Operationalizing Information Security Standards in UAE Security Agencies

Abdulla Aljallaf

MA Thesis

December 2017

جامعة خليفة
KHALIFA UNIVERSITY

A thesis submitted to Khalifa University of Science and Technology in accordance with the requirements of the degree of Master of Arts in International and Civil Security

Operationalizing Security Standards in UAE Security Agencies

By

Abdulla Aljallaf

A thesis submitted in partial fulfilment of the requirements for the degree of

Master of Arts in International and Civil Security

at

Khalifa University

Thesis Committee

Dr. Athol Yates (Supervisor & Examiner), *Khalifa University*

Dr. Brendon Cannon (Second Examiner), *Khalifa University*

Dr Ash Rossiter (Committee Chair), *Khalifa University*

December 2017

جامعة خليفة
KHALIFA UNIVERSITY

i Abstract

Abdulla Aljallaf, “Operationalizing Security Standards in UAE Security Agencies”, M.A. Thesis, M.A. in International and Civil Security, Institute of International and Civil Security, Khalifa University of Science and Technology, United Arab Emirates, December, 2017.

This paper illustrates the operationalizing process of information security best practice standards and the use of checklist approach for auditing and assessing activities to enhance and improve the information security practices in UAE security agencies. The research question is “How can Information security best practice standards be operationalized into checklists for auditing and assessing UAE security agencies?”

The topic has been selected and addressed due to the importance of information security and the current massive rise in information security threats, which targets and attacks government and private business sectors to achieve different political, military and economic objectives.

The thesis consists of five main chapters, and the research methodology is the action learning research, which has been implemented to execute a project that will answer the research question. The literature will discuss three domains, operationalizing the security standards, Auditing and assessing practices as well as the benefits of using a checklist.

The key objectives were, to review and analyse number of international information security standards, produce a comprehensive checklist that will facilitate the audits and assessments activities, identify the security posture and finally to enforce the implementation of the applicable security controls.

Indexing Terms: Information security, UAE security agencies, and Information security best practice standards.

ii Acknowledgments

I would first like to show my gratitude to my thesis advisor Dr. Athol Yates for his continues support, guidance, directions, recommendations and great supervision efforts throughout my years of study and through the process of researching and writing this thesis.

I would also like to acknowledge Dr. Brendon Cannon as the second reader of this thesis, and I am gratefully indebted to his very valuable comments on this thesis.

Many thanks to My Colleagues and My Friends for their passionate participation and input into this thesis.

Finally, I must express my very profound gratitude to my caring, loving, and supportive Wife, for providing me with unfailing support and continuous encouragement.

This accomplishment would not have been possible without them. Thank you.

Abdulla Aljallaf

iii Declaration and Copyright

iv Declaration

I declare that the work in this thesis was carried out in accordance with the regulations of Khalifa University of Science, Technology and Research. The work is entirely my own except where indicated by special reference in the text. Any views expressed in the thesis are those of the author and in no way represent those of Khalifa University of Science and Technology. No part of the thesis has been presented to any other university for any degree.

Author Name: Abdulla Aljallaf

Author Signature: 

Date: **19-12-2017**

v Copyright ©

Table of Contents

i Abstract i
ii Acknowledgments ii
iii Declaration and Copyright iii
iv Declaration iii
v Copyright © iii
Table of Contents 1
List of Figures 3
List of Tables 3
Chapter 1: Introduction 4
1.1 Context to the topic 4
1.2 Problem statement 12
1.3 Research Objectives 13
1.3.1 Research Aim 13
1.3.2 Research question 13
1.3.3 Concepts 13
Chapter 2: Academic Literature Review 15
2.1 The implementation of Security Standards 15
2.2 The process of operationalization Security Standards 17
2.2.1 Securing the support of the executive 17
2.2.2 Definition of the Scope of the Information Security 18
2.2.3 Assets evaluation and Risk Analysis 18
2.2.4 Definition of the Information Security 18
2.2.5 Training and Building Competencies 19
2.2.6 Standards Maintenance and Monitoring 20
2.3 Auditing and Assessing Security Measures 20
2.3.1 Red Teaming and Penetration Tests 20
2.3.2 Assessing Security Measures 21
2.4 Checklists: Benefits in Operationalizing Security Standards 23
Chapter 3: Research Approach 24
3.1 Action Learning research methodology 24

3.2 Cases of Action Learning Research Methodology....26
3.2.1 Case 1: Internet-Based Collaborative Learning Initiative for Community Health..26
3.2.2 Case 2: Conferencing in a learning society....26
3.3 Application of Action Learning to the thesis. 27
3.4 Limitation of Findings....28
3.4.1 Validity....28
3.4.2 Reliability....28
3.4.3 Generalizability....28
Chapter 4: Results....29
The Plan and Act stages....29
4.1 Plan....29
4.2 Act....29
4.2.1 Producing a comparison Table of the key International Standards....29
4.2.2 Working out which elements to include in the checklist....34
4.2.3 Producing the checklist....34
4.2.4 what results did you get when you applied the checklist. 35
The Reflect and Learn stages....35
4.3 Reflect 35
4.4 Learn....36
4.4.1 what went well and not so well?....36
4.4.2 The changes of the checklist as a result of the learning stage 37
4.5 Plan: the second cycle 38
Chapter 5: Conclusions....39
5.1 Answering the research question....39
5.2 Benefits of using Automated Checklist....40
5.3 Common Recommendations for government agencies....41
5.4 Research reflection....44
References....46

List of Figures

Figure 1: Top 5 attacks on government web applications Q1-2017 5

Figure 2: Top 10 attacks on web applications Q1-2017 5

Figure 3: Most common attacks Q1-2017 5

Figure 4: UAE Government sector incidents categories-2016 6

Figure 5: Action Learning Cycle 27

List of Tables

Table 1: Overall government and critical infrastructures-2016 6

Table 2: Government organisations-2016 6

Table 3: Information security standards comparison 30

Chapter 1: Introduction

1.1 Context to the topic

Nowadays, a majority of the world's governments are experiencing and witnessing the current trend in information security threats targeting different sectors and utilizing creative and innovative attacking types and methods, governments are facing a severe challenges against these threats and investing a huge budget on developing and implementing information security measures and controls in order to protect their critical sectors focusing on the information infrastructure such as energy, industrial, financial and others important sectors which falls under the national security mandates.

With the current trend in the security threats, which targets and attacks different government and private business sectors to steal information, disrupt systems and manipulate data to achieve different political, military and economic objectives. All measures must be taken at a strategic level and should covered different components and dimensions of Information security. Key dimensions of information security form the thesis perspectives will cover cyber, physical, document and human recourses security which considered the main elements of any security system especially for the security agencies.

With the rising sophistication of the types and methods of attacks and after reviewing and analysing different information security reports form leading specialize international organization such as Symantec, Gartner and Positive Technologies. Also referred locally to aeCERT, to understand, highlight and illustrate the key information security threats trends and statistics that associated with four information security dimension that will be discussed in details later in this section. The following samples of these statistics will clarify some threats and shows their current trends:

