DOCTOR OF PHILOSOPHY

Development of a Comprehensive Information Security System for UAE e-Government

Al Mayahi, Ibrahim Humaid

Award date:
2016

Awarding institution:
Bangor University

Development of a Comprehensive Information Security System for UAE e-Government

Ibrahim Humaid Al Mayahi

School of Computer Science

Bangor University

A thesis submitted for the degree of

Doctor of Philosophy

September 2016

Declaration and Consent

I hereby agree to deposit the following item in the digital repository maintained by Bangor University and/or in any other repository authorized for use by Bangor University.

Author Name: Ibrahim Humaid Al Mayahi.

Title: Development of Comprehensive Information Security System for UAE e-Government

Supervisor/Department: Dr. Sa'ad Mansoor/ School of Computer Science.

Funding body (if any): Ministry of Higher Education UAE.

Qualification/Degree obtained: PhD.

This item is a product of my own research endeavours and is covered by the agreement below in which the item is referred to as "the Work". It is identical in content to that deposited in the Library, subject to point 4 below.

Non-exclusive Rights Rights granted to the digital repository through this agreement are entirely non-exclusive. I am free to publish the Work in its present version or future versions elsewhere. I agree that Bangor University may electronically store, copy or translate the Work to any approved medium or format for the purpose of future preservation and accessibility. Bangor University is not under any obligation to reproduce or display the Work in the same formats or resolutions in which it was originally deposited.

Statement 1:

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree unless as agreed by the University for approved dual awards.

Signed ..... (candidate)

Date : 30 September 2016

Statement 2:

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s).

All other sources are acknowledged by footnotes and/or a bibliography.

Signed ..... (candidate)

Date : 30 September 2016

Statement 3 (bar):

I hereby give consent for my thesis, if accepted, to be available for photocopying, for inter-library loans and for electronic repositories after expiry of a bar on access.

Signed ..... (candidate)

Date : 30 September 2016

Statement 4:

I agree to deposit an electronic copy of my thesis (the Work) in the Bangor University (BU) Institutional Digital Repository, the British Library ETHOS system, and/or in any other repository authorized for use by Bangor University when the approved bar on access has been lifted.

In addition to the above I also agree to the following:

- That I am the author or have the authority of the author(s) to make this agreement and do hereby give Bangor University the right to make available the Work in the way described above.
- That the electronic copy of the Work deposited in the digital repository and covered by this agreement, is identical in content to the paper copy of the Work deposited in the Bangor University Library, subject to point 4 below.
- That I have exercised reasonable care to ensure that the Work is original and, to the best of my knowledge, does not breach any laws including those relating to defamation, libel and copyright.
- That I have, in Instances where the intellectual property of other authors or copyright holders is included in the Work, and where appropriate, gained explicit permission for the inclusion of that material in the Work, and in the electronic form of the Work as accessed through the open access digital repository, or that I have identified and removed that material for which adequate and appropriate permission has not been obtained and which will be inaccessible via the digital repository.
- That Bangor University does not hold any obligation to take legal action on behalf of the Depositor, or other rights holders, in the event of a breach of intellectual property rights, or any other right, in the material deposited.
- That I will indemnify and keep indemnified Bangor University and the National Library of Wales from and against any loss, liability, claim or damage, including without limitation any related legal fees and court costs (on a full indemnity bases), related to any breach by myself of any term of this agreement.

Signature: ..... Date : 30 September 2016

Acknowledgements

First and foremost, I owe a deep debt of gratitude to God Almighty.

I am so grateful to my wife, Hamda, who encouraged me and provided endless support all throughout my PhD when I was at my lowest. She truly was a god send and an angel.

I owe my special heartfelt devotion to my children. I hope as they grow older, they will understand my absence from their lives during this period when they needed me the most and often couldn't express in words how much I love them and missed being part of their lives.

I would like to thank all my family in the UAE, especially my sister, Huda. My gratitude of thanks to the Ministry of Higher Education for the financial support they have given me to pursue my studies and the Ministry of Interior for their unlimited support.

My sincere gratitude to University of Wales - Bangor, my supervisor Dr Sa'ad Mansoor and all my colleagues in the academic department.

Finally, it is from the deepest depth of my heart, through tears and joy that I dedicate this thesis to my departed parents (RIP), Thank you very much for everything, I hope you are proud of me and look down on me with pride. Yours prays were my main source of strength for the completion of this work.

Abstract

The UAE has a vision of delivering unified e-Government services across numerous departments of seven emirates. The primary goal is to bring all aspects of the government information services online for every citizens and business by completely replacing the existing paper-based bureaucracy. This creates significant risks and information security challenges which the UAE e-Government is seeking to address. This thesis makes a comprehensive review of the UAE e-Government's information security posture. An analysis of the current strengths and weaknesses of the e-Government was carried out, SWOT analysis was employed and based on the results, a TOWS matrix was constructed facilitating the development of new e-Government strategies to mitigate external threats. To implement an Information Security Management System (ISMS) across the e-Government departments, a framework was developed based on a multi-layered approach that is used to structure the information security program. It considers three factors; technology, operations and people (employees), to increase the effectiveness of information security system. To implement the framework, several international standards were evaluated and subsequently the ISO 27001 standard was used as a benchmark for achieving a secure e-Government. A Gap Analysis was carried out to evaluate the current state of the security culture within the e-Government against the standard and a Risk Assessment was carried out to demonstrate the existing risks faced by e-Government services. A comprehensive series of penetration tests were commissioned on e-Government network infrastructure.

Having made interventions to improve the security of physical information technologies and organisational operations, a comprehensive questionnaire was developed to obtain quantitative evaluation of the security

culture within the organisation. Subsequently, a training programme was devised and developed for the employees to demonstrably improve the security culture as measured by this approach. Finally, the findings, in conjunction with a consultation with security heads within the UAE e-Government, are used to construct a single comprehensive information security policy that can be rolled out to all e-Government departments within the seven emirates.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The United Arab Emirates (UAE) is a Gulf state consisting of seven individual Emirates. The UAE government has a vision of creating a unified e-Government information system to enable the federal government and citizens to utilise its electronic services in a safe and effective way across the whole country. The main challenge is to establish a secure and reliable ICT systems infrastructure. The UAE government has been investing substantial financial resources with the aim of creating these systems; however in creating new information systems necessarily new issues of information security will arise. This thesis takes a comprehensive look at all aspects of information security related to the emerging e-Government system and makes a number of findings and recommendations to ensure the highest standards of information security are reached.

Information security is a complex and ever challenging issue for modern organisations due to the wide variety and ever changing nature of the technologies used for

information management. Often, there is little or no standardisation or consistency, even within an organisation. Where there is no standardisation, users of different systems lack concrete methods to evaluate the security features of their systems. The result is that all too often significant security flaws and vulnerabilities in software are often discovered only after damage has already occurred. Furthermore, when writing software the software developers have no approved methods or guidelines that are prescribed in order for them to determine when they have reached the appropriate level of security necessary to minimize the possibility of vulnerabilities.

To our achieve aims we have researched the development of a comprehensive Information Security Management System (ISMS). During this process the need to adopt an effective information security standard became apparent. We first evaluated four different internationally recognised standards before ultimately selected ISO 27001 as the most appropriate for the UAE e-Government's requirements. Beyond applying the standard, it was felt there would be significant benefit in achieving formal ISO 27001 certification. The certification programme will help the UAE e-Government establish and maintain an effective ISMS. Its establishment will help reassure all users (citizens, businesses and employees) that the e-Government manages information security appropriately, as to be certified it must put in place predefined state-of-the-art processes to deal with information security threats and issues.

It's clear in the literature (1) and (2), that organisations that seek certification through a proactive approach driven by a continuous improvement strategy, are more likely to derive significant business benefits as a result. Organisations can effectively use the certification process as a means of facilitating and promoting organisational change toward achieving the highest standards of organisational culture. For ISO 27001, the process of attaining the standard can facilitate information security cul-

ture changes by making management more aware of the issues and processes that need to be in place to achieve the standard.

Certification is a powerful tool that can both be a vehicle towards and a measure of reaching the highest standards of information security practices. However, certification itself may not be sufficient for guaranteeing the overall security of an organisation's information as human factors, which may fall outside the scope of certification, can impact security. Therefore it is necessary to put in place a working culture of informational security where the recommendations and procedures recommended by the standard deeply permeate to and are reflected at all levels of the organisation's workers behaviour (3). The organisation's need for a strong culture of information security is paramount as even a well maintained state-of-the-art security technology can readily be circumvented if a single user from within the organisation, either from malicious intent or incompetence, fails to act in the appropriate manner. Lim et al (4) suggested that up to 80% of major security breaches in an organisation result from the incorrect behaviour of employees, rather than from any technical weakness in the information systems of the organisation.

Organisations cannot achieve effective information security without the establishment, implementation, and maintenance of a clear and rigorous information security policy. The formulation and utilisation of the information security policy can enhance the effectiveness of the ISMS (5). As part of this work we have uncovered that there was no standardised information security policy across all departments of the UAE e-Government thus we have developed a comprehensive policy which can be applied across all departments to ensure standardised procedures are adopted by all employees. In addition, there is a need for organisations to ensure their information security policy is structured and organised effectively (6). Establishing a policy in itself is not

sufficient to guarantee information security since it does not guarantee that individuals will comply with the policy, as a result, policy enforcement is essential. To affect a culture of strong information security awareness within the e-Government we have developed a heuristic for measuring this in e-Government employees as well as a training programme which is effective at improving employee's culture of information security awareness.

1.2 Problem Statement

All government agencies are deeply concerned with information security. The essential goal of information security is to ensure that data resources are safeguarded and to maintain the three key measures of information security comprising of confidentiality, integrity and availability of data (7). Information security is widely acknowledged to be important as it contributes not only to overall economic development but also builds the basis for effective and sustainable interactions between different economic branches.

Failure to protect this information could result in exposure to internal and external threats, risk of identity theft, or loss of confidence from its constituents, and possibly litigation. e-Government could expose the networks and systems to increasing internal and external threats, possibly making them susceptible to data breaches. Security breach can be defined as the ***theft, loss or unintended exposure of personally identifiable information that could result in the misuse or unauthorised access to personal information***. The occurrence of such incidents can compromise the integrity of government operations and result in significant asset loss and negative publicity for organisations (8).

The implementation of e-Government within developing countries continued apace over the last decade. Nevertheless e-Government services continue to face significant security challenges in application and adoption in many countries including those in the Gulf Cooperation Council (9). Cyber-attacks emerge in many different forms and although some must be launched from specific systems or networks while others require access to special accounts, they can originate from anywhere.

e-Government security threats are asserted by Karokola et al. (10) to potentially emerge from both technical and non-technical related issues. Technically-related issues include vulnerabilities arising from ineffective and weak system design, development, implementation, configuration and vertical and horizontal integration in addition to issues with maintenance. A range of non-technical security challenges may arise from issues such as a lack of managerial or administrative policies, procedural and operational guidelines, awareness programmes, cultural and ethical standards and norms, or legal and contractual agreements. However, despite high levels of investment in e-Government and associated technologies leading to rapid advancements developing countries are confronted by a range of challenges linked to both non-technical as well as technical issues. Technical concerns include a significant lack of appropriate skills and knowledge among IT human resources to support e-Government services. Potentially more significant, technological advancement has not been accompanied by progress in non-technical areas such as the cultural and people dimensions of technological systems.

The UAE government has been investing substantial financial resources with the aim of creating new secure information systems. However, in creating such systems new information security issues will arise. Bakari (11) emphasises a widening gap increasing over time between e-Government advances in implementation and service

delivery and both technical and non-technical security services. This situation is exacerbated by the rapid and fast growing sophistication of government e-Services that acknowledged to be accompanied by new security threats and risks, posing challenges for critical information infrastructure and assets in e-Government domains.

In transitioning countries such as UAE, research studies have shown that e-Government security development, have ignored factors such as organisational and national culture, in addition to levels of awareness and environment, and the relationship between these and general perceptions and beliefs about information security management (12). This underlines that with the rapid pace of e-Government development and implementation, the reinforcement of security awareness and the implementation of preventive measures in technology and management is critical. The research indicates a link between security issues, management and e-Government.

The context and issues outlined forms the motivation to undertake a holistic assessment of the e-Government security in the UAE, and develop a system which addresses the continually evolving context in both the technical and social dimensions. The central research hypothesis of this work is that in order to ensure the safe and effective deployment of its e-Government provisioning, the UAE government must implement the framework developed by this thesis which will lead to a comprehensive Information Security Management System (ISMS).

The framework developed was based on the utilisation of a defence- in-depth strategy in which a multi-layered approach is used to structure the information security program. The basic premise of this approach is to mitigate any attacks and to increase the chances that any attacks will be detected and neutralised as quickly as possible. The framework considers three factors; people, technology, and operations; understanding these is necessary to increase the effectiveness of information technology initiatives

and to protect information. Of the three elements, people are considered to be the key element to the protection of information and are the focus of this study. A successful defence in depth strategy includes security checks at each level of the organisation (13).

People: employees have a significant impact on data security; they play a large role in the success of an information security strategy within an organisation. People can pose a significant threat, whether intentional or accidental, that could cause significant risk and cost to an organisation (14). The research has shown that human factors can play a significant role in ensuring the effectiveness of information security controls. Employee negligence and error have led to significant data breaches for organisations, resulting in the loss of millions of dollars. The finding show that while some breaches are the result of malicious activity, many breaches result from employee negligence and ignorance of security policies. Although organisations create information security policies to protect information and assets, these actions can be thwarted by the lack of employee knowledge or unwillingness to follow the policies.

Kabay (15) notes that many people are uneducated in the basics of information security and that those that are knowledgeable often ignore security considerations or bypass security policies. Therefore, employee knowledge and implementation of information security concepts and procedures are integral to the protection of information and information assets. The actual adoption and use of security practices can be challenging for employees.

According to Veiga (16), employees can often develop habits that could potentially pose a threat to the security of information assets, such as sharing passwords and not reporting potential security incidents. Examples of improper use

include lack of security awareness training, mishandling of documents, and improper communication between employees. Information security countermeasures cannot be effective if employees are not aware of information security issues and trained to appropriately operate information systems. Employees can be the front line in protecting information and information assets but they can also, wittingly or unwittingly, pose a significant threat to local e-Governments. Often employee attacks or errors go undetected. Examples of user or operator errors may include accidental alteration, manipulation or destruction of programs, data files or hardware as a result of poor documentation or training (17).

Security awareness training for employees is important to minimize risks to information and information systems from internal, external, and environmental threats. To ensure effective information assurance and security, Wade (18) suggested helping employees understand their roles and responsibilities and in implementing controls and safeguards to mitigate damage if threats should occur. Thomson (19) stated that effective information security awareness training should address the different groups of employees within organisations, such as management, IT personnel, and end users. They also suggested that the training should address attitudes, behaviour and knowledge.

Technology: with the constant evolution of increasingly sophisticated technologies, as well as the growing number of threats, both internal and external, organisations must address technology as an element of their information security strategy (13). Information control systems are constantly under siege from simple to very sophisticated attacks. In addition, organisations often do not apply security updates in a timely manner and some of the solutions to information technology

problems and vulnerabilities also do not work well, exposing the organisation to additional risk.

Past literature on defence in depth strategy has focused on the use of intrusion detection software and the implementation of compensation measures to detect, mitigate and compensate for vulnerabilities that cannot be eliminated directly by information security technologies.

Overall, the use and implementation of effective technologies are essential to ensuring that organisations are capable of protecting information and information systems. The risk of both internal and external threats may require that organisations analyse their current security posture and make the technological changes necessary to mitigate threats and improve information security.

Operations: the operations element focuses on the organisation and organisational operations, including the daily activities necessary for the protection of information and assets. Identifying security policies, management, and continuity of services are key operational elements to be included in an information security strategy. Failures in operations can create human safety issues, financial losses and possible environmental damage. In addition to technology improvements, organisations often add redundancies and increase the capacity and efficiency of operations to reduce the risks associated with operations (20). While the people element is the focus of this study, the technology and operations elements are also essential to effective information security.

During the framework development process, the need to adopt an effective information security standard became apparent . We first evaluated four different internationally recognised standards before ultimately selected ISO 27001 as the

most appropriate for the UAE e-Governments requirements, beyond applying the standard, it was felt there would be significant benefits in achieving formal ISO 27001 certification.

1.3 Aims

This study aims to establish the requirements for a maximum information security management system for the UAE e-Government. Several key objectives have been formulated to address this aim:

- Develop an information security strategy for all the departments of the UAE e-Government, using SWOT and TOWS analysis.
- Evaluate international standards for information security management systems.
- Undertake a Gap Analysis of the UAE e-Government security measures.
- Perform extensive penetration testing of the e-Government environment.
- Conduct a risk assessment and identify mitigation strategies.
- Evaluate the e-Government information security culture.
- Develop a comprehensive information security policy to be adopted by the entire e-Government organisation.

1.4 Thesis Outline

This thesis has 10 chapters, it begins with the first chapter that describes the introduction of the work. Chapter 2 presents background information about e-Government

practices worldwide followed by highlighting the issues affecting the development of this initiative in the UAE. Then introduction to information security was presented in a context of development of secure e-Government. Subsequently, the literature review regarding Information Security Management System (ISMS) is discussed in Chapter 3. Different routes to implement and validate ISMS are also described. Four competing standards are introduced and a comprehensive comparison and evaluation was conducted and the decision was made to select the ISO 27001 standard as a framework for the UAE e-Government's ISMS. A certification route was chosen, to achieve this three principle components need to be completed; namely, Gap Analysis, Risk Assessment and Penetration Testing.

In Chapter 4 SWOT Analysis is applied to identify the internal strengths, weaknesses and external opportunities and threats on the UAE e-Government. Then a TOWS Matrix is used to develop strategies that utilise the e-Government strengths to take advantage of opportunities in the external environment and also to mitigate the external threats.

In Chapter 5 Gap Analysis was undertaken to evaluate the gap between the current state of the e-Government systems and the ISO 27001 standard. This process was conducted to identify the difference between the existing management procedures and those required by the international standard. Compliance analysis, maturity modelling and Management Technical Operational (MTO) model was used to establish the compliance of the four e-Government departments used as a case study.

Chapter 6 deals with Risk Assessment. Here we describe a risk assessment methodology and use it to evaluate the security risks arising from threats and vulnerabilities to UAE e-Government assets. A full risk assessment was carried out in two phases (documentation and risk determination) the results show that some assets have a high

associated level of risk and consequently mitigation measures were put in place to address these.

Chapter 7 describes a comprehensive penetration test procedure that was carried out to evaluate the UAE e-Government computer network security by simulating attacks on the network. The tests were applied to web portals and internal network systems, including routers firewalls and wireless networks. The results identify vulnerabilities and their level of impact in the event of exploitation. Recommendations were prescribed to address these.

Chapter 8 highlights a survey conducted within the e-Government organisation to address the culture of information security. In order to understand where weakness may exist, a comprehensive questionnaire was developed to sample all aspects of information security culture and produce a quantitative score for assessing the strength of each aspect. Next we devised a bespoke training programme designed to strengthen the culture of information security and carry out a controlled trial to demonstrate its effectiveness.

Then in Chapter 9 an information security policy for the UAE e-Government was developed which is to be applied across all departments ensuring a standard and consistent approach to security will be followed by all employees and allowing information to be passed across departments securely. This was developed in consultation with the heads of security at four departments as well as a review of the results from Chapter 7 to establish the current practices. The ISO 27001 standard was then used as a benchmark to produces an effective policy for the whole organisation.

Finally, Chapter 10 draws general conclusions on this study and suggests the possible direction and nature of future work.

1.5 Contribution to Published Literature

As a result of this work, the following publications have been produced:

1. AL-Mayahi.I., & Mansoor, S. (2010). ISO 27001 Gap Analysis - Case Study, Proc of The 2012 International Conference on Security and Management " World-Comp12 ", (pp. 113-117), Las Vegas, USA.

2. AL-Mayahi.I., & Mansoor, S. (2012). UAE E- Government: SWOT analysis and TOWS Matrix, Proc of IEEE ICT and Knowledge Engineering, 2012 Tenth International Conference, (pp. 201-204), Bangkok, Thailand.

3. AL-Mayahi.I., & Mansoor, S. (2013). Information Security Culture Assessment: Case Study, Proc of The Third IEEE International Conference on Information Science and Technology (ICIST 2013), (pp. 113-117), Yangzhou, Jiangsu, China.

4. AL-Mayahi.I., & Mansoor, S. (2013).Heuristics to evaluate organisational information security culture, International Conference on Advances in Social Science, Management and Human Behaviour (SMHB - 2013), (pp. 42-45),Zurich, Switzerland, 2013.

5. AL-Mayahi.I, and Mansoor S. "Information Security Policy Development", Journal of Advanced Management Science Vol(2) 2014.

And the following are invited talks through the study:

1. AL-Mayahi.I, Invited talk "Information Assurance: Case Study UAE e-Government", The Government Summit, 11 - 12 February 2012, Dubai, United Arab Emirates.

2. AL-Mayahