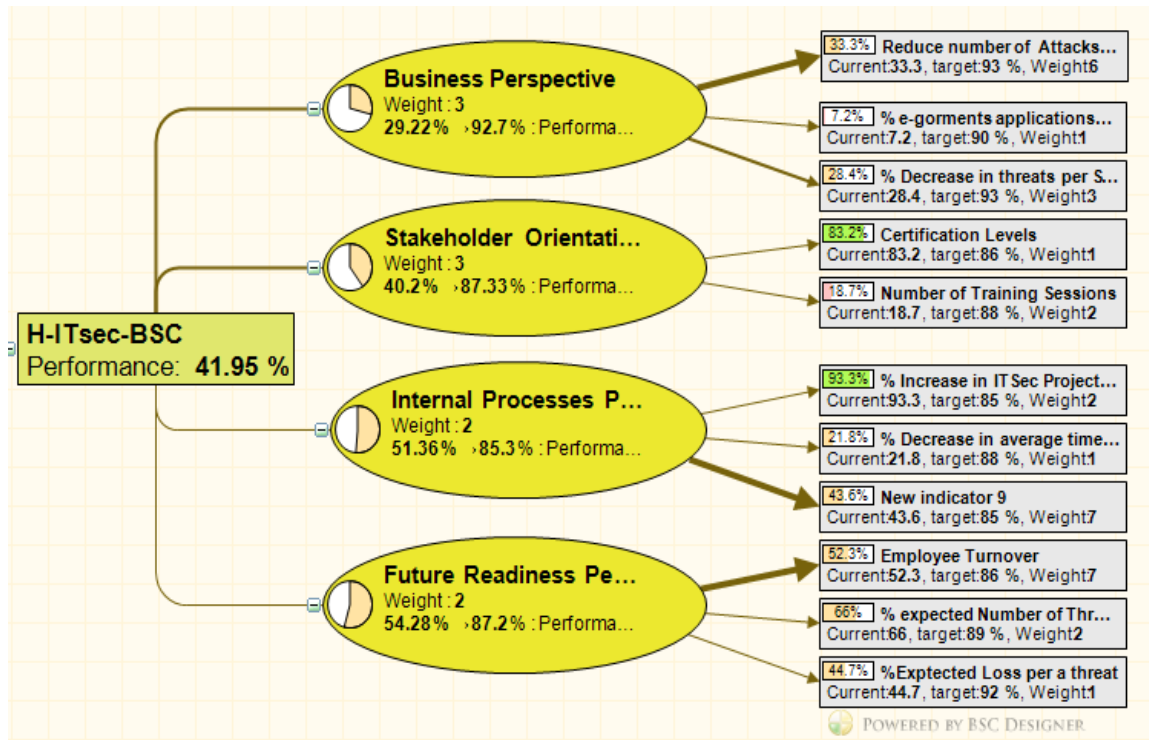


Figure 5-4 Example – Strategy Map of H-ITsec-BSC for NIACS (BSC Designer).

#### STEP5: MEASURE ACHIEVED SECURITY LEVEL.

Utilizing the set of Audit and Governance controls in the CSS-IF, the NIACSA should be able to measure the achieved security level. The security level depends on implemented Security Strategic Moves, Security Maturity Models, and International Standards. Refer to Section 3.4.5.3 for details about calculating the security level. Figure 5-5 shows how Strategic Moves are mapped to objectives where each objective might be achieved by one or more than one Strategic moves and each Strategic Move may contribute to achieve one or more than one objectives. Unless the NIACSS is fully implemented with the required resources, we will not be able measure the real achieved security level. Other options to measure the level of security are shown in Section 2.2.4 but these are very domain specific such as procedures and security policies and are not intended to map achieved goals to the CSS.



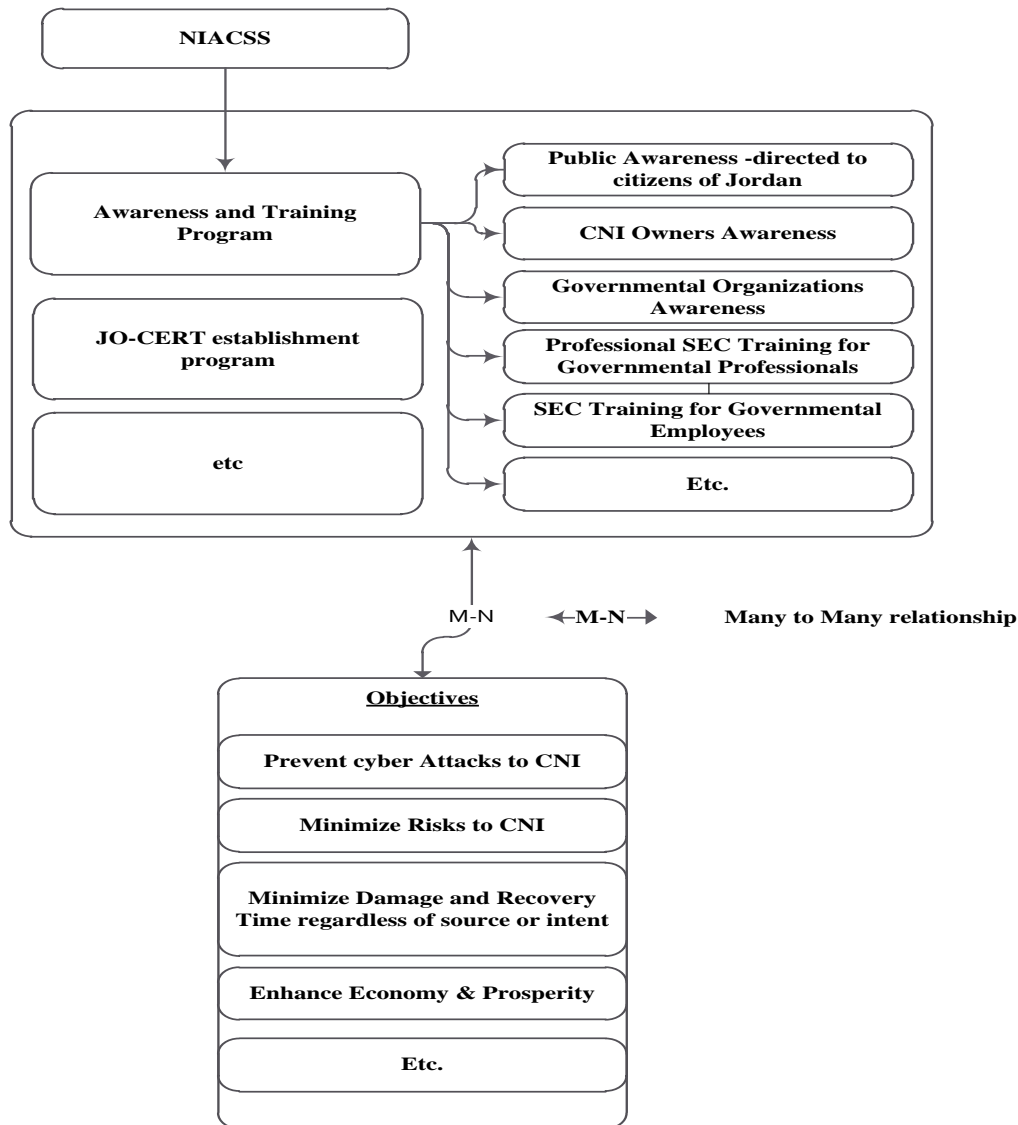


Figure 5-5 Example –Mapping Security Moves to Security Objectives.

### 5.2.3. NITC PRACTITIONERS

The case study has been conducted and approved by the following parties shown in Table 5-4 We have conducted a series of meetings and reviews with NITC’s directors and advisors based on the collaboration letter shown in (Appendix D). NITC officials were asked if the CSS-IF is applicable to the NIACSS. This is not an alternative solution to surveys. Surveys are still an option; however we defer it for future research. The Officials have developed their judgment based on the case study presented in this chapter; the actual

implementation of NIACSS will probably take more than three years. The complete list of NITC participants are in Appendix E.

Table 5-4 Summary of NITC's Practitioners Evaluation.

<b>Specialization</b>	<b>Applicability of CSS-IF to the NIACSS</b>
Cyber security strategy formulator and implementer, PMO manager, Senior Consultant	Yes  No - comments
Head of Jordan's DNS/IDN Team ( . jo الاردن )	Yes  Comments: need further analysis in change management
Networks Senior Engineer	Yes  Human Resources will be very critical to the success of the implementation

#### **5.2.4. CASE STUDY SUMMARY**

The CSS-IF is applied to the National Cyber Security Strategy of Jordan to illustrate the CSS-IF's validity. An analysis team is formed to manage and execute the case study. The team found a list of sample security strategic objectives, build a sample strategic roadmap, and illustrated how a possible execution of these objectives is reflected on holistic dashboards that monitor the whole process including its performance measures. Results are demonstrated to NITC directors and security managers. They have made a consensus on the

applicability of the CSS-IF to implement the CSS of Jordan. They had suggested a need for further analysis in the fields of human resources and change management which are outside the scope of our research.

### 5.3. VALIDATION MODEL USING BAYESIAN BELIEF NETWORK

First, we introduce Bayes Networks. Then, we provide an example on Belief Networks. Finally, we use Belief Networks to validate the CSS-IF.

#### 5.3.1. INTRODUCTION TO BAYES NETWORKS

A Bayesian network(invented by Thomas Bayes in 1763), also called( Bayes network, belief network, hierarchical Bayes(ian) model or directed acyclic graphical model, BN) is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a directed acyclic graph (DAG) to reason about uncertainty.

The simplest form of the Bayes Theorem (formula ( 5-1) ):

$$P(A \cap B) = P(A|B)P(B) = P(B|A)P(A) \quad (5-1)$$

Where:

**A** and **B** are any random events.

$$P(B) \neq 0$$

This formula is read as: Probability of A and B = (Probability of A given B) TIMES (Probability of B).

The Bayes Chain product rule for **n** variables is defined as in (formula ( 5-2)):

$$P\left(\bigcap_{k=1}^n A_k\right) = \prod_{i=1}^n P(A_k | \bigcap_{j=1}^{k-1} A_j) \quad (5-2)$$

Where:

$A_k$  is any random variable  $k$  .

$n$  is number of random variables .

$\bigcap_{k=1}^n A_k$  list of random variables.

Applying formula ( 5-2) for 4 variables for example we got:

$$P(A_4, A_3, A_2, A_1) = P(A_4 | A_3, A_2, A_1) \cdot P(A_3 | A_2, A_1) \cdot P(A_2 | A_1) \cdot P(A_1)$$

### 5.3.2. EXAMPLE ON BELIEF NETWORKS

To illustrate the BN in an Example, suppose that there are two events that could cause a system to be unsecured(S): either the security policy (L) is not enforced or a system failure (F). Also, suppose that the policy has a direct effect on a system being failure. Then the situation can be modelled with a Bayesian network. All three variables have two possible values, Y (for Yes) and N (for No). See Figures (Figure 5-6 to Figure 5-8).

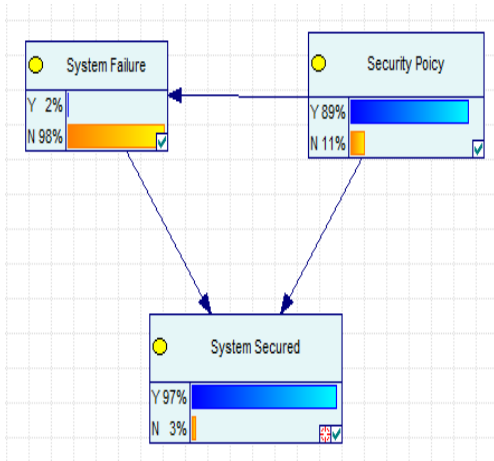


Figure 5-6 Belief Network Example Before An Evidence Is Set.

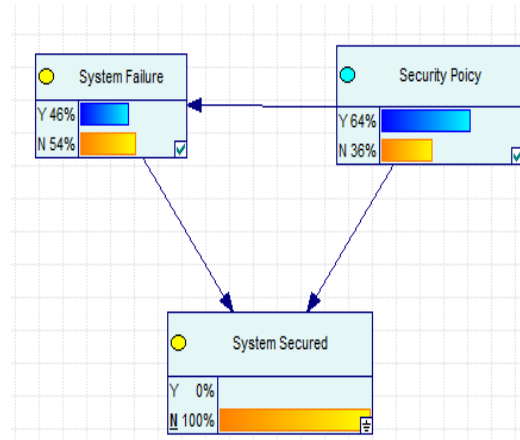


Figure 5-7 Belief Network Example After An Evidence Is Set (S=N).

System Failure(F)	Security Policy(L)	
	Y	N
Y	0.01	0.05
N	0.99	0.95

Security Policy(L)	
Y	N
0.9	0.1

		System Secured(S)	
Security Policy(L)	System Failure(F)	Y	N
Y	Y	0.2	0.8
N	Y	0.1	0.9
Y	N	0.99	0.01
N	N	0.95	0.05

Figure 5-8 List Of Probabilities Values For BN Example.

The model can answer questions like "What is the probability that a system policy is not enforced, given the system is unsecured?" by using the conditional probability formulas ( 5-1 ) , and chain product rule ( 5-2):

$$P(L = N|S = N) = \frac{P(S = N, L = N)}{P(S = N)}$$

$$\begin{aligned}
&= \frac{\sum_{F \in \{N, Y\}} P(S=N, L=N, F)}{\sum_{L, F \in \{N, Y\}} P(S=N, L, F)} \\
&= \frac{0.9 * 0.1 * 0.05 + 0.05 * 0.1 * 0.95}{0.9 * 0.1 * 0.05 + 0.05 * 0.1 * 0.95 + 0.01 * 0.9 * 0.99 + 0.8 * 0.9 * 0.01} \\
&= \frac{0.0045 + 0.00475}{0.0045 + 0.00475 + 0.00891 + 0.0072} \\
&= \frac{0.00925}{0.00925 + 0.01611} \\
&\cong 0.36
\end{aligned}$$

The joint probability will become more difficult to calculate manually especially if the number of variables increases and the number of states increases, so software tools are usually used. Moreover, these software tools have set of algorithms that could be used to calculate the probabilities especially for large networks. Example on these tools are (Bayesia SAS., 2012) Or an open source software such as GeNIe (Decision Systems Laboratory/University of Pittsburgh, 2011). In this research, we use the GeNIe.

### 5.3.3. BAYES NETWORK FOR CSS-IF

In addition to the two previous validation techniques, we use the BN to formally validate the ability of the CSS-IF to achieve the required security level utilizing a set of controls that have an effect on each other as illustrated in CHAPTER 2. Figure 5-9 is the Bayesian Belief Network model for the CSS-IF using GeNIe.

In the CSS-IF, the supportive evidence values toward cyber security objectives are mainly: the Controls, the Strategic Moves, the Requirements, Identified Goals and the CSS. Unfortunately, to our knowledge there is no direct way to calculate the probability of each component. So, we depend on domain knowledge and expert expectation. Other works such as Trust-Based Security Level Evaluation using Bayesian can be used to integrate both domain expert and knowledge base (Houmb et al., 2010).

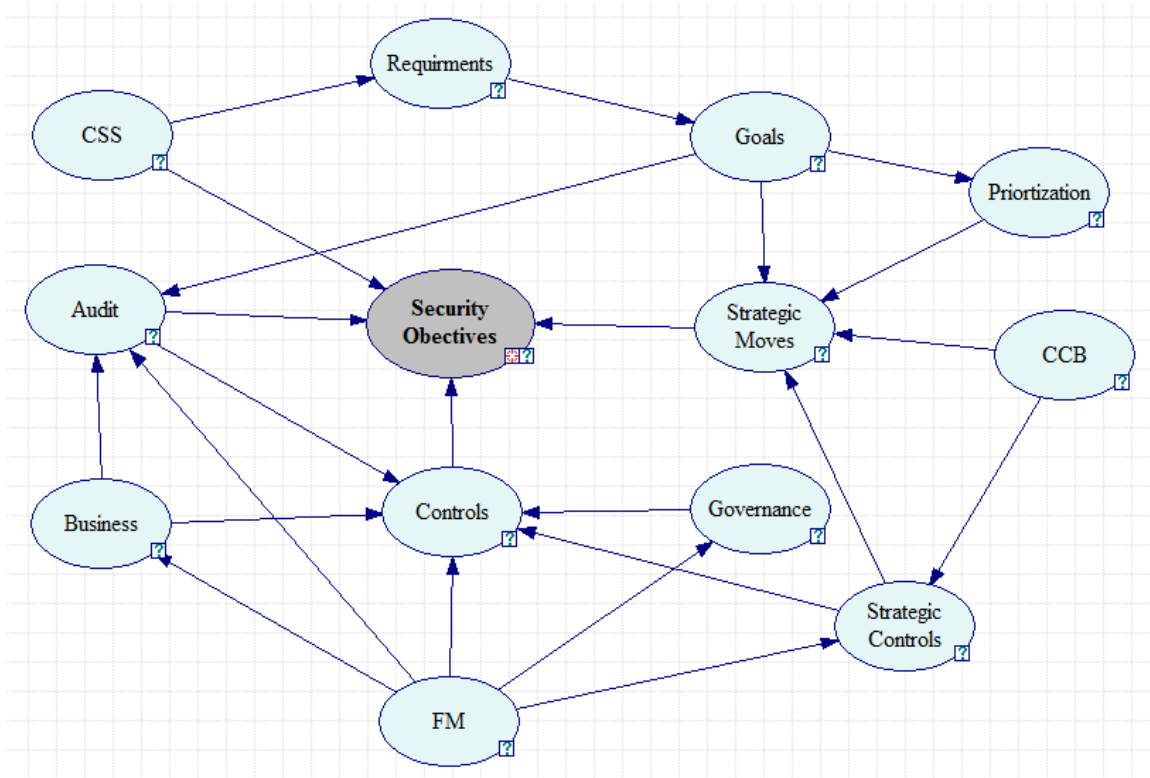


Figure 5-9 Belief Network of CSS-IF.

One advantage of the CSS-IF is that it lends itself to this suggested validation model; the more related components we identify the more accurate the measured security level. For example, the CSS-IF has already identified a set of controls that govern the implementation efforts to guarantee the achievement of the required security. (Refer to 3.4.5). To illustrate the model shown in Figure 5-9, we make 2 runs, the first with feedback from experts and the result is shown in Figure 5-10. The latter run is shown in Figure 5-11 by making evidence that Business, Framework, Audit, Governance, Strategic Controls are not satisfied. We got a security level of 88% in the first case compared to a security level of only 28% in the second case.

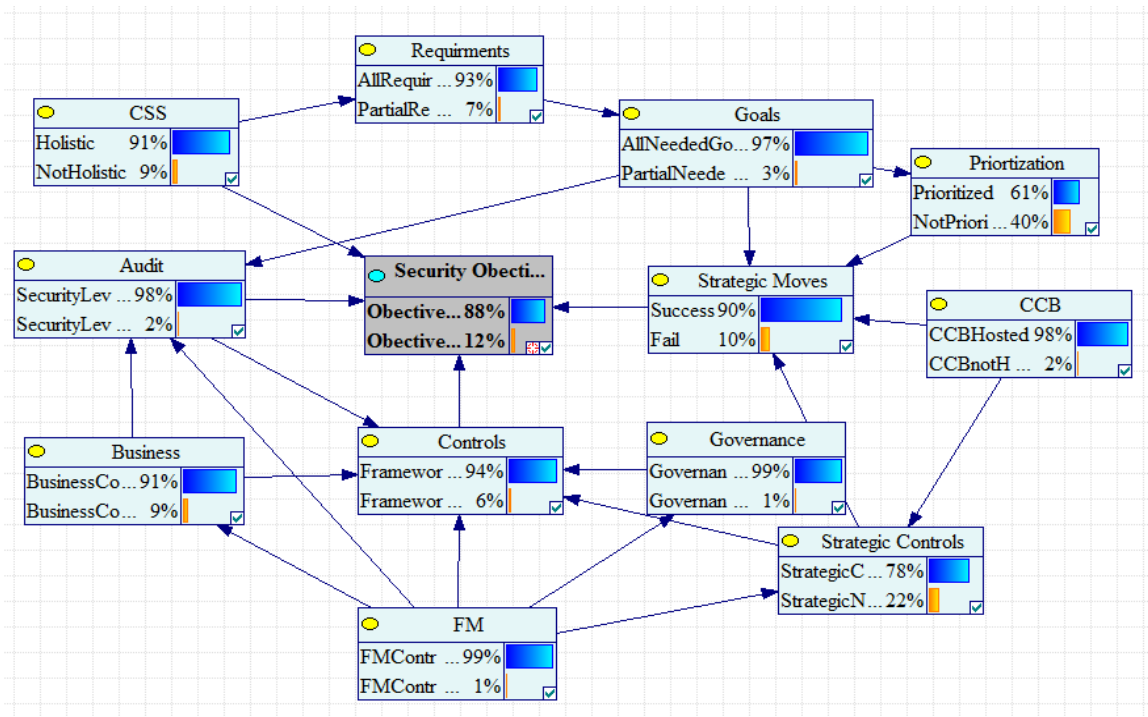


Figure 5-10 Sample Network of CSS-IF ( Assigning Values By Experts).

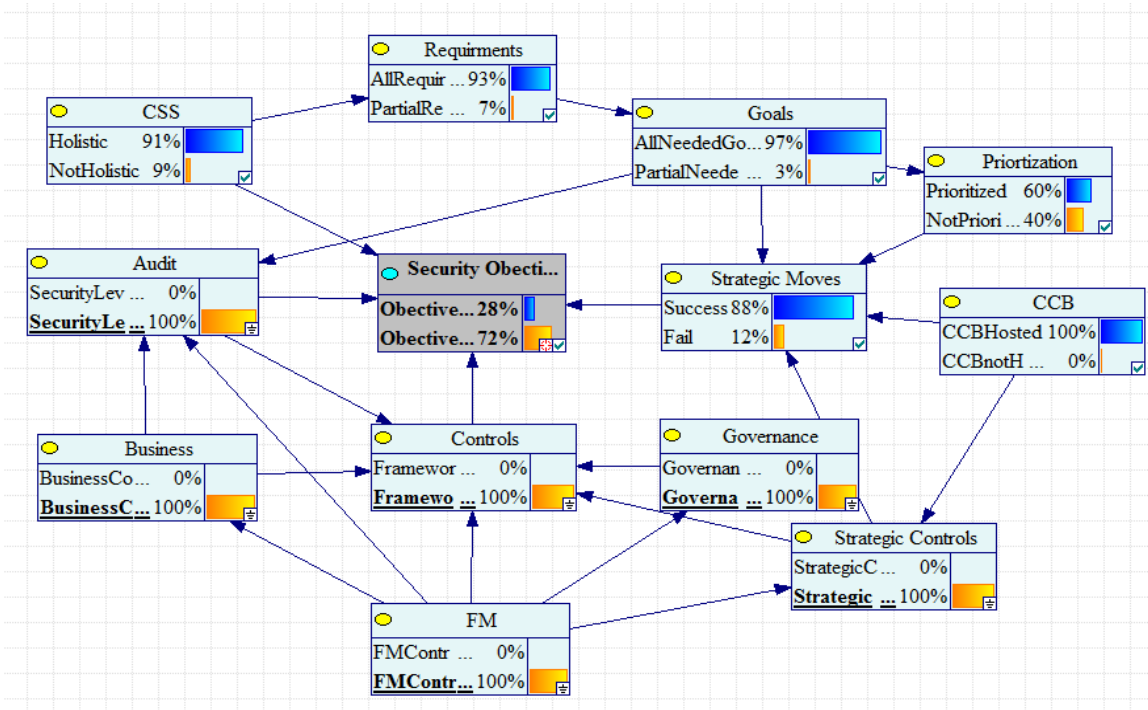


Figure 5-11 Sample Network of CSS-IF ( Assigning Evidence of Controls to False).



A further step has been done in order to test the BN; we created 10,000 records of the network with a probability of 50% for each variable. Then, we test the network shown in Figure 5-9 using: the generated data, 10-fold cross validation. The result was 68% for the security objectives success which relatively provides a good indication for the BN model validity.

Unfortunately, we have noticed that the results are highly dependent on the generated data and its distribution. Since we are not able to get data to our model due to fact that most available data sets are on the operational level of cyber security, and even if we were able to aggregate such data the semantic of the data will get lost. Thus, we suggest further research in order to find the best weight of each random variable and then generate a representative data to test the model; this option is listed as a limitation and is left for future research.

#### **5.4. COMPARISON WITH OTHER FRAMEWORKS**

Security frameworks have been adopted to secure cyberspace. Most of them target a specific domain or developed for specific entities. To our knowledge, there is no complete CSS implementation framework at the national level except for few ones illustrated in Sections (2.2.2, 2.2.3, 2.2.5) with major drawbacks. Nevertheless, we compare CSS-IF framework with a list of international frameworks that has been implemented for various organizations. These international frameworks intersect with the CSS-IF in common objectives of increasing security levels despite of their limitations and scope. We need to confirm that the CSS-IF is an overarching holistic approach to implement cyber security, therefore it is not intended to replace any other framework that we are comparing against.

Comparison is carried out against a list of features that are either extracted from literature reviews (CHAPTER 2) or suggested by this research. The suggested features enable the CSS-IF to overcome the limitations of the existing frameworks; in fact, most of those features were the original motives to this research from the first place. We rate each feature against all included frameworks grouped as per discussed in literature review (CHAPTER 2). A feature is subjectively rated; rating is performed utilizing the knowledge extracted

from the literature review along with our judgement. Below is the list of features that we compare frameworks against and how they are rated.

1. Resilience: means the ability of the framework to be agile, flexible and be able to deal with unseen changes in technology, environment, attack methods, etc.(Erol, Sauser, & Mansouri, 2010; The White House, 2011). Resilient management systems and processes will provide greater protection against multidimensional attacks (Trim & Lee, 2010). The CSS-IF support this feature because it is configurable see section (3.4.5.4.1) and it has the controls of risk , quality and vigilance as illustrated in section (3.4.5.2).
2. Measure Performance: Measure performance of security initiatives effectively at various organization levels and report to higher levels. Refer to Performance Measurement CHAPTER 4.
3. Compliance: follow a known standard or best practice and let the cyber security strategy implementation framework to manage differences between different standards. (IsecT Ltd, 2011) . The CSS-IF supports compliance by using the control of UCF as illustrated in section (3.4.5.4.1).
4. Measure Security Level: to measure the level of security at a particular point of time an implementer has achieved so far. Refer to Audit Controls Section 3.4.5.3 and Security Maturity Models Section 2.2.4.
5. Identify Gaps in CSS document: the framework should be able to detect if CSS needs further modification in case it does not guarantee required security level. Refer to Audit Controls Section 3.4.5.3
6. Holistic: the framework should be implemented at the national level. “security should be broadly interpreted and placed in a holistic and management setting” (Trim & Lee, 2010,pp5) . “Information Security is a strategic approach that should be based on a solid, holistic framework encompassing all of an organization's Information Security requirements, not just those of individual projects” (Oracle, 2011,pp4). “It is well-recognized that cyber security is a multi-dimensional problem, involving both the strength of security technologies and variability of

human behavior and any solution to address this problem will require a holistic approach.” (Dasgupta & Rahman, 2011). The framework is holistic by all its components illustrated in section 3.4.

Table 5-5 is the summary of the compared frameworks. The complete comparison can be found in Appendix B. The proposed CSS-IF succeeds other frameworks. This advantage is mainly achieved by the ability of CSS-IF to lay the ground to implement cyber security on a holistic level. We need to confirm the message that the CSS-IF is not intended to replace other frameworks nor it can. The CSS-IF is designed to exploit and embed other frameworks where appropriate. We have seen in Section 3.4.5.4.1 that the CSS-IF has a built in configuration components that makes the integration of other frameworks possible.

Table 5-5 Cyber Security Frameworks (category) Comparison.

Framework Category(Section 2.2)	Resilience	Measure Performance	Compliance	Security Level	CSS Gaps	Holistic
Management and Governance (2.2.1)	✓	✗	✗	✗	✗	✗
Generic Frameworks(2.2.5)	✗	✓	✗	✗	✗	✓
Security Maturity Models and Metrics (2.2.4)	✓	✗	✓	✓	✓	✗
Customized Frameworks(2.2.3)	✗	✗	✓	✗	✗	✓
Guidelines(2.2.2)	✓	✗	✗	✓	✗	✓
Provider's Specific Frameworks(2.2.6)	✓	✓	✓	✓	✗	✗
Open Frameworks(2.2.7)	✓	✓	✓	✓	✗	✗
CSS-IF(CHAPTER 3)	✓	✓	✓	✓	✓	✓

## 5.5. CHAPTER SUMMARY

We validate the CSS-IF by a case study and using Bayesian Belief Networks. We have shown that each of the validation techniques has its own strengths and weaknesses; however they provide an acceptable proof of concept for CSS-IF's validity. Table 5-6 shows these used techniques and lists their major advantages and disadvantages.

Table 5-6 CSS-IF Validation Techniques Advantages and Disadvantages.

Validation Technique	Advantages	Disadvantages
Case study	<ul style="list-style-type: none"> <li>• Real life scenario that helps a buy in.</li> <li>• Triggers the need to do research in other domains.</li> </ul>	<ul style="list-style-type: none"> <li>• Does not guarantee all cases and hard to generalize.</li> <li>• Not tested on the complete life cycle of the implementation that is going to take years to be fulfilled</li> </ul>
Belief Network	Belief networks have a built-in independence characteristic that permits formal evaluation of the CSS-IF.	In our case, there is no real data available for learning which poses a limitation

## **CHAPTER SIX**

### **CONCLUSTIONS AND FUTURE WORK**

## CHAPTER 6

### CONCLUSTIONS AND FUTURE WORK

#### 6.1. CONCLUSION

Cyber Security Strategy Implementation frameworks have a great influence on securing the cyberspace. Although there are lots of researches on various cyber security domains, little has been done on cyber security holistic implementation frameworks from the security engineering perspective.

In the context of our research, a holistic cyber security strategy implementation framework develops and/or integrates a set of high level conceptual security components, solutions, entities, tools, techniques, or mechanisms to collectively collaborate in order to implement cyber security strategies and thus enhances the security level on the national level. A component, in the context of this research, is a constituent part of the CSS-IF; the component may integrate one or more necessary functions or solutions to help in the implementation of cyber security strategy towards achieving the overall cyber security objectives.

In this thesis, we proposed a holistic, coherent, and systematic cyber security strategy implementation framework (CSS-IF) that essentially facilitates transforming the cyber security from the current state to the future required state. The CSS-IF major core components are: CSS, Requirement Elicitation, Security Strategic Moves, Strategic Controls, Security Objectives and Framework Repository. The CSS is assumed to be a holistic document satisfying Fielden properties (Fielden, 2011). The CSS-IF proposes a methodology to analyze the CSS and break it down into well-defined requirements that will be eventually transformed into Strategic Moves. These Strategic Moves are executed under the defined framework controls in order to achieve the required security objectives. The implementation is guided and managed via the help of a focal implementation framework repository.

During the execution, a set of metrics will be exposed into and imported from the Implementation Framework Repository. Moreover, the implementation process will be

governed monitored, regulated and controlled with the set of security controls. Finally, the set of achieved security objectives will be compared to the targeted objectives and corrective or proactive actions will be possible.

The major advantages of the CSS-IF and its supporting components are:

1. Overarching cyber security consolidation. The CSS-IF helps the international governments to take on a consolidated approach to enforce the implementation of CSS across their nations. The CSS-IF provides an early detection of likely threats and mitigate risks related to government information systems and critical infrastructure. Thus, the CS-IF enables decision makers to take necessary actions once needed, and assists the government in creating a safe and trustworthy environment for business. The framework places a foundation for a global risk on the national level, global CSS implementation performance measurement concept and governs many aspects of security such as human resources, technology layering, and future plans for the unseen threats.
2. Holistic Performance. The proposed Holistic IT security Balanced Score Card (H-ITsec-BSC) enhances security by providing leading and lagging measures of cyber security at the national level which ultimately oversees the current implementation efforts.
3. Requirements Elicitation. The Requirements Elicitation embedded within the CSS-IF helps convert the CSS from the natural language to a set of business and security requirements. The elicitation is important to break the CSS into manageable understandable requirements and identify Strategic Moves that will eventually enhance the overall security level.
4. Integrating Components. The CSS-IF integrates viewpoints, a concept being used in Software Engineering, an enhanced Holistic Information Security Balanced Score Card (H-ITsec-BSC) , Strategic Moves , Security Controls and other necessary components in various areas to implement the CSS. This integration will oversee the security from various aspects at the same time.

5. Configurability. The CSS-IF is a configurable framework where strategy implementers can decide on several input components, standards, and strategic moves.
6. Conceptually and practically proven. The CSS-IF is validated using two formal and informal approaches: 1) validate the CSS-IF through a case study; results show that the CSS-IF is applicable to the cyber security strategy of Jordan, and 2) Validate CSS-IF using Bayesian Belief Networks; results show the strong relevance of CSS-IF and its components to achieve the required security level. We have shown that each of these validation techniques has its own strengths and weaknesses, however using both techniques provide an acceptable proof of concept to demonstrate the CSS-IF's validity. The CSS-IF is compared with other frameworks; results show that CSS-IF outperforms other frameworks on six selected cyber security features.

## **6.2. FUTURE WORK**

One of the main contributions of this thesis is that it opens a wide area for future research. In addition to the technical domains in computer security, the CSS-IF lays the ground for other nontechnical domains to take their role in cyber security strategy implementation such as project management, regulation regimes, human resource management, organization structure, and governance, which makes the framework more thorough in covering interrelated multi diverse domains. Moreover, the CSS-IF balances between detailed and abstract levels of cyber security, any future additional details will for sure enrich this work and make it more mature for cyber security strategy implementation. The following is a list of possible future research direction.

1. Enrich the framework in other dimensions such as: Human Resource, Organization Structures, Global Governance, Regulation Regimes, Awareness Programs, and thus provide a more detailed framework. For example, a complete and detailed organizational structure for the CSA could be built by considering: a) different types of organizational structures, b) duties and jobs description, c) scope and size, d) resource allocation, and e) working processes and procedures. This will enrich the CSS-IF and makes it more detailed.



2. Enhance the requirements elicitation. The inputs to various models play a major factor in achieving expected outputs. The Requirement Elicitation process has a major effect on cyber security. Requirements are extracted from the CSS, usually with direct human involvement, and then these requirements are converted to goals and executed at later stages. If requirements were not fully captured then possible unsuccessful cyber security efforts might be introduced, and as a result cyber security projects might be subject to fail. Thus, we suggest investigating possible enhancements to the Requirement Elicitation Component in order to reduce human intermediation.
3. Investigate governance alternatives. As an alternative to the CSA, the governance entity, outsourcing of cyber security strategy implementation to various vendors could be investigated. A starting point toward this direction will be utilizing the components that we have identified such as Vendor management, Contracting and Global Governance.
4. Validate the framework using surveys. Surveys could be used to validate the CSS-IF, but since the framework is holistic at the national level, covers many security aspects, and is proposed for any country then a diverse set of survey teams should be considered to perform such complex and time consuming survey. In other words, the survey should consider demographic factors, expert's domains, and regulations. One possible direction is to use a set of international groups or governments agencies throughout the world.
5. Enhance the Belief Network validation technique used for the CSS-IF: We have noticed that the results of BN validation model are highly dependent on the generated data and its distribution. Since we were not able to get data to our model due to the fact that most available data sets are on the operational level of cyber security, and even if we were able to aggregate such data the semantic of the data will get lost. Thus, we suggest further research in order to find the best weight of each random variable and then generate a representative data to validate the model.
6. Build a CASE tool. This thesis suggests a CASE tool to oversee the implementation via adopting the CSS-IF's suggested approach.

## APPENDIXES

### A. REFERENCES

- Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security*, 18(4), 226-276. doi:10.1108/09685221011079180
- Ahern, D., Clouse, A., & Turner, R. (2008). *CMMI ® distilled: a practical introduction to integrated process improvement, third edition* (Third.). Addison-Wesley Professional.
- Al-Salloum, Z. S., & Wolthusen, S. D. (2011). Threat analysis model of an agent-based vulnerability mitigation mechanism using Bayesian Belief Networks. *Network Science Workshop (NSW), 2011 IEEE* (pp. 144-151). doi:978-1-4577-1049-0
- Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional.
- Arab Advisor Group. (2010). Telecom: Arab Advisors Group. Retrieved January 12, 2011, from <http://www.arabadvisors.com>
- Barnat, R. (2005). Strategic Management :: The Nature Of Strategy Implementation. Retrieved February 3, 2012, from <http://www.strategy-implementation.24xls.com/en100>
- Bartol, N., Bates, B., Goertzl, K. M., & Winograde, T. (2009). *Measuring Cyber Security and Information Assurance -State-of-the-Art Report (SOAR)*. (K. J. Knapp, Ed.). IGI Global. doi:10.4018/978-1-60566-326-5
- Bayesia SAS. (2012). BayesiaLab. Retrieved from [www.bayesia.com](http://www.bayesia.com)
- Broom, A. (2009). Security consolidation and optimisation: Gaining the most from your IT assets. *Computer Fraud & Security*, 2009(5), 15-17. Elsevier Ltd. doi:10.1016/S1361-3723(09)70061-2
- Buecker, A., Borrett, M., Lorenz, C., & Powers, C. (2010). Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security. *IBM Redpaper*, 1-96.
- Carnegie Mellon University. (2010). *Systems Security Engineering Capability Maturity (SSE-CMM®) Model Document Ver 3.0*.
- Central Intelligence Agency/US. (2011). The World Fact Book. Retrieved December 2, 2011, from <https://www.cia.gov/library/publications/the-world-factbook/geos/jo.html>

- Cole, E. (2011). *Network security bible* (Vol. 768). Wiley.
- Constantine, L. L. (2011). From virtual digits to real destruction: lessons from Stuxnet. *Cutter IT Journal*, 24(5), 6.
- DOS, & MoICT. (2010). *Survey the use of information and communication technology Indoors*. Retrieved from [http://www.dos.gov.jo/dos\\_home\\_a/main/Analasis\\_Reports/it\\_tech/tech\\_2010.pdf](http://www.dos.gov.jo/dos_home_a/main/Analasis_Reports/it_tech/tech_2010.pdf)
- Dasgupta, D., & Rahman, M. (2011). A Framework for Estimating Security Coverage for Cloud Service Insurance. *Proceedings of Cyber Security*, 1. New York, New York, USA: ACM Press. doi:10.1145/2179298.2179342
- David, F. (2011). *Strategic management: Concepts and cases* (13th Ed.). Prentice Hall. Retrieved from [http://www.malone.edu/media/1/39/480/MMP405\\_Online\\_Corporate\\_Strategy.pdf](http://www.malone.edu/media/1/39/480/MMP405_Online_Corporate_Strategy.pdf)
- Decision Systems Laboratory/University of Pittsburgh. (2011). GeNIe & SMILE. University of Pittsburgh. Retrieved from <http://genie.sis.pitt.edu/?ver=20043341>
- EAdirections. (2007). *EA Frameworks : Pros and Cons – Inventory and Insights*. doi:EA-7004
- Erol, O., Sauser, B. J., & Mansouri, M. (2010). A framework for investigation into extended enterprise resilience. *Enterprise Information Systems*, 4(2), 111-136. doi:10.1080/17517570903474304
- Estonia Department of Defence. (2008). Cyber Security Strategy -Estonia. Retrieved February 1, 2012, from [http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku\\_strateegia\\_2008-2013\\_ENG.pdf](http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf)
- European Network and Information Security Agency (ENISA). (2011). *Cyber security : future challenges and opportunities*. Retrieved from <http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011>
- Fielden, K. (2011). An Holistic View of Information Security : A Proposed Framework. *International Journal*, 4(1), 427-434.
- Fischer, E. A. (2005). *CRS Report for Congress Creating a National Framework for Cybersecurity : An Analysis of*. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA463076&Location=U2&doc=GetTRDoc.pdf>
- Fitzgerald, T. (2011). *Information Security Governance Simplified: From the Boardroom to the Keyboard*. CRC Press.

- Fortinet. (2011). A survey from network security provider Fortinet. Retrieved from <http://www.infosecurity-magazine.com/view/2520/network-security-consolidation-trend-very-strong-in-europe/>
- Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., Blackbird, J., et al. (2011). *Symantec Internet Security Threat Report trends for 2010* (Vol. 16).
- Goldman, J. E., & Ahuja, S. (2011). Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework. *ICT Ethics and Security in the 21st Century: New Developments and Applications*, 277. Information Science Pub.
- Gonsalves, P. G., Call, C. D., Ho, S., & Lapsley, D. (2011). Security system for and method of detecting and responding to cyber attacks on large network systems. Google Patents.
- Goodyear, M., Goerdel, H. T., Portillo, S., & Williams, L. (2010). Cybersecurity Management in the States : The Emerging Role of Chief Information Security Officers. *IBM Center for the Business of Government*.
- Government of Australia. (2009). Austian Cyber Security Strategy. Retrieved from <http://www.ag.gov.au/Cybersecurity/Pages/default.aspx#h2strategy>
- Györy, A. (2012). Finding the Right Balanced Scorecard for Business-Driven IT Management A Literature Review. *Review Literature And Arts Of The Americas*. doi:10.1109/HICSS.2012.280
- HM Government. (2010). *A strong Britain in an age of uncertainty: the national security strategy*. The Stationery Office (pp. 1-39). The Stationery Office. Retrieved from <http://www.official-documents.gov.uk/>
- Haley, C. B., Moffett, J. D., & Laney, R. (2006). A framework for security requirements engineering. *Proceedings of the 2006 international workshop on Software engineering for secure systems* (pp. 35–42). ACM. Retrieved from <http://dl.acm.org/citation.cfm?id=1137634>
- Heavey, C., & Murphy, E. (2012). Integrating the Balanced Scorecard with Six Sigma. *The TQM Journal*, 24(2), 108-122. doi:10.1108/17542731211215062
- Henze, D. (2000). IT baseline protection manual. *Federal Agency for Security in Information Technology, Germany*.
- Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. *Information Systems Management*, 27(1), 72-81. doi:10.1080/10580530903455247

- Hewson, M., & Sinclair, T. J. (1999). *Approaches to global governance theory*. State Univ of New York Pr.
- Houmb, S., Ray, I. I., & Chakraborty, S. (2010). Trust-Based Security Level Evaluation Using Bayesian Belief Networks. In M. Gavrilova, C. Tan, & E. Moreno (Eds.), *Transactions on Computational Science X* (Vol. 6340, pp. 154-186). Springer Berlin / Heidelberg. Retrieved from <http://www.springerlink.com/index/MT8066M37547V22J.pdf>
- Hunker, J. (2010). U . S . International Policy for Cybersecurity : Five Issues That Won ' t Go Away. *National Security Policy*, 4, 197-465.
- IGRC. (2011). The integrated governance, risk and compliance (iGRC) Consortium. Retrieved April 1, 2012, from <http://www.informationsecurityprotection.com/>
- Iheagwara, C. M., & Charless M. Iheagwara. (2011). *The strategic implications of the current Internet design for cyber security*. Massachusetts Intstitute of Technology. Retrieved from <http://dspace.mit.edu/handle/1721.1/67554>
- Int@j. (2011). Jordan Ict Sector Profile. Retrieved January 1, 2012, from [http://www.intaj.net/sites/default/files/JORDAN\\_ICT\\_SECTOR\\_PROFILE\\_-\\_FINAL.pdf](http://www.intaj.net/sites/default/files/JORDAN_ICT_SECTOR_PROFILE_-_FINAL.pdf)
- Int@j, & MoICT. (2010). ICT & ITES Industry Statistics & Yearbook 2010. Retrieved January 1, 2012, from <http://www.intaj.net/content/2010-it-and-ites-industry-statistics>
- International Telecommunication Union(ITU). (2008). *Management Framework for Organizing National Cybersecurity / CIIP Efforts*.
- International Telecommunication Union(ITU). (2009). Cybersecurity guide for developing countries.
- International Telecommunication Union(ITU). (2011a). ICT and Telecommunications in Least Developed Countries: Review of Progress made during the Decade 2000-2010. *Fourth United Nations Conference on the Least Developed Countries (UNLDC-IV)*. Istanbul, Turkey.
- International Telecommunication Union(ITU). (2011b). *ICT Facts and Figures*. Retrieved from <http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf>
- IsecT Ltd. (2011). Information security compliance. *information security awareness service(NoticeBored)*, (March), 1-10. Retrieved from [http://www.isect.com/html/white\\_papers.html](http://www.isect.com/html/white_papers.html)
- Jalaliniya, S. (2011). *Enterprise Architecture & Security Architecture Development*. Lund University.

- Janssen, M., & Hjort-Madsen, K. (2007). Analyzing enterprise architecture in national governments: The cases of denmark and the netherlands. *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (p. 218a–218a). IEEE. doi:10.1109/HICSS.2007.79
- Jo, H., Kim, S., & Won, D. (2011). Advanced Information Security Management Evaluation System. *KSII Transactions on Internet and Information Systems, 5*(6), 1192-1213. doi:10.3837/tiis.2011.06.006
- Kaplan, R. S., & Norton, D. P. (1996). Strategic learning & the balanced scorecard. *Strategy & Leadership, 24*(5), 18-24. MCB UP Ltd. doi:10.1108/eb054566
- Kaplan, R. S., & Norton, D. P. (2004). Measuring the strategic readiness of intangible assets. *Harvard business review, 82*(2), 52-63.
- Kaplan, R. S., Norton, D. P., & others. (1992). The balanced scorecard--measures that drive performance. *Harvard business review, 70*(1), 71-79. Boston.
- Klein, N., Kaplan, R. S., Chemical Bank (New York, N., & Corporation, C. B. (1999). *Chemical Bank: Implementing the Balanced Scorecard*. Harvard Business School.
- Kondakci, S. (2010). Network security risk assessment using Bayesian belief networks. *Social Computing (SocialCom), 2010 IEEE Second International Conference on* (pp. 952-960).
- Ku, C.-Y., Chang, Y.-W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy, 33*(7), 371-384. doi:10.1016/j.telpol.2009.03.002
- Kurrek, H. (2002, April). SMM - Assessing a Company's IT Security. *ERCIM News*. Retrieved from [http://www.ercim.eu/publication/Ercim\\_News/enw49/kurrek.html](http://www.ercim.eu/publication/Ercim_News/enw49/kurrek.html)
- Lee, E., Park, Y., & Shin, J. G. (2009). Large engineering project risk management using a Bayesian belief network. *Expert Systems with Applications, 36*(3), 5880-5887. Elsevier.
- Marcos, A., & Rouyet, J. (2012). An IT Balance Scorecard Design under Service Management Philosophy. *2012 45th Hawaii*. doi:10.1109/HICSS.2012.107
- Maughan, D. (2010). The need for a national cybersecurity research and development agenda. *Communications of the ACM, 53*(2), 29. doi:10.1145/1646353.1646365
- MoICT. (2011). National Information Assurance and Cyber Security Strategy (NIACSS). *Ministry of Information and Communications Technology*. Retrieved February 2, 2012, from [http://www.moict.gov.jo/pdf\\_files/NIACSS Draft - Public Consultation.pdf](http://www.moict.gov.jo/pdf_files/NIACSS Draft - Public Consultation.pdf)

- National Institute of Standards and Technology (NIST). (2001). *Security Requirements For Cryptographic Modules*. Gaithersburg. Retrieved from <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- Neely, A. (1999). The performance measurement revolution: why now and what next? *International Journal of Operations & Production Management*, 19(2), 205-228. MCB UP Ltd.
- Neubauer, T., Klemen, M., & Biffel, S. (2005). Business process-based valuation of IT-security. *ACM SIGSOFT Software Engineering Notes* (Vol. 30, pp. 1–5). ACM. doi:10.1145/1082983.1083099
- Nguyen, A. (2012, February 8). UK cyber strategy implementation “too slow”, says former security minister. *Computerworld UK*, 1. Retrieved from <http://www.computerworlduk.com/news/security/3335972/uk-cyber-strategy-implementation-too-slow-says-former-security-minister/>
- Nnolim, A. L. (2007). *A framework and methodology for information security management*. Security. Lawrence Technological University.
- Norreklit, H. (2000). The balance on the balanced scorecard a critical analysis of some of its assumptions. *Management accounting research*, 11(1), 65-88. Elsevier.
- Nudurupati, S. S., Bititci, U. S., Kumar, V., & Chan, F. T. S. (2011). State of the art literature review on performance measurement. *Computers & Industrial Engineering*, 60(2), 279-290. doi:10.1016/j.cie.2010.11.010
- Nuseibeh, B., Kramer, J., & Finkelstein, A. (2003). ViewPoints: meaningful relationships are difficult! *Software Engineering, 2003. Proceedings. 25th International Conference on* (pp. 676–681). IEEE. doi:10.1109/ICSE.2003.1201254
- Oda, S. M., Fu, H., & Zhu, Y. (2009). Enterprise information security architecture a review of frameworks, methodology, and case studies. *2009 2nd IEEE International Conference on Computer Science and Information Technology* (pp. 333-337). Ieee. doi:10.1109/ICCSIT.2009.5234695
- Othman, R. (2008). Enhancing the effectiveness of the balanced scorecard with scenario planning. *International Journal of Productivity and Performance Management*, 57(3), 259-266. Emerald Group Publishing Limited.
- Otoom, A. (2011). A Proposed Implementation Framework (PIF) for the National Information Assurance and Cyber Security Strategy (NIACSS). *Conference on Security and Safety in the Cyberspace*. Amman, Jordan: Jordan University.

- Pattaya Today. (2012, February). ICT Ministry plans cyber-security framework. *Pattaya Today*. Retrieved from <http://pattayatoday.net/news/thailand-news/ict-ministry-plans-cyber-security-framework/>
- Pearl, J. (2011). Bayesian networks. *Handbook of brain theory and neural networks*. The MIT Press.
- Phahlamohlaka, L., Jansen van Vuuren, J., & Coetzee, A. (2011). Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation. *Proceedings of the first IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW)* (pp. 1-14). Gaborone, Botswana. doi:9780620500500
- Rosenau, J. N. (1999). Toward an ontology for global governance. *Approaches to global governance theory*, 287-301. Albany: State University of New York Press.
- Salem, A. M. (2010). Requirements Analysis through Viewpoints Oriented Requirements Model (VORD). *International Journal of Advanced Computer Science and Applications*, 1(5), 6-13. Retrieved from [http://www.thesai.info/Downloads/Volume1No5/Paper 2-Requirements Analysis through Viewpoints Oriented Requirements Model \(VORD\).pdf](http://www.thesai.info/Downloads/Volume1No5/Paper 2-Requirements Analysis through Viewpoints Oriented Requirements Model (VORD).pdf)
- Schjolberg, S., & Ghernaouti-Helie, S. (2011). *A Global Treaty on Cybersecurity and Cybercrime* (Second edi.). © Stein Schjøberg and Solange Ghernaouti-Hélie. Retrieved from [http://www.cybercrimelaw.net/documents/A\\_Global\\_Treaty\\_on\\_Cybersecurity\\_and\\_Cybercrime,\\_Second\\_edition\\_2011.pdf](http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf)
- Schwab, K. (2011). *The global competitiveness report 2011-2012* (Vol. 198, p. 220). Geneva, Switzerland: World Economic Forum. doi:978-92-95044-74-6
- Schwalbe, K. (2010). *Information technology project management* (6th ed.). Course Technology Ptr.
- Self, J. (2004). Metrics and management: applying the results of the balanced scorecard. *Performance Measurement and Metrics*, 5(3), 101-105. doi:10.1108/14678040410570111
- Seppanen, V., Heikkila, J., & Liimatainen, K. (2009). Key Issues in EA-implementation: Case study of two Finnish government agencies. *2009 IEEE Conference on Commerce and Enterprise Computing* (pp. 114–120). Ieee. doi:10.1109/CEC.2009.70
- Shin, K. S., Shin, Y. W., Kwon, J. H., & Kang, S. H. (2012). Risk propagation based dynamic transportation route finding mechanism. *Industrial Management & Data Systems*, 112(1), 102-124. Emerald Group Publishing Limited.



- Stacey, T. R. (1996). Information security program maturity grid. *Information Systems Security*, 5(2), 22-33.
- Suid-afrika, R. V. A. N. (2010). *South African National Cybersecurity Policy* (pp. 1-16). doi:9771682584003-32963
- Tagert, A. (2010). *Cybersecurity Challenges in Developing Nations*. Carnegie Mellon University. Retrieved from <http://repository.cmu.edu/dissertations/22/>
- Taticchi, P. (2008). *Business performance measurement and management: implementation of principles in SMEs and enterprise networks*. PhD Thesis, University of Perugia, Italy.
- Taticchi, Paolo, Tonelli, F., & Cagnazzo, L. (2010). Performance measurement and management: a literature review and a research agenda. *Measuring Business Excellence*, 14(1), 4-18. doi:10.1108/13683041011027418
- The Insight Research Cooperation. (2012). Worldwide Telecommunications Industry Revenue. Retrieved from [http://www.insight-corp.com/pr/1\\_2\\_12.asp](http://www.insight-corp.com/pr/1_2_12.asp)
- The Open Group. (2012). Open Group Architecture Forum. Retrieved from <http://www.opengroup.org/architecture/>
- The White House. (2009). *The Comprehensive National Cybersecurity Initiative* (pp. 1-5). Retrieved from <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>
- The White House. (2011). Cyberspace Policy Review, Assuring a Trusted and Resilient Information. Retrieved from [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)
- Toal, P., Herron, A., Rees, J., McLaughlin, P., & Young, D. (2011). *Information Security: A Conceptual Architecture Approach [White Paper]*. Retrieved from [www.oracle.com/technetwork/articles/entarch/arch-approach-inf-sec-360705.pdf](http://www.oracle.com/technetwork/articles/entarch/arch-approach-inf-sec-360705.pdf)
- Trim, P. R. J., & Lee, Y.-I. (2010). A security framework for protecting business, government and society from cyber attacks. *2010 5th International Conference on System of Systems Engineering*, 1-6. Ieee. doi:10.1109/SYSOSE.2010.5544085
- Tsohou, A., Kokolakis, S., Lambrinoudakis, C., & Gritzalis, S. (2010). Information Systems Security Management: A Review and a Classification of the ISO Standards. *Next Generation Society. Technological and Legal Issues*, 220-235. Springer.
- U.S. DoD. (2009). *The DoDAF Architecture Framework Version 2.0*. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.190.7841&rep=rep1&type=pdf>

- U.S. DoD. (2011). *Department of defense Strategy for operating in cyberspace*. Retrieved from <http://www.defense.gov/news/d20110714cyber.pdf>
- Unified Compliance Framework™ (UCF). (2012). The Unified Compliance Framework™. Retrieved from <https://www.unifiedcompliance.com/>
- Von Solms, R., Thomson, K. L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security South Africa (ISSA), 2011* (pp. 1–6). Johannesburg: IEEE. doi:978-1-4577-1481-8
- Wang, A. J. A. (2005). Information security models and metrics. *Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43*, 2, 178. New York, New York, USA: ACM Press. doi:10.1145/1167253.1167295
- Wangenheim, C. von, Hauck, J., & Salviano, C. (2010). Systematic Literature Review of Software Process Capability/Maturity Models. *Page 1 Proceedings of International Conference on Software Process. Improvement And Capability dEtermination (SPICE)*. Pisa. Retrieved from [http://www.inf.ufsc.br/~gresse/download/SPICE2010\\_Systematic\\_Literature\\_vf.pdf](http://www.inf.ufsc.br/~gresse/download/SPICE2010_Systematic_Literature_vf.pdf)
- Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Course Technology Ptr.
- Wu, I.-L., & Kuo, Y.-Z. (2012). A Balanced Scorecard Approach in Assessing IT Value in Healthcare Sector: An Empirical Examination. *Journal of medical systems*. doi:10.1007/s10916-012-9834-2
- Zachman International®. (2012). Zachman Framework 3.0. Retrieved from <http://www.zachman.com/>
- Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & Security*, 26(3), 256–265. Elsevier. doi:10.1016/j.cose.2006.11.003
- el Kettani, M. D. E., & Debbagh, T. (2008). NCSec: a national cyber security referential for the development of a code of practice in national cyber security management. *Proceedings of the 2nd international conference on Theory and practice of electronic governance* (pp. 373–380). ACM. doi:10.1145/1509096.1509174
- office of Management and Budget. (2012). Federal Enterprise Architecture (FEA). *The White House*. Retrieved from <http://www.whitehouse.gov/omb/e-gov/fea>

## B. DETAILED FRAMEWORKS COMPARISON

Framework/Model	Category	Resilience	Measure Performance	Security Level	Compliance	CSS Gaps	Holistic
Nnolim (2007)	Management and Governance(Section 2.2.1)	Y	N	N	N	N	N
Zuccato (2007)		Y	N	N	N	N	N
Janssen & Hjort-Madsen (2007)		Y	N	N	Y	N	N
ITU(2008)		Y	N	N	N	Y	Y
Von Solms, Thomson, & Maninjwa(2011)		Y	Y	N	Y	N	N
Jo Kim, & Won(2011)		Y	N	Y	N	Y	N
Neubauer et al. (2005)		Y	N	Y	N	N	N
Management and Governance		Y	N	N	N	N	N
Barnat(2011)	Generic Frameworks (Section 2.2.5)	N	Y	N	N	N	Y
Trim & Lee (2010)		N	N/A	N/A	N/A	N/A	Y
Generic Frameworks		N	Y	N	N	N	Y
Otoom (2011)	Customized Frameworks	N	N	Y	N	N	Y
iGRC(2011)		N	N	Y	Y	N	Y

Framework/Model	Category	Resilience	Measure Performance	Security Level	Compliance	CSS Gaps	Holistic
el Kettani & Debbagh(2008)		Y	N	N	N	N	Y
Customized Frameworks		N	N	Y	N	N	Y
Fielden (2011)	Guidelines(Section 2.2.2)	Y	N	N	Y	N	Y
ENISA(2011)		Y	N	N	Y	N	Y
HM Government(2010)		Y	N	N	Y	N	Y
The White House (2009)		Y	N	N	Y	N	Y
U.S. DoD(2011)		Y	N	N	Y	N	Y
Phahlamohlaka et al. (2011)		Y	N	N	N	N	Y
Estonia Department of Defense (2008)		Y	N	N	Y	N	Y
Federal Ministry of the Interior(2011)		Y	N	N	Y	N	Y
Government Of Aus.(2008)		Y	N	N	Y	N	Y
MolCT(2011)		Y	N	N	Y	N	Y
Guidelines		Y	N	N	Y	N	Y
SSE-CMM,ISO/IEC 21827	Security Maturity Models (Section 2.2.4)	Y	N	Y	N/A	N/A	N

Framework/Model	Category	Resilience	Measure Performance	Security Level	Compliance	CSS Gaps	Holistic
CMMI,Ahern, Clouse, & Turner(2008)		Y	Y	Y	N/A	N/A	N
ISPMG,Stacey, (1996)		Y	N	Y	N/A	N/A	N
SMM,Kurrek(2002)		N	N	Y	N/A	N/A	N
OCTAVE®,Alberts & Dorofee(2003)		Y	Y	Y	N/A	N/A	Y
FIPS PUB 140-2		Security Metrics (Section 2.2.4)	N	N	N	N/A	N/A
ITSEC,TCSEC, Common Criteria	N		N	N	N/A	N/A	Y
ISO/IEC 15408	N		N	N	N/A	N/A	N
CTCPEC	Y		N	N	N/A	N/A	Y
German IT protection Manual	Y		N	N	N/A	N/A	Y
Security Maturity and Metrics			Y	N	Y	Y	Y
IBM, Buecker et. Al. (2010)	Provider's Specific Frameworks(Section 2.2.6)	Y	Y	Y	Y	N	N
Oracle, Toal et. Al.(2011)		Y	Y	Y	Y	N	N
Provider 's Specific Frameworks		Y	Y	Y	Y	N	N
EISA	Open Frameworks (Section 2.2.7)	Y	Y	Y	Y	N	N

Framework/Model	Category	Resilience	Measure Performance	Security Level	Compliance	CSS Gaps	Holistic
SABSA		Y	Y	Y	Y	N	N
Zachman		Y	Y	Y	Y	N	N
E2AF		Y	Y	Y	Y	N	N
TOGAF		Y	Y	Y	Y	N	N
FEA		Y	Y	Y	Y	N	N
DoDAF		Y	Y	Y	Y	N	N
Open Frameworks		Y	Y	Y	Y	N	N
CSS-IF	Holistic Framework CHAPTER 3)	Y	Y	Y	Y	Y	Y
Holistic Frameworks		Y	Y	Y	Y	Y	Y

### C. HOLISTIC BALANCED SCORECARD FOR NIACSS

Holistic ITsec-Balanced Scorecard(H-ITsec-BSC)										
Perspective		Progress								
Business Perspective		23.40%								
Stakeholder Orientation Perspective		52.05%								
Internal Processes Perspective		55.32%								
Future Readiness Perspective		56.88%								
Total Progress		45.07%								
Scorecard includes 4 categories, 11 indicators										
Help										
- You can change the values in "weight" column, the value must be between 1 and 10;										
"10" value means that the perspective or goal is the most valuable										
- You can change the values in "Value" column;										
Strategy tree and scorecard details for 13/04/2012 :										
Perspective	Indicator	Weight (x of 10)	Description	Value	Measure unit	Target Value			Progress	Absolute Progress
Business Perspective		3		23.40%						
	Reduce number of Attacks to less than 5%	6		33.30%	%	93.00%			31.38%	1.8827586
	% e- guments applications availability	1		7.20%	%	90.00%			-8.95%	-0.0894737
	% Decrease in threats per Service Offered	3		28.40%	%	93.00%			18.23%	0.5468354
Total Progress in group		3	Business Pers	23.40%					23.40%	0.7020361

	<i>Stakeholder Orientation</i>		3		52.05%					
		Certification Levels	5		83.20%	%	86.00%		96.50%	4.825
		Number of Training Sessions	5		18.70%	%	88.00%		7.60%	0.38
	Total Progress in group		3	Stakeholder C	52.05%				52.05%	1.5615
	<i>Internal Processes Persp</i>		2		55.32%					
		% Increase in ITSec Project Success	2		93.30%	%	85.00%		110.64%	2.2128205
		% Decrease in average time to recover from threats	1		21.80%	%	88.00%		18.27%	0.182716
		New indicator 9	7		43.60%	%	85.00%		44.80%	3.136
	Total Progress in group		2	Internal Proce	55.32%				55.32%	1.1063073
	<i>Future Readiness Perspe</i>		2		56.88%					
		Employee Turnover	7		52.30%	%	86.00%		54.46%	3.8121622
		% expected Number of Threats	2		66.00%	%	89.00%		72.62%	1.452381
		%Exptected Loss per a threat	1		44.70%	%	92.00%		42.32%	0.4231707
	Total Progress in group		2	Future Readin	56.88%				56.88%	1.1375428
	Total Progress in Holistic ITsec-Balanced Scor				45.07%					
	Powered by	<a href="#">BSC Designer PRO</a>								



## D. LETTER OF COOPERATION WITH NITC

PHILADELPHIA UNIVERSITY  
Faculty of Information Technology

Dean's Office



جامعة فيلادلفيا  
كلية تكنولوجيا المعلومات  
مكتب العميد

التاريخ : 2012/03/20  
الرقم : 825-20/100

عطوفة مدير مركز تكنولوجيا المعلومات الوطني المحترم

تحية طيبة وبعد ،،،

يرجى التفضل بتسهيل مهمة طالب الماجستير "عيسى علي فلاح" من قسم علم الحاسوب  
كلية تكنولوجيا المعلومات بجامعة فيلادلفيا لإنجاز بحثه في مجال أمن المعلومات حيث يمكن الاستفادة  
من نتائج البحث في خدمة المؤسسات الحكومية.

للتفضل بالإطلاع وإجراء ما ترونه مناسباً،،،

رئيس الجامعة  
الدكتور مروان واسم كمال



م.د. الشؤون الإدارية  
م.د. أمم المعلومات والاعتماد  
م.د. التعليم والتطوير الأكاديمي  
م.د. المستشار والمدير العام لتنظيم الاستراتيجيات

✓  
✓  
✓

مركز تكنولوجيا المعلومات الوطني	
البريد الإلكتروني	
الرقم : ٦٥٨ / ع	التاريخ : ٢٠١٢ / ٤ / ١
ملاحظات :	

### E. APPLICABILITY OF CSS-IF TO JORDAN NIACSS

**Question: Do you think that the CSS-IF is applicable to the NIACSS?**

Specialization Domain(s)	Yes/No	Comments
Cyber security strategy formulator and implementer, PMO manager, Senior Consultant	Yes	-
Networks Senior Engineer	Yes	Human Resources will be very critical to the success of the implementation
Head of Jordan's DNS/IDN Team ( الاردن، .jo )	Yes	need further analysis in change management
e-services and Technical Support senior engineer	Yes	-
Systems Engineer	Yes	-
Accountant	Yes	-
HR Manager	Yes	-
Network Engineering	Yes	-

# إطار تنفيذي عام لاستراتيجيات الأمن السيبراني

من قبل

عيسى علي فلاح عتوم

بإشراف

د. عامر أبو علي

د. أحمد عتوم

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في علم الحاسوب

عمادة البحث العلمي والدراسات العليا

جامعة فيلادلفيا

أيار ٢٠١٢

## ملخص

يعتبر تنفيذ استراتيجيات الأمن السيبراني (Cyber Security Strategy) مشكلة لكثير من الدول. يعتبر الفضاء السيبراني (Cyber Space) غير آمن لأسباب متعددة نذكر منها ما يلي: عدم توفر إطار تنفيذي منظم ، قلة ادوات فحص الأداء الشمولية على مستوى الدول وقلة التعاون بين الحكومات في مجال الأمن السيبراني. بالرغم من وجود عدة أطر للأمن السيبراني إلا أن معظمها ينظر للمشكلة من منظور إداري بدلا من منظور هندسة أمن المعلومات.

تقترح هذه الرسالة إطارا تنفيذيا لاستراتيجيات الأمن السيبراني (CSS-IF) والذي يوفر الفوائد التالية:

- (١) يساعد مختلف الحكومات على تنفيذ استراتيجيات الأمن السيبراني بطريقة ممنهجة تساعد على تطافر جهود جميع المعنيين. (٢) يوفر الاطار المقترح طريقة لكشف تهديدات أمن المعلومات مبكرا ومعالجة مخاطرها لمختلف أنظمة المعلومات خاصة الحرجة منها. (٣) يدعم أمن المعلومات من خلال أدوات قياس شمولية. (٤) يساعد على تحويل استراتيجيات الأمن السيبراني من اللغة الطبيعية إلى مجموعة من متطلبات النظم الادارية والأمنية .

تم اثبات الاطار المقترح بطريقة مفاهيمية وطريقة عملية : بتطبيق الاطار المقترح على استراتيجية أمن المعلومات في الاردن (Case Study) وباستخدام شبكة بايز (Bayes Belief Network) . تبين أن الاطار المقترح قابل للتطبيق في الاردن وترتبط مكوناته بعلاقة قوية تهدف الى تحقيق أهداف الامن السيبراني المتوقعة. تفوق الاطار المقترح على الاطر الاخرى بست خصائص. بالرغم من أن الاطار المقترح طُوّر لتنفيذ استراتيجيات الامن السيبراني الا انه قد يمكن تعميمه في المستقبل لتنفيذ استراتيجيات ضمن مجالات أخرى.