Positive technologies, cyber attacks statistics report Quarter 1, 2017

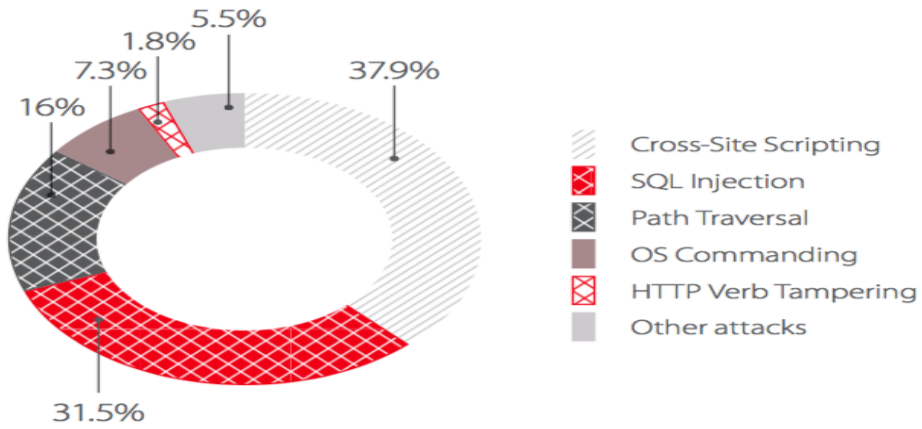

Figure 1: Top 5 attacks on government web applications Q1-2017

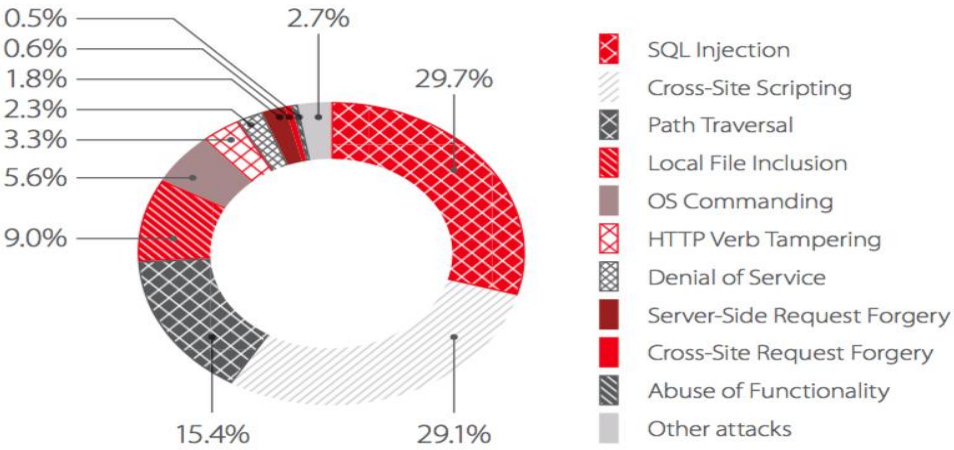

Figure 2: Top 10 attacks on web applications Q1-2017

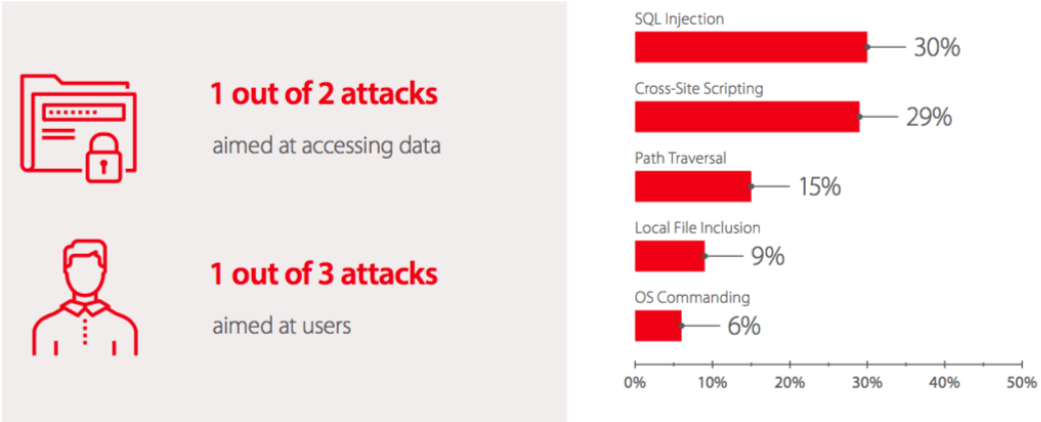

Figure 3: Most common attacks Q1-2017

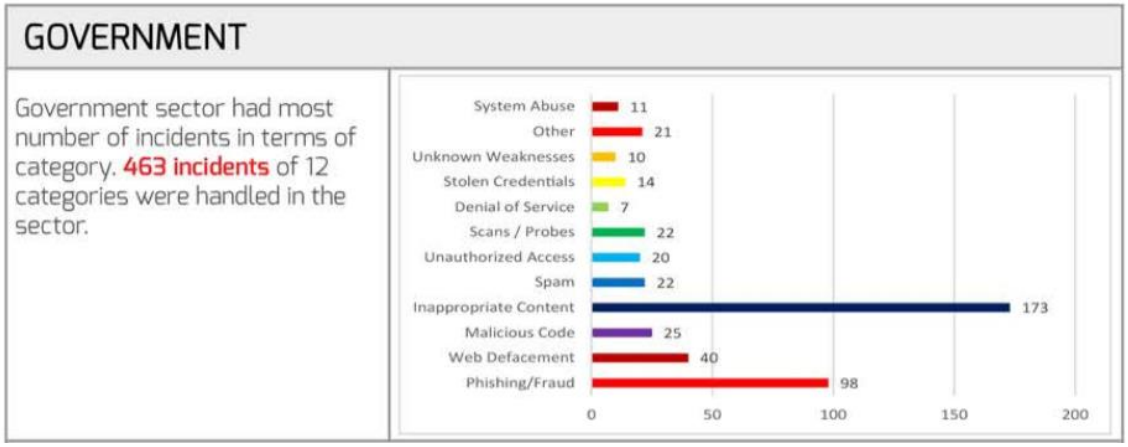

Figure 4: UAE Government sector incidents categories-2016

Symantec, Internet Security Threat Report- Government 2016

Top attacks	%
Web (server)	35.6%
Shellcode/Exploit	31.5%
Web (browser)	25.2%
DoS	2.9%
FTP (server)	0.7%

Table 1: Overall government and critical infrastructures-2016

Top attacks	%
Web (server)	35.6%
Shellcode/Exploit	31.5%
Web (browser)	25.2%
DoS	2.9%
FTP (server)	0.7%

Table 2: Government organisations-2016

The first key threat that is faced by these governments is injection attacks, which are classified into LDAP (Lightweight directory Access protocol) injection, SQL (Structured Query language) injection, and Operating System Injection. This attack occurs for systems that require user input of data from the background where they can run a command which intron queries the database either inserting unwanted data or altering the contents of the database (Timothy, Helsey, & Baston, 2013). Despite the existence of many types of attacks, the most common one is the SQL injection commonly known as the SQLi, which exposes the data in the database.

The second key security threat facing governments across the world is the Broken Authentication and Session Management (Zadelhoff, 2016). It occurs to systems whose functions lack proper implementation creating a surface through which attackers exposes them to criminals through violation of the existing session Identifications and passwords, thereby exploiting data and privileges using the existing authenticated session. Based on the fact that sessions are unique for specific users, attackers can masquerade as the particular users through stolen passwords or tokens and gain access to the system.

Thirdly, according to Zadelhoff (2016), Cross-Site Scripting is an attack that mainly targets the web-based applications and information systems. It entails the insertion of scripts on the web pages allowing the attackers to bypass the existing access controls (Zadelhoff, 2016). In this regard, the browser is tricked to enable the input of untrusted data from a user and happens when the attacker has access to the software codes. When a cross-site script is run successfully, it can allow the attacker to trick the users to key in information in sites that are not authenticated although, to the users, these sites appear authentic (Zadelhoff, 2016). These other sites may either steal data from the users or contain codes that are malicious.

Fourthly, all systems should have a way of drawing a line between what is permitted for all the users depending on the privileges that it allocates them. The type of attack that breaks the set access controls is known as the broken access control (Melvins, 2013). With this method of access control, it requires that users should have access to only what is necessary for their functionality and when it is broken, users with lower privileges can access tasks that are needed by people with higher rights. According to Melvins (2013), broken access control occurs when developers fail to implement proper access control mechanisms through the limitation of the rules of access. It is a requirement that rules should be put all across the code and not at one point alone. Therefore, failure to implement these access controls at specific points of the code creates loopholes that allow these users access information for higher privileged users.

According to Melvins (2013), the fifth most dangerous threat faced by the governments is the security configuration. A majority of the systems are not configured correctly regarding the manner in which their databases are designed; servers are configured, as well as the frameworks they operate on (Melvins, 2013). All these configurations should be updated on a regular basis to ensure that they are not exploitable by the attackers. Failure to this, it gives the attacker an opportunity to access the systems through the privileged mode thus accessing sensitive data and functionalities. An example of poor configuration is where the developer leaves the root to a particular resource open or leaves the path open thus enabling the attacker to use diversionary tactics and in return access other resources illegally.

System security measures standardization is of utmost necessity. A majority of the problems that are emerging in the field of information security are similar, and therefore approaches that are adopted should be constant. This is crucial, as it will ensure that the strategies that are selected in problem solving are identical. With the standardization of security measures, it will be possible for countries to cooperate and partner in viable areas (Puskar, 2012). Moreover, widespread and rigid security measures will be implementable in their security initiatives through the cooperation. Standardization of security measures will also encourage innovation as the needs of the security agencies will be known, and therefore their analysis becomes quite easier (Puskar, 2012). According to Erik Puskar (2012), standardization will not only encourage both cooperation and innovation, but it will also improve on economic efficiencies when dealing with information security challenges.

There are a number of organizations that specialize in the development of the security standards across the world. One of these organizations is the International Organization for Standardization (ISO) which a federation that was pioneered in 1947 functions worldwide and is made up of many regional agencies from about one hundred and forty-five countries (Steve, 2014). This organization is famous for the ISO 27001: 2013, which is an international standard that has been developed to provide requirements of regularly improving information systems security. It argues that the adoption of an information system by any organization is a critical milestone although the mechanisms of protecting these information systems should be purely dependent on the ever-changing requirements and risk management process (Steve, 2014). It, therefore, ensures that information systems are placed exclusively at the centre of the overall management structure of an organization as well as its processed. Thus, it is expected that information systems be changed and scaled according to the needs of the agencies.

The second organization and developer of standards is the National Institute of Standards and Technology (NIST) that is a governmental institution in the United States that is responsible for the definition of standards for protecting and ensuring that sensitive as well as unclassified data (NIST, 2013). It has a Computer security Resource Center (CSRC) that handles NIST Information Technology security standards. This canter has developed many standards including but not limited to: Federal Information Processing Standard 200 and 201, Computer Security Publication (SP800 series), and NIST Information Security handbook (NIST, 2013).

Institute of Electrical and Electronic Engineers (IEEE) refers to an international body that develops engineering standards that are usable across the world. Additionally, its standards are also established around the globe involving significant stakeholders in different disciplines. Some of these disciplines are engineering as a profession and recently information security. Other than the development of security standards, it develops as well as advances global technologies to facilitate interoperability. In the recent past, it has embarked on the development of standards that will increase cybersecurity while at the same time increasing web presence of cybersecurity experts.

ASIS International, on the other hand, is a group of professionals that have joined hands to ensure that security standards in the information security are adhered to. Having a membership of over thirty-eight thousand, the ASIS is determined to ensure that the security professional's productivity and effectiveness are raised. It, therefore, ensures that the professionals handling the system's information security.

The British Standards Institute (BSI) is the other standards organization and its existence spans over one century. It specializes in the development of security policies as well as standards of information systems (UK Cabinet Office, 2012). It has developed one of the most famous standards and policy is known as the British Standard 7799 which has earned recognition worldwide (UK Cabinet Office, 2012). This standard applies to information systems audits as well as their prescribed standards. It also has a section of requirements for information security standard certification.

Even though there is a very thin line separating information security from IT security, there are a number of things that distinguish them. With information security, it encompasses a wider scope than that of IT security (Anderson, Mesic, & Scheiern, 2003). With information security, it ensures that information is protected against destruction, modification, disruption, access, disclosure, and use and is used regardless of the data form in question (Anderson,

Mesic, & Scheiern, 2003). This means that it applies to both the physical data and the electronic data. According to ISO, information security defined as the protection and preserving the confidentiality, integrity and availability of information. It also involves protecting and preserving the authenticity and reliability of information and ensuring that entities are implementing the related security measures and controls.

Although the discussion of this section is purely for information security, and most of the key threats seems to be related to IT security, it is essential to understand the meaning of the term information security from the research perspectives. Information security can be explained from four different dimensions. These four dimensions are; cyber security, document security, physical security, and human resource security. Cyber security refers to the process of assuring the continuity of business operations through maintenance of integrity, confidentiality, and availability of information systems (Timothy, Helsey, & Baston, 2013). This is assured through installation of tools that help identify, detect, protect, and prevent digital information from being compromised. Irrespective of the format in which the data is stored or the manner in which it is being transmitted, the purpose of information security is to ensure that informational assets are protected. With confidentiality, sensitive information at rest and on transit should be protected against being accessed by unauthorized parties (Vlacheas, Stavroulaki, & Demestichas, 2011). For Integrity, data on transit must not be altered or modified without being authorized by the right parties. With the objective of availability, the system or information must be up and running at the required times (Vlacheas, Stavroulaki, & Demestichas, 2011).

Document security refers to the process by which crucial documents are delivered, backed up, processed, stored, filed, and eventually disposed off if need arises (Emily, 2015). To a greater extent, document security involves the process of ensuring that at no point are the organization files, accessed by the unauthorised parties, or unavailable from access. There are different ways of ensuring that these processes happen. These entail document encryption, document password protection, and document access control. (Schimdt, Caolionn, Hirokazu, & Akhil, 2015). This should cover all classified documents in any forms.

Physical security refers to protection that is afforded to information systems through tangible mechanisms such as sign-in/sign-out options, biometrics, lock and key methods, and through cabling protection such as shields (Waters, Ball, & Dudgeon, 2008). With the lock and key method, it aims at preventing intruders from accessing sensitive areas such as the server rooms where padlocks are used and keys kept in custody of a single person (Emily, 2015).

Visitor passes on the other hand are ways of ensuring that no unauthorized people gain access to organizations and in return who might compromise information security. With all these and other information security approaches, they are bound to add a layer on to the existing information security architecture.

Human resource security entails the use of human beings to offer protection against information systems. Different approaches are used here which entails equipping employees with the necessary technical knowhow of information systems such as certifications (Ajit & Johnson, 2008). It also involves screening of all employees prior, during and post of their employment period and adopting a specific security clearance process for those who have access to sensitive information. Other than these two approaches, it may include signing non-disclosure agreements with different stakeholders on how they must maintain information privacy.

No matter the size of the organization or the government agency, it is very critical to ensure that information security is guaranteed. First, information security ensures that confidential and sensitive data not accessed by unauthorized persons (Vlacheas, Stavroulaki, & Demestichas, 2011). With information security, it will also be easy for the government to transfer as well as securely receive information. It also not only secures the informational assets of the organization but also shows how serious the government agency is towards securing its data and information. When information is not adequately secured, the customers, employees and other shareholders are also exposed and therefore information security ensures that they are protected (Vlacheas, Stavroulaki, & Demestichas, 2011).

Example of information systems compromise include Estonia Attack, and the Georgia Denial of Service Attack. The Estonia attack occurred in April 2007 and involved major government agencies, news houses, and financial institutions (McGuinness, 2017). This attack emanated from the decision by the Estonian government to shift the Russian Monument from the city centre to the military cemetery (McGuinness, 2017). Prominent people's websites and systems were compromised defacing them and rendering others unavailable. As a result, several measures were taken to ensure that the country's information systems will never be compromised in terms of their confidentiality, integrity, and availability (McGuinness, 2017).

The Georgian denial of service attack occurred in 2008 and emanated from the crush between Russia and Georgia over the area of Ossetia (Nazario, 2008). The attack targeted Georgia government website especially that of the president although since the first incident a number of them have occurred. Compared to the Estonia's case, this one has been more intense owing to the extended use of botnets, which have a high bandwidth and faster computers

(Nazario, 2008). These attacks have yet to be settled although they have highly deteriorated the information security trust on the users in the country.

1.2 Problem statement

Since the security sector and the security agencies considered as an important target for information security attacks, it is necessary to have a comprehensive methodology within the sector to ensure the security of information, as many security agencies are ignored the application of the international security standards mentioned earlier due to many reasons such as, the lack of its recognition within the sector, the absence of the compliance requirements from the regulators and the lack of interest to obtain the certificates such as ISO for security purposes.

As discussed and due to the security purposes, security audit and assessment activities were very limited and assigned only to internal auditors in some of the security agencies. Their experiences are based on their academic knowledge or the previous job practices and they do refer and use the international security standards and best practices, but often not in systematic approaches.

Due to the different specialties and nature of work of the UAE security agencies, it is necessary to develop a customized information security standard to cover all the information security dimensions mentioned previously, and to achieve this, a comprehensive auditing checklist and guidance should be prepared after studying and analysing the international standards and best practices. This will help to adopt a risk management methodology that includes assessing the current situation, identifying and analysing the compliance risks with the security controls related to each security dimension, developing plans to address them and mitigating their potential impact, activating the role of those concerned to assess the security situation systematically and work on the continuous improvements of the security system overall.

Information security and the relationship of the four dimensions should also be clarified and explained to support and ensure information security. The security responsibilities in the authorities are often distributed and managed by different teams with limited and poor coordination between them.

1.3 Research Objectives

1.3.1 Research Aim

The aim of this research is to develop a systematic approach and a comprehensive audit and assessment checklist in order to improve the information security practices by applying the action learning research methodology

1.3.2 Research question

My research questions is:

How can Information security best practice standards be operationalized into checklists for auditing and assessing UAE security agencies?

1.3.3 Concepts

- **Information security:** In the context of this research, information security refers to the protection of information confidentiality, integrity and availability, by following international security standards and best practices and implementing security controls that are applicable to the working environment.

- **UAE security Agencies**: The security agencies within the scope of my work in a supervisory body, which are major security agencies, share a single vision towards the national security. The security agencies cannot be listed due to their sensitivity.

1.4 The Structure of the thesis

The paper will consists of five chapters that will cover the following:

- Chapter 1: Introducing the context of the topic, discussing the problem statement, stating the research aim and question. Also defining relevant and key concepts.
- Chapter 2: will cover the academic literature review on operationalizing the securitry standards, auditing and assessing practices and the benifits of using a checklist.
- Chapter 3: In this chapter, the research methodology will be discussed and illustrated by two case studies, also the application and the model of action learning cycle as well as the limitations of findings.
- Chapter 4: will cover the results based on the application of each stage of the action learning cycle which are, Plan, Act, Reflect and Learn
- Chapter 5: is the final chapter that will answer the research question, discuss the recommendations and summarise the research reflection.

Chapter 2: Academic Literature Review

2.1 The implementation of Security Standards

With the increase in cybersecurity concerns, companies are slowly and effectively taking the necessary measures to ensure that information security risks are being addressed. However, the approach taken by the private sectors is different compared to the one adopted by governments as well as government agencies (Schimdt et al. 2015). Experts argue that the boundary between the public and the private sectors' mode of operations especially the information security concept is being blurred by the increased public-private sector partnerships establishment (Schimdt et al. 2015). It is hard to make a conclusion on the network security status of private sectors based on the network attacks that occur to them. This is based on the fact that a majority of them do not disclose this crucial information although available statistics show that both the public and the private sectors have been affected by data security breaches (Schimdt et al. 2015).

According to Schimdt et al. (2015), statistics and studies have it that a majority of private sector companies are still losing crucial data, which ends up being used against them. For instance, in the United States, two significant retailers exposed their data on debit cards which made over forty-five million holders suffer the breach. Another incident is where a United States company lost crucial information about 4.5 million bank customers whose information was contained on a backup tape, which was also not encrypted (Schimdt et al. 2015). To ensure that these incidences do not recur in the future, the companies have adopted NIST standards.

These standards have been adopted to make sure that better security strategies are put in place. For instance, for organizations that lost massive data in the process, it has been made a requirement by their management that data must not be sent or kept without proper encryption (Schimdt, Caolionn, Hirokazu, & Akhil, 2015). The companies have also made it compulsory for the information stored in disks to be protected using strong passwords that comply with the latest security framework of the organization.

As is the requirement for the primary standards that exist, significant organizations in the world such as Walmart have made it compulsory for some things to be done (Melvins, 2013). The company conforms to the requirements of these standards through establishment and development of requirements. One of the requirements that these companies have complied with is the setting up of the protection profiles. These protection profiles set and create a definition of implementation-independent objectives and requirements that must be met in information security. For systems that have been implemented to meet specific needs of the

customers and those of the related products for their specific IT needs. All the protection profiles are meant to be reusable for systems that are related and contain useful requirements to help meet the set objectives. The PP (Protection Profile) can be developed as a functional standard in the procurement department or general user security requirements.

Security targets are the other documentation that has been implemented as part of the standards and involves all the IT security goals and objectives (UK Cabinet Office, 2012). Commonly known as terms of engagement (TOE), the security targets define the security assurance as well as functional requirements, which all work together to meet the expected requirements. The security target can conform to two or more protection profiles acting as a basis for system security evaluation. Upon evaluation of the security targets, the end product of the process is the protection profile, which is classified regarding the area it addresses. The first area addressed is the invalid input to a system, interconnection, and interrelations of multiple operations as well as physical probing.

Private companies that attempt to meet the requirements of these standards face some benefits and challenges. One of the benefits is that they have managed to improve the quality of services that are offered to their clients (Puskar, 2012). Secondly, it has improved and enabled many companies to participate in the improvement of international cybersecurity (Puskar, 2012). Thirdly, it has allowed organizations to raise their status to international status thereby enabling them to compete globally and enable them to acquire global approval in business competitions (Puskar, 2012).

The first challenge that has been that a number of the companies especially business start-ups may not afford to finance the requirements of these standards (NIST, 2013). Secondly, a majority of them are incapacitated with the human workforce that is required to maintain these standards. In fact, due to the high demand of the employees who are specialized with the certifications required by these standards, a majority of these companies receive high employee turnover (NIST, 2013). This occurs due to the fact that they are not able to maintain them with the little pay while they are receiving better pay from the companies' competitors.

The fourth challenge is that despite the standards having been passed and authorised to operate, quite some employees are not aware of what is expected of them and how they could work in such a complex environment. As a result of failure to comply with the requirements of these standards, many companies and individuals have fallen victims of severe systems attack (NIST, 2013). An issue such as the NIST's password policy has not been adhered to. A number of organizations and government agencies allow organizations to re-use their passwords once they have changed it.

2.2 The process of operationalization Security Standards

The process of operationalizing standards in an organization is chronological in order. This means that a series of steps have to be followed with some of them coming before others. This section addresses these steps that are followed in operationalizing information security standards. If chronology is not followed, this process risks suffering major setbacks, which can affect its successful implementation. However, strong adherence to these requirements and chronology can lead to better and more beneficial operationalization of information security standards. Additionally, strong adherence to these steps can increase the magnitude of information protected and secured saving the organization against losses both financially and socially (reputation).

Before operationalization of any information security standard, it is crucial for any company that plans to do so to ensure that it develops the necessary capacity concerning human resource. This involves making it a requirement that employees are handling the information security aspect of the organization must have the relevant professional experience, certification, and exposure. Below is the description of the approach that is followed when operationalizing the above-mentioned information security standards.

2.2.1 Securing the support of the executive

When adopting and implementing any system security standard, the decision must come from the top management of any organization. Because the management structure has the top, middle, and the lower level of administration, the decision of whether to adopt the standard must come from the top management. Top management in any organization is responsible for making decisions that affect the business on a long-term as well as on a long-term basis. With the middle management level, it is concerned with ensuring that these decisions that are made by the top management are interpreted and implemented in the right manner. Other than making crucial decisions, the senior management is concerned with authorization and allocation of resources for the standards that are being proposed to them.

Because a majority of these standards requires annual or periodic approval, it is crucial for the management to be involved in both approval and receiving updates after the specified time. Additionally, the top management is central to this process because it ensures that it determines the information security objectives and ensures that the set targets meet the regulatory needs and reflect the needs of the business.

2.2.2 Definition of the Scope of the Information Security

Contrary to the public opinion that has been developed out of the experience with many information security standards, a majority of the recent information security standards have addressed previous setbacks. They are therefore grounded on information security technical requirements as well as the reality of the same. It is, thus, a requirement that organizations must select the sections of the standards that affect them directly as opposed to generalizing the standard. Therefore, the scope of the standard chosen must not be lower than or higher than the existing requirements. The standard selected must define the processes of the organization as well as the security requirements for each of them whose results provide ground for the subsequent steps to be implemented.

2.2.3 Assets evaluation and Risk Analysis

This is the third step and involves evaluation of processing resources as well as a detailed risk analysis for these resources. Asset evaluation refers to the series of steps that are followed in reviewing information system resources, which culminates in a description of all the informational resources in an organization. Some of the assets of an organization that are tasked with information handling entail; network infrastructure, servers, customer information, hardware and cloud services. Assets that fall under the category of hardware include; the physical data storage and the computers. Servers are both virtual and physical which build up on the IT infrastructure of the company. Cloud services are the services that are offered by companies that rent virtual space and infrastructure as opposed to the companies buying their infrastructure.

Even as the evaluation process takes place, it is quite significant to note that only the relevant assets regarding sensitivity are subjected to evaluation. This information coincides with the Personal Data Protection Regulation (EU) which requires that organizations must maintain a proper filing system of their customers' personal information. For each of the assets that are mentioned above, the evaluation is based on the sensitivity of the information concerning the loss. After the resources have been evaluated; it is time for the relevant people to be assigned roles to perform in securing information.

2.2.4 Definition of the Information Security

In this step of the implementation process, the support of the top management has been secured, the objectives of the information security standard have been set, assets evaluation, as

well as risk evaluation, has already taken place, and a risk mitigation strategy has already been put in place. Therefore, the pending elements of information security can now be defined and necessary measures adopted in the organization. Based on the fact that requirements keep evolving, the process of definition of information security is a repetitive process. In this regard, adjustments have to be made on a regular basis. The components of information security are; roles, normative sources, knowledge sources, guides, training, outputs and inputs, instructions, procedures, processed, and policies.

The scope of these activities and the information standard should be carried out by the consultant or ensuring that the tools bought are ready-made. It is important to note that the standard should reflect the actual processes of an organization while at the same time introducing the required mechanisms of security. Defining know-how will enable the organization determines people who are responsible for specific roles and specific processes. These people will work together with the group to ensure that the standards are maintained and updated on a regular basis

2.2.5 Training and Building Competencies

After any standard has been selected and adopted by any organization, it is crucial for the organization to develop its workforce to respond to the changes that are bound to occur. At this stage, the organization has to specify the competencies that are required to handle the information security requirements. After the standard has been adopted and implemented, it should be explained to the entire organization as well as to its employees to acquaint them with its requirements. The training should be based on the requirements of the information security as well as on how the employees affect the information security of the organization. Training of organization employees is meant to improve competencies as well as redefine the role of the staff members in promoting the organization's information security.

Even as the training continues, it is important to define the roles, guides as well as training profiles of all the employees. Among the roles include; employees who represent any individual who has been employed in the organization, internal auditor who conducts audits to the systems. IT administrator will be responsible for handling and maintaining relevant IT infrastructure of the company. The top management is responsible for the establishment if directions as well as setting up organizational control.

2.2.6 Standards Maintenance and Monitoring

Before the standards become certified for full operation of information security, it must be tried to ensure that it is effective. In reality, a fully functional standard should incorporate all the organizational requirements. Additionally, before the audit process starts, it must have been implemented a few months before providing room for the necessary prior procedures. During this stage, the necessary risks mitigation plans must have been established and tried. After they have been developed, they need to be monitored to determine whether their operations are effective. Additionally, it is meant to ensure that the organization improves the information security infrastructure over time through the various recommendations.

2.3 Auditing and Assessing Security Measures

Two approaches are adopted in information systems audits. These entail internal audits and external audits. With the internal audits, it is conducted by the internal audit bodies although the feedbacks of the audits are discussed with the management of the agency (Timothy, Helsey, & Baston, 2013). Strategies for mitigating against the issues identified are suggested to the management which then is tasked with their implementation. With the external audits, they are conducted by an independent party who has neither the right nor the capability to make updates on the system being audited (Timothy, Helsey, & Baston, 2013). They differ from the internal auditors in that they do not share their findings with the government agency, are confined to reporting any existing gap in the organization.

However, although both of the two approaches of auditing aim at ensuring that organization's system security, none of them can be applied in the design process of a system. They may evaluate the system design process as well as implementation to determine whether it meets the expected standards but they cannot be used to offer advice on the real design should be done. In fact, if an auditor has designed a system, he or she should be involved in its audit. It is important to note that all audits are rigorous programs that must be followed from the beginning to the end. Different methods are used to perform the audit process in governments and their agencies as discussed below.

2.3.1 Red Teaming and Penetration Tests

A penetration test is an activity that is carried out with the aim of trying to bypass the access controls as well as gaining access to systems through unlawful means (Zadelhoff, 2016). The primary objective of carrying out a penetration test is to provide proof that the system is

subject to compromise. It acts as a red teaming exercise as opposed to a feasibility test for the systems as it does not determine the relative strength of control of the system. It has one setback, and this is the fact that it is impossible to determine if all the vulnerabilities have been found. The strength of this method is that it has a high level of ability to determine if the system requires internal control improvements. Based on the fact that the most significant threat to many organizations is the internet, penetration tests do not aim at addressing the security concerns, but instead, it has an unfocused effort.

According to Zadelhoff (2016), red teaming is different from penetration tests in that it attempts to compromise the system at all costs. This means that no vector limits it as it employs different approaches including physical approaches and virtual methods. A typical example of red teaming would entail attempting to steal 10,000 from a bank. This technique is applied by both the government and the private businesses to perform logical and physical tests (European Commission, 2013). This, therefore, indicates that there is simply no correlation between ethical attacks and red teaming.

Other than the penetration tests, the other auditing method is the vulnerability assessment that determines how vulnerable an organization or government agency is to external threats or attacks. All the primary vulnerabilities are identified and classified depending on the overall impact each of them can have on information security. In this approach of auditing information security, conventional methodologies such as cause-consequence analysis as well as fault tree analysis are used. After a vulnerability assessment has been conducted, the impact analysis should follow accompanied by the threat report to enable the agency know the risk of the organization as well as the attack points. Some of the standards used here are AS/NZS 4360:2006 (European Commission, 2013).

2.3.2 Assessing Security Measures

Information security assessment is a continuous process which entails discovery, correction, and prevention of various information security problems (Emily, 2015). It also forms a central part in the risk management process and is usually designed to ensure that information security levels are kept high. According to the Commonwealth Enterprise Information Security policy, it forms one of the most recommended security tasks that guarantee information security in organizations (UK Cabinet Office, 2012). However, before carrying out a system information security assessment, a number of considerations have to be carried out involving;

Justification of costs and it entails determining whether a new security approach would raise the expense (NIST, 2013). Due to the fact that this exercise may not generate direct income, it is difficult to justify the expense. If a security risk assessment is to be effective, it should educate the managers on how to cover information security concerns that affect the company. Productivity is the second consideration that requires to be carried out. This aims at determining the areas that require improvement to generate better results of operations. This entails determining whether the information systems are available and usable at the required times. Also, it entails determining whether the information systems authentication process is carried out as expected.

The process of assessing security measures follows well-defined sets of steps, which are aimed at understanding the information security systems, as well as environment in which it operates (Maxwell, 2013). By default, it should be noted that data format does not matter and what matters is the relevant information to be considered. Below are the steps for carrying out an analysis. First, the determination of a set of requirements and objectives expected of the systems. This should be done in comparison with the set standards and the acceptable standards at the same time. For instance, systems should not be easy to penetrate through vulnerability testing. Secondly, the systems and the network architecture need to be checked in terms of the assets that have been invested on it and whether they are sufficient to secure information. The red teams can be check the systems to ensure that they have been implemented in the right way and the loopholes have not been created for attack.

Thirdly, information available publicly or the one that has been made available to the onlookers is assessed. The size, the number, and the nature of the hardware assets can now be verified to see if any one of them is vulnerable to attack or has been vulnerable to attack. Information security requires that both physical security and human resource security be enabled. Documents that are containing useful information about the organization and the organization employees should not be exposed to the outsiders. In this regard, operating systems, systems on servers as well as systems used to manage networks should be assessed next for their vulnerability. Next, authentication and identification mechanisms should be assed with processes that are followed being no exception. Once all these aspects are assessed, it is time to ensure that the findings are documented for future use.

2.4 Checklists: Benefits in Operationalizing Security Standards

Checklists are important to an organization in different ways and can also be applied to the organizational processes in various ways. Just as it applies to other areas of business operations, so does it apply to the operationalization of standards in information security. Due to the fact that there are a number of tasks that require to be accomplished for an organization to be approved, a checklist would be important in different ways. Additionally, with a large number of things to be checked, chances are that one might end up forgetting if a check is not put in place. Additionally, with the many tasks at hand to be checked, chances are that one might also forget to accomplish all of them. Therefore, a checklist presents a better solution to these problems as well as a better way of resolving problems that might arise from errors made. Below is a detailed discussion of how beneficial these lists are to the process of operationalizing standards in information security.

First, according to Emily (2015), checklists can help build on the motivation of the implementer of standards. Checklists help outline all the things that require being done. The size of the checklist can act as motivation for all the work that needs to be done is placed right in front of you. The more detailed the checklist is, the more effective it is. Despite the fact that different people like a sequential process of doing things, checklists may not adopt such an approach and therefore due to work displayed in front of the researcher, they are able to present some motivation.

Emily (2015) argues that checklists can be very crucial when implementing the information security standards in that they can promote some sense of organization. In this regard, checklists require people to arrange the things that are required by order of accomplishment. This is crucial in that it is hard for one to forget a single item that is listed on the list. If it is a given standard that is being operationalized, all the requirements for the approval of the standard are written down, and therefore none of them is left out. However, despite the fact that the list promotes the organization, it is also time-consuming to organize a checklist one item at a time.

Thirdly, checklists facilitate prioritization of various items. In this regard, it enables the user to order the tasks to be accomplished first and at the same level with the most important ones (Emily, 2015). Once you organize the items, it is sometimes overwhelming to complete the tasks in order which can slow down the entire process. Because some people feel better skipping certain jobs and not following chronology, checklists are useful in letting them prioritize their important areas. Therefore, if one desires to complete certain tasks ahead of others, a checklist can help them do so quickly.

Chapter 3: Research Approach

3.1 Action learning research methodology

This approach involves in studying a scenario entails identification of a problem, and actions are taken to resolve the issues identified (Susman, 1983). After measures are taken, this research methodology is followed by an assessment of whether the efforts undertaken were successful or not and if the latter is true, better mechanisms are tried to resolve the issue. The difference between this research methodology and the rest is that it attaches some practical emphasis on solving problems while at the same time furthering social science concerns (Susman, 1983). Therefore, it is a dual commitment process of carrying out a research and obtaining a desirable direction in information systems security.

The model of implementing action research was developed by Kemmis and follows a cyclic nature with two cycles and many steps for each cycle. Gerald Susman(1983) researched on the various stages of this methodology and distinguished between the five phases that are followed in the methodology. The initial step of this methodology will be the detailed diagnosis, which aims at identifying the problems that are affecting the item under investigation. In the case of information systems research, this phase will attempt to gather as much information as possible about the security issues that are affecting an organization's information systems.

After the first phase of diagnosis is carried out, the postulation of the possible solutions takes place. The problems that have been identified in the diagnosis stage will be evaluated to determine the different ways through which the issues can be solved. It usually entails classification of the problems identified into subcategories, which are then assessed concerning possible alternatives that exist for their solutions (Kurt, 1946). In the case of information security, issues such as loss of confidentiality, integrity, and availability will be assessed regarding how they can be resolved.

The third phase entails selection and implementation of the real solution to the problem involves the selection of the best alternatives and its application (Kurt, 1946). The primary purpose of this action is to ensure that the identified issue is resolved. After this solution is implemented in the form of an action, the next phase entails an evaluation of the effectiveness of the action taken. In this regard, the activity is assessed concerning whether it helped solve the problem earlier identified by the researcher.

The fifth and the last phase of the action learning methodology involves specification of the learning findings (Kurt, 1946). In this regards, the outcomes of the research are identified in a document and prepared for a future necessary action. In case, the action taken in the previous phase did not yield the expected results, the researcher cannot proceed to the final specification phase. Instead, they have to implement the other best alternatives, and it is only after the selected method works that they can move on.

Other than the above discussed set of phases and steps, the action learning research employs some principles, which again make it unique, compared to different research approaches. One of the principles that is used by action learning is the reflexive critique evidence must be provided in the form of official documents, transcripts, and notes. This law is meant to ensure that people reflect on the processes and issues that they faced in the research in an interpretive manner as judgments are made depending on the findings.

The second principle of action learning research methodology is the critique of dialect which entails the consensual validation of the social reality (Lau & Hayward, 1997). This means that the interpretation of the fact is done through the use of language. The dialectical concept implies that a link must be established between the context and the phenomena at hand, which in turn is made up of some elements. In this case, the items that are offered attention are those that did not behave stably or which are not able to function in unison with others.

The third principle is the resource collaboration, which entails that all the researchers, must work as a team (Lau & Hayward, 1997). This implies that in research, the ideas of a single person are so significant that they cannot be ignored at all. They are therefore not viewed just as ideas but as potential resources that are helpful both to the organization and to the work of the individuals carrying out the research. It is especially useful in acquiring insightful notes that will help eliminate contradictory remarks and suggestions.

The final principle that must be applied is the one that focuses on theory, practices as well as transformations. In this regard, for the action researchers, they must aim at transforming theoretical concepts to practical things that can be helpful to organizations. Additionally, in an environment where there are theoretical assumptions that have been put in place, the theoretical knowledge existing must be advanced.

3.2 Cases of Action Learning Research Methodology

In the following paragraph, two case studies on the application of the Action learning research method for utilizing technology in the health and education sectors in the 90's, despite the lack of techniques, resources and solutions we have at the present time. However, by identifying and analysing the problem and developing appropriate and feasible solutions, remarkable results has been achieved and contributed to the future development of work in these sectors. These cases to illustrate the value of this methodology in different fields and sectors.

3.2.1 Case 1: Internet-Based Collaborative Learning Initiative for Community Health

Over a period of two years, Lau and Hayward (1997) used collaborative teams to work on an action research. They acted as instructors in a research cycle that took three phases and entailed problem-solving among a group of fifteen facilitators, health staff, and project professionals. They aimed at determining how communications over the internet can help determine the evolution of a collaborative team. Their first phase entailed requirements definition as well as the expectation towards the end of the project initiative. The second cycle involved deploying the full system, and here they evaluated the learning curve. The third and the final cycle entailed stabilizing the system as well as creating virtual groups that would work together.

3.2.2 Case 2: Conferencing in a learning society

In this case, the two researchers Fox and Comstock (1995) documented their findings while carrying out an integration of computer conferencing into a community that is currently in their middle level of learning in Seattle. In this research, they used dial-up connections to create a learning collaboration in an environment outside the classroom setting. They then assessed how this approach improved their learning experience. After they had done the assessment, they ensured that identified hiccups were identified and alternative solutions implemented.

3.3 Application of Action Learning to the thesis.

In order to start implementing the Action learning method in our scope of work as a regulatory authority to a number of UAE security agencies, it was necessary to look at few relevant examples of the implementation mechanism and case studies to ensure that this method will be suitable for enhancing and improving the audit and assessment activates for these security agencies in the area of information security. Based on the previous explanation of the methodology, an integrated model has been adopted covering all relevant stages to apply the action learning cycle that consists of four main phases as shown in the following model: Plan, Act, Reflect and lean.

Figure 5: Action Learning Cycle

It has been developed in a preliminary project plan for (10 months) and divided into different stages, taking into account the distribution of tasks and activities to the team members and ensuring the existence of relevant competencies and capabilities. During the different stages of the project, teamwork approach was effectively applied to ensure that skills and abilities of all members were fully utilized.

As for my role in this project, I have worked in different stages, starting with the preparation of the initial plan, selecting the relevant international information security standards and best

practices, developing the audit checklist and conducting the audit and assessment activities to the security agencies within the scope. In addition to that, I have conducted a comparison study among the selected standards and finalized the most applicable security controls and the checklist that applicable to the working environment.

3.4 Limitation of Findings

3.4.1 Validity

Validity refers to the extent to which the clear and logical conclusions drawn from the research results and were relevant to the key objectives, and whether these conclusions are likely to be applicable to other cases or similar situations.

Due to the similarity of the scope of application and the information security systems of government and private entities in the country, all conclusions and outcomes related to the research objectives are applicable in all entities in all different sectors. However, it is necessary for all entities to provide the necessary competencies and capabilities to implement this initiative in the ongoing audit and assessment activities of the information security systems, as the application of international standards and best practices, particularly in this area requires a set of advanced skills in technology, administration systems and security practices.

3.4.2 Reliability

Reliability refers to that if the approached used is repeated, it is possible to obtain the same results with a high level of accuracy. In our case, the reliability is very high due the common understanding of the key objective, the importance of the initiative as well as the use of the checklists that guide the audit and assessment activities.

3.4.3 Generalizability

Generalizability refers to the applicability of the findings to other context or in this case to other sectors. By considering the importance of information security, the findings of the research are most likely to be applicable to other government agencies in different sectors as well as to any private entities under similar regulatory structures.

Chapter 4: Results

The Plan and Act stages

4.1 Plan

At this stage and after identifying and highlighting the main problem and agreed on the research aim, a work plan has been developed. This plan includes studying relevant information security international standards and best practices and examining their suitability for the working environment, shortlisting the most applicable standards, defining the sub categories for the four information security domains discussed in chapter one, and finally developing a comprehensive checklist to be used in the information security audit and assessment activities.

4.2 Act

4.2.1 Producing a comparison Table of the key International Standards

In order to select the relevant security controls and develop the checklist we have analysed number of international information security standards that disused in chapter one and selected three standards due to its recognition within the region, implementation guidance, various categories of security controls and the scope of application. ASIS mostly covering the key physical security requirements and practices, while the ISO 27001:2013 and NIST special publication 800 series are more focused on information security from technical and operational perspectives.

The following table divided into three parts, the similarities, the differences and the scope of application. This in order to define the applicability level and extract relevant security controls and requirements to generate a comprehensive audit and assessment checklist.

Table 3: Information security standards comparison

S/N	Standards	Similarities
1.	ASIS ISO 27001: 2013 NIST SP800 series	1. All of them maintain security standards of IT infrastructure. 2. All of them require that organizations must maintain their certifications. 3. All of them maintain that consumer data must be protected. 4. All of them maintain that employee data must be protected. 5. Organizations must comply with the applicable security and privacy laws. 6. They require that system connections should be restricted. 7. All of them agree that network connections should only be established upon authenticating that connection. 8. All system activities must be logged and monitored to keep track of the activities that can affect the system functionality. 9. Network responsibility should be separated from other operations that are related to system operations. 10. In both of them, the responsibility of network monitoring and management should be clearly defined and established in all network operations. 11. In both of them, the process of acquiring certification is similar in that the steps that are followed are the same. 12. In both of these standards, they must define the scope of their information security management.

		13. For both of them, information being passed over a public network or wireless network should be protected through establishment of special controls. 14. Both of these standards emphasize the need for management of an organization to emphasize on coordination of security initiatives to optimize service provision. 15. All the standards focus on how to prioritize and optimize on information security of an organization.
Differences Among the Standards		
S/N	**Standards**	**Differences**
1.	ISO 27001:2013 versus ASIS	It is mandatory for ISO 27001:2013 to provide a risk assessment process as well as the remedy for all the risks identified. For ASIS, it does not require one to provide any risk identification and mitigation strategies.
2.	NIST SP800 versus ISO 27001:2013	For NIST SP800, it is not a requirement that multiple drafts be developed prior to certification. Instead, this standard advocates for a single comprehensive documents clearly outlining the security infrastructure of the organization. For the ISO 27001:2013, it is a requirement that two drafts are developed before coming up with the final documentation.
3.	ASIS versus NIST SP 800	The ASIS security standard focuses on the system security requirements especially from the authentication point of view while the NIST SP800 focuses on the security of the information systems from an overall point

		of view. In this regard, emphasis is attached on both infrastructure and infostructure.
Scope of the Standards and Application		
S/N	**Standard**	**Scope**
1.	ISO 27001:2013	a. The scope of this standard is not defined as it may be as wide as possible or may be as narrow as possible. However, they argue that scoping of the standard is very crucial. Moreover, the sole responsibility of determining the scope of this standard rests on the shoulders of top management. b. With treatment of application of this standard, the Statement of Applicability states that any approach can be used when treating risks assessment. The assessment may take the approach of a matrix form to determine the next necessary action. c. The ISO 27001:2013 is generally applied in IT governance. It is used to set out guidelines covering several information security areas such as validation of input, authentication, handling of errors as well as maintaining sessions and system logs. d. In fact ISO 27001:2013 is greatly applied in web security management for any organization. It focuses on the cyber aspect of information systems as well as the IT infrastructure.
2.	NIST SP800 series	a. The scope of this framework is more of a high-level compared to other standards. In this regard it focuses on other existing documents for more details as well as control processes. The language used is clearer therefore making it more suitable to executives to read and implement it easily

		although it has a procedure for implementation. In case of a buy-in cyber security initiative, the framework can be more useful. Finally, the framework adds functionality onto the existing framework and does not eliminate it instead. b. This a standard is applied to Federal Systems as a risk mitigation strategy. It therefore provides guidelines for mitigating against physical attacks to information systems as well as loss of crucial documents.
3.	ASIS	a. The scope of ASIS is very clear based on the fact that it is centred on a number of issues of concern to the security of information systems. In this regard, it clearly defines the security of the entire system, the security of the database systems, and that of network security. It therefore clearly defines the roles of a network administrator, the required qualifications, and the areas where it can be applied. It does the same for the database manager and the database administrator. b. It is greatly applied in management systems audits as a way of determining how resilient systems are. It is also used to audit whether systems can recover upon the striking of a catastrophe. c. It deals with the human resource aspect of information security determining whether the organization is on the verge of losing crucial information.

By understanding the characteristics of the above selected standards and comparing between the scope of application, the above table provides guidelines for what we will be selecting and identifying as key elements for the checklists, the security controls and requirements to cover

the four information security dimensions. In addition, this will assist the team to avoid any overlapping or duplication while developing and finalising the checklist.

4.2.2 Working out which elements to include in the checklist

After analysing each of the selected international information security standards and using the comparison table as a guidance, the team have decided to select the security controls and requirements based on the ease of adoption, practicality, implementation methods and the general applicability to the UAE security agencies. At this stage, the team have built a number of scenarios and situations to assess the applicability of the security controls and requirements taking in to consideration the different working averments and nature of business and the size of each security agency. Also considering the footprint and recognition of these standards helped to select and adopt the logical sequence and key elements provided in ISO and ASIS for physical, Human resource and document security controls and practices as well as the technical, operational requirements and prioritisation as per NIST SP 800 series specially for the cyber security related areas.

4.2.3 Producing the checklist.

Based on the team decision and selection of key elements from three international information security standards, the team have started to draft the checklist by listing the four main security dimension, which are; cyber security, document security, physical security, and human resource security, then the different main categories and sub- categories falls under each dimensions. After that, all relevant security controls and requirements that agreed on in the previous stage were listed under its relevant categories and sub- categories. For example: in cyber security, main category such as Network security will consist of number of sub-categories that include Access control, Firewalls, and Intrusion prevention systems (IPS). Also in Human resource security, main category such as Security clearance, Contractors/third- party employees and awareness. Each of these sub-categories will be audited and assessed by number of question that reflects the relevant security controls or security requirements; the questions have four possible answers to the security control status; yes/implemented, partially implemented, no/not implemented and not applicable. The concerned teams in the UAE security agencies must answer all questions and provide justifications for partially implemented and not applicable answers.

4.2.4 What results did we get when we applied the checklist?

By implementing the checklist during the audit and assessment activities, the responds were very positive as each agency have to follow the checklist to conduct a self- assessment that enable the auditors to understand the current information security posture if each agency based on the concerned and specialized team in each information security dimensions. All questions were answered as per the instruction given and the justification column was filled in details for the partially implemented and not applicable answers. The main outcome from this stage was to understand the current status, the applicability of the security controls and requirements as well as the readiness of the security agencies to change and adopt this approach.

The Reflect and Learn stages

4.3 Reflect

After reviewing the completed checklist and answers, the auditors asked for the relevant evidences and documentation to verify the implementation status and justifications in order to draw a conclusion on the security posture, compliance against the selected information security standards as well as to identify the gap and areas of improvements. Most of the answers were based on the individual's knowledge, experiences and their work practices while refereeing to some international standards and best practices but not in a systematic approach. In addition, we have noticed a lack in integration between the four information security domains. Also after reviewing the relevant evidences and justifications, many answers for all security dimensions were ticked without understanding the key requirements or the scope of security controls. For example, in the cyber security domain under the Network security; access controls sub-category consists of number of questions such as; do you have an access control policy? Do you review users' access rights? And do you have a privilege management system? Most of the answers were yes/Implemented, but by looking at the evidences, most of the agencies did not have a policy, which identify the scope, responsibilities, procedures and endorsed or approved by the top management. There is only set of rules that generated by the IT security department which lacks the enforcement power and the accountability statements. For the Access rights the reviewing activities where done on random basis without any clear roles and responsibilities and a proper schedule, while for the privilege management system they follow similar practices. The level of understanding for the main purpose of this checklist were varies among the agencies, as some tried to complete the checklist as part of their compliance requirements with us as a regulator, so they have answered most of the questions as partially implemented then provide unclear justifications in order to achieve an average score. Many did

not adopted for the purpose of improving and enhancing their information security practice. For example, in the physical security dimension, in different categories and sub-categories there were many not applicable answers as well, but after reviewing the justifications with the concerned team, we found out that most of these controls or requirements were applicable. But since the agency did not implement it or the security team did not understand the value of having these measures, they have provided general justification that did not reflect the current situation or why it is not applicable specially for the common security practices such gourdes operation procedures manuals, visitors protocols and ANPR (automotive number plate recognition systems)

On the other hand, the use of this approach during the audit and assessment activities helped in identifying the need for a customized security standards and a set of relevant high-level frameworks for UAE security agencies, while highlighting the benefits form operationalizing the international security standards and best practices to produce a statement of applicability and an improvement plans based on the security gap for each security dimension in each agency. After explaining the findings and producing relevant reports to the concerned top management, highlighting the key areas of improvements and the current security postures as well as the risk levels of failing to comply with the security controls and requirements. Based on the reports all security agencies have updated there answers and justifications and develop an action plan for all areas of improvements as per the directions, including the risk level, mitigation plan and action with a completion date. This plans used as reference in the follow up in the assessment that took place during the fourth quarter of the year to ensure that all comments and finding are met and the necessary actions have been take to mitigate the risk or reduce the risk levels.

4.4 Learn

4.4.1 What went well and not so well?

The outcomes of the assessment and review session have supported our key objectives of operationalizing the selected intonations information security standards and best practices, as the improvement level were remarkable and the security agencies started to implement and value the security controls effectively in order to enhance their security status and meet the compliance requirements. This is a clear indicator that the approach was valid as the implementation process went very smoothly without any complications. The use of the

checklist to guide the audit and assessment process and conducting the self- assessment lead to a high level of acceptance from the security agencies and direct the auditors to focus on all security dimensions in a systematic approach and ensuring covering all aspects of each categories and sub categories.

We have also received some feedback from the concerned teams in the security agencies on the implementation method, as we need to improve the checklist format and conduct sessions prior to the audit and assessment visit to explain in details the questions and related security controls and requirements.

4.4.2 The changes of the checklist as a result of the learning stage

In order to improve our information security audit and assessment approach, we have reviewed the implementation process, the comments and feedback received as well as the obstacles and challenges experienced by the team during the application of the checklist, reviewing the comments and finalizing the security gap and areas of improvement reports. Because of this stage, the team has agreed to apply some changes and improvement to the checklist, implementation method and the audit and assessment cycle.

First, we have faced some difficulties reading and reviewing the checklist as it was required to be filled manually by hand and signed off by the concerned management team for each security dimension. We have planned to automate the checklist and develop an electronic version with programmed formulas to calculate and analysis the results and indicates the pre-requisite for missing fields.

Secondly, for most of the categories and sub-categories of each security diminutions the security controls and requirements are interrelated and depend on the implementation of other controls or requirements, so we have reviewed all relevant questions to ensure the consistency among all controls and requirement for all security dimensions. Finally, the checklist consists of 450 questions covering the four information security diminutions in details and at some point, it involves partially in the execution level. As a regulatory body we need to provide a high level security controls and requirements only and based on the statement of the applicability for each security agencies, nature of business and work environment the proper controls will be implemented after considering the areas of improvement and risk level stated in the audit and assessment reports. Therefore, we have reviewed these questions and controls and modified them to avoid facing these issues.

4.5 Plan: the second cycle

For the next audit and assessment cycle and as part of the action learning cycle as well, the plan stage here will consist of reviewing the final audit and assessment reports for all security agencies, reviewing the findings of our assessment and review sessions and the lessoned learned from the first cycle. This will ensure that all team members are in line and ready to implement the same approach again. For the application of the checklist, the plan as mentioned in the previous section is to automate the checklist, develop an electronic version and conduct a pilot test for one of the security agency to check and validate its functionality before the formal application. The updated checklist will be communicated and discuss with all concerned teams from the security agencies in a pre-audit sessions to explain the changes, integration and pre-requisite were applicable in order to achieve a high level of understanding and acceptance. Also, a secure mechanism to be developed in order to share and transfer the electronic checklist due to its criticality and sensitivity of stating the current information security posture of the security agencies. Finally, all selected information security standards and best practices to be reviewed and checked for an updates, while considering the current information security trends in order to priorities the questions and security controls.

Chapter 5: Conclusions

5.1 Answering the research question

To answer the research question, which is "How can Information security best practice standards be operationalized into checklists for auditing and assessing UAE security agencies?"

The answer is referred to the application of action learning research methodology as discussed in the previous chapter and following each stage of the cycle and summarized as follow:

- Studying, reviewing and analysing the international information security standards and best practices based on its remarkable footprint and recognition in the area of information security.
- Defining suitable selection criteria for the relevant security controls and requirements such as: the ease of adoption, practicality, implementation methods and the general applicability to the UAE security agencies
- Defining the main categories and sub-categories under each information security diminutions.
- Generating a set of comprehensive questions that interrelated to cover the scope of the information security dimensions
- Developing a brief guidelines and relevant standards answers to control the outcomes.
- Considering the checklist as a self-assessment tools and a key input to guide the audit and assessment activities.

With the successful application of the checklist approach for the first time during the audit and assessment cycle, and based on the reports, the assessment and review sessions, the action plans developed by the security agencies, all this have clarified and verified the advantages and benefits of using the checklist approach which enabled us to operationalize different security standards and extract what suits the nature of our businesses and working environment. Also, With high commitment towards achieving our objective and following a systematic research methodology, the aim of this research is achieved and continuous improvement activities will be carried on in order to enhance the information security level in UAE security agencies.

As discussed in the chapter two, there are many important benefits for using a checklist to implement or operationalize security standards, but after we have experienced these benefits, applied the checklist approach to our case and achieved the intended objectives, it is highly recommended to use such approach while planning to implement any standards to facilitate the

process, guideline the implementers and manage the desired outcomes. In addition, the checklist should be dynamic and flexible to any changes and relevant updates while considering the consistency and the logical sequence of the questions or item. The format should be clear with a proper presentation, include a remarks/comments column with separation of different section, parts and categories. The checklist should be managed, controlled and classified as per the organization policies and its ownership should be assigned to a concerned section, department or project team. Before applying the checklist a brief guidelines should be attached with it and communicated as well to the end users. Based on our experience and as part of our improvement plan, the development of an electronic version to automate the checklist will guarantee the full utilization of its benefits and will foster the implementation process as well as the audit and assessment activities, this will be discussed in details in the following section.

5.2 Benefits of using Automated Checklist

There are many benefits and advantage using automated checklist the first advantage of these checklists is the fact that these forms can increase consistency and quality (Emily, 2015). This is made possible because these checklists are handled similarly as opposed to the manual way of filling them. This guarantee of consistency and quality together with efficiency and time saving which translates that organizations and government agencies can raise their quality of operations.

The second benefit of automating the process of filling checklists is that it saves time as they can be filled faster in systems as opposed to filling them manually (Emily, 2015). Additionally, since human beings are prone to making errors, correcting these errors takes time and therefore lowering the standards of operations. Other than the low probability of making mistakes, automation has the capacity to reduce the number of tasks to be performed. The fact that these activities of filling checklists are accomplished quite faster, then the motivation of the employees is raised.

Thirdly, automation of checklists improves operational efficiency (Emily, 2015). This is since effort, time, as well as costs, are efficiently applied to the tasks that are intended. Additionally, the effort required for the tasks at hand is minimized thereby minimizing the cost that would have otherwise been used. The reduction of errors also has a role in improving the efficiency of filling checklists because the mistakes are error-free thereby eliminating the task of counterchecking the list as well as confirming the details.

Fourthly, with automated checklists it facilitates easier governance of the tasks to be performed. Just as mentioned in another section of this research paper, the person filling the checklist can delegate the tasks of filling the checklists. When this happens, the leader of the team can monitor the progress of every person filling the checklist thereby facilitating easier and better governance.

Finally, a checklist will be beneficial when performing the delegation task. This is possible when the tasks are large and require more than one person to accomplish them. Since the size of standard requirements is high in some cases, the use of a checklist allows the users to delegate a given section of the checklist to another person and also will enable them to focus on areas that appeal to them (Emily, 2015). The challenge of this approach is that as the user, one may lose control of the information that is captured on the checklist.

5.3 Common Recommendations for government agencies

Based on the self-assessment reports, audit and assessment discussions and findings summaries, as well as after studying and reviewing leading information security standards and relevant information security statistics and reports. Most of the findings considered to be general and applicable to all government agencies, so the following common recommendations will discuss how the government agencies can raise the information security levels with reference to a number of literature, articles and relevant best practices this section

First, the government and its organizations should try to plan for an explicit authentication address (Waters, Ball, & Dudgeon, 2008). Although the element of authentication is a single element of information security, it is important that any cybersecurity initiative address some of these concerns. Secondly, all government systems are networked pervasively compared to those of the private companies (Waters, Ball, & Dudgeon, 2008). The government also relies on the third-party solutions, which are determined by the existing market trends. Despite the fact that it is important to isolate and protect government systems, they also need to ensure that their conventional technologies are protected.

Thirdly, policies that have been formulated by government agencies should be practical and realistic. According to Waters, Ball, and Dudgeon (2008), a majority of the government policies are very practical, and if implemented, they can lead to more benefits in the government. If these policies can be made practical and implemented, then more benefits are bound to arise. For instance, it might be confirmed that the government plans to implement the IEEE standard. It should, therefore, ensure that a total follow-up is followed which ensure the

discussion becomes a success should be made practical in the organization and government agency.

Fourthly, the government agencies require to benchmark with the countries that have successfully implemented a secure work plan (Puskar, 2012). Ones they have benchmarked with the right institutions, it is the role of the agency to ensure that the findings are implemented or advanced beyond their fellow agencies. Additionally, the government agencies should meet regularly to discuss the best ways of promoting best practices.

Fifthly, according to Puskar (2012), the government should use its existing pool of employees to improve the security of their information systems. This can be made possible by the government investing heavily in the youthful population in the country as well as the technical people who are passionate about information security improvement. Moreover, other than supporting the workforce to operate as expected, the government can also finance research on computer security improvement. Although this last strategy is not as fast as it would be expected, it is the most effective in that it will seek an everlasting solution to the existing problems. Other than financing the general research for improving their security, it is essential for them to find advice from professionals in the area of information security. Hiring professional consultants would somehow be expensive for them considering the nature of systems they have and the services they require, but it would be a better initiative than hiring the professionals entirely (Puskar, 2012).

Sixthly, the agencies should refrain from focusing on a single technology and outcomes. A majority of these standards recommend that more than one IT solution should be provided to solve security issues. However, even as technology is being selected, the room for interoperability must be provided. International standards require that the technology that is being developed should easily integrate with other technologies that have been developed so far. Therefore, their concern should be whether the solutions being offered to them are compatible with other existing solutions or not.

A majority of researchers argue that government information security can be boosted if the government decided to assess its information systems' security to determine whether it is the latest technology-based. Since a majority of government systems are based on legacy technology, evaluating them regularly will ensure that their problems are identified and addressed in time before being escalated.

A number of government systems and network are based on the internet and interoperate with other technologies in safeguarding information. The fact that they interoperate with other technologies is a reason for them to worry about the attacks posed by this integration.

Therefore, the government should ensure that adequately configured security tools are implemented at their boundary with the private companies. Failure to this move, there will be more cases of attacks from their interconnection of devices.

Other than investing in the young people of the country, investment in managed security services is important. These services provide a suitable option that can be used when governmental agencies do not have sufficient resources. In this case, the government agency can choose to pay for the service of storing and handling their data and information as opposed to incurring considerable costs in their attempt to boost security.

With the advancement in both the level of technology and complexity of the attackers, the government should also have a reason to worry. Puskar (2012) suggests that it would be recommended that the government adopts a different security approach other than the conventional ones. If the government chose efficient technology such as the biometrics, it is bound to secure their components and data in a better way (Puskar, 2012). Biometric can be chosen as the best approach based on the fact that no characters require being memorized by the seller as the authorization is stored in the fingerprints.

Even as these methods are being done, it is important to note that not all problems from cybersecurity can be eliminated. Therefore, all governmental agencies and the government itself can team up to provide a platform through which they will share the challenges that are facing them and at the same time offer common solution for all of them.

Finally, open source solutions are better than proprietary products although they require a large number of open source experts to be present (Waters, Ball, & Dudgeon, 2008). This is because open source solutions have their challenges at hand, which require proper addressing. Due to their ready availability, these sources are usually prone to a lot of risks although they offer an extensive and better solution. Another setback of these solutions is that they require regular patching and therefore these patches must be made available from time to time to ensure that government institutions do not suffer a security setback.

There are many leading security software products that have been implemented and are helping solve the problems that exist. The first software product is the SolarWinds RMM, which is used to remotely manage and monitor the network and software solutions that have been implemented (Vlacheas, Stavroulaki, & Demestichas, 2011). It is ranked as one of the most powerful software product providing a set of tools for network management. Some of the tools are used to maintain, secure, and improve the IT infrastructure. The solution is web-based and incorporates patches of antiviruses, web filtering tools, patch management tool, remote

access tool, monitoring, and maintenance tool as well as the remote access tool (NIST, 2013). Other than the SolarWinds RMM, there exists the Kaspersky Internet Security and Antivirus which is used both on the computer device and on the internet (Waters, Ball, & Dudgeon, 2008). The software tool has managed to obtain a high level of popularity due to its effectiveness. In this software, protection is enhanced in that users are notified of any attempts advanced by the attacker to steal data from the organizations and government agencies. On the local devices that are used, this tool enables the user to first scan devices that are connected to computer systems to ensure that malicious software is not installed in them, which can adversely affect the effectiveness of the information system

5.4 Research reflection

I have learned many things while working on completing the thesis requirements; following an academic approach and applying a scientific research methodology I have enhanced my knowledge, skills and abilities as well as other benefits the following areas:

- Improved my self-learning abilities, as being able to study and analyse different topics that not directly related to the research topic
- Enriched my knowledge and understanding of the research topic, as I have to read many articles, latest security trends and review related international best practice standards.
- Improved my analytical skills, as I have to conduct a comparative study for all key security standards and best practices and define the most relevant and applicable ones.
- Learned a new research methodology, by applying the action learning cycle in a real case scenario and identifying an important problem that need to be addressed at a strategic level.
- Teamwork approach, as this considered one of the key success factors of applying the methodology, which contributes effectively in fulfilling the research requirements.
- Literature review, as it benefits me in assessing the current status of the topic as well as understands the related previous research areas and identifies the key standards and best practices.

To conclude my experience in doing this thesis, it is very important to select the right topic after reviewing in details all the thesis requirements. Also the topic should be related to your areas of interest, linked with the course objectives and aligned with you current job role and

responsibilities as well as your academic background or specialties. This to ensure a better utilization of your knowledge and skills while trying to identify an important situation and related problem that will contribute effectively in the community and will require further research or continuous improvements.

References

Abrahams, J. (2013). Emergency risk management for health: Communicable diseases. *Journal of international health*, 1-2.

Ajit, A., & Johnson, E. (2008). *Information security and privacy standards in the healthcare: Current state of research.* Hanover: Centter for Digital strategies. 23-45.

Anderson, P., Mesic, R., & Scheiern, M. (2003). *Concepts And Definitions. In Finding and Fixing Vulnerabilities in Information Systems: The Vulnerability Assessment and Mitigation Methodology* . Santa Monica, CA; Arlington, VA; Pittsburgh, PA: RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/mr1601darpa.10.

Emily, y. (2015). *The benefits of automating audit processes.* Washington DC: Quality Digest. 5-8.

European_Commission. (2013). *Cybersecurity Strategy of the European Union: An open, safe, and secure cyberspace.* Brussels: European Commission.

Fox, S., & Comstock, D. (1995). "Computer conferencing in a learning community: opportunities and obstacles". *Journal of socio technical issues*, 17-24.

Kurt, L. (1946). "Action research in minority problems". *Journal of social issues 2*, 34-46.

Lau, F., & Hayward, R. (1997). Structuration of Internet-based collaborative work groups through action research. *http://search.ahfmr.ab.ca/tech_eval/gss.htm*, 12-34.

Martin, C., Libicki, C., Ablon, L., & Webb, T. (2015). The defender's dilemma: Charting a course towards cyber security. In *Chief Infromation Officers Surveyed* (pp. 9-21). Santa Monica, Calif: RAND Corporation.Retrieved from http://www.jstor.org/stable/10.7249/j.ctt15r3x78.10.

Maxwell, M. (2013). *The Himeland Security cyber attack preparedness.* New York: Homeland Security.

McGuinness, D. (2017). How a cyber attack transformed Estonia. *BBC News Review*, 1-4.

Melvins, J. (2013). *The OWASP ten security threats to infromation systems 2013.* Payson Arizona: OWASP.Retrieved from https://www.owasp.org/index.php/Top_10_2013-A5-Security_Misconfiguration, 13-17.

Nazario, J. (2008). Georgia DDoS attacks- Quick summary of observations. *International journal of technology*, 2-5.

NIST. (2013). *Security requirements for cryptographic modules.* California: National Institute of Standards and Technology.

Office, U. C. (2012). *Open standards principles-for software and network interoperability, data and document formats.* London: Prentice Hall.

Puskar, E. (2012). *The benefits of U.S.-European Security Standardization.* New York: National Institute of Standards and Technology.

Schimdt, L., Caolionn, O., Hirokazu, M., & Akhil, S. (2015). Cyber practices. In *What can the US Airforce learn from the commercial sector?* (pp. 33-58). New York: RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/j.ctt19rmczn.10.

Steve, P. (2014). *Standards for cyber security: European Union Network and Infroation Security Agency (ENISA).* London: Prentice Hall.

Susman, G. (1983). "Action Research: A Sociotechnical systems perspective,". *ed. Morgan*, 102-107.

Timothy, S., Helsey, R., & Baston, J. (2013). *Identifying infromation security threats.* Londond: Routledge.

Vlacheas, P., Stavroulaki, V., & Demestichas, P. (2011). *Ontology and taxonomies of resilience, ENISA report.* Mumbai: ICMA.

Waters, G., Ball, D., & Dudgeon, I. (2008). Australia and Cyber-Warfare. In *Information Warfare: Attack and Defence* (pp. 33-53). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt24h2tt.9 .

Zadelhoff, M. (2016). *The biggest cybersecurity threats are inside the company.* Washington: International Business Machines (IBM), 23-27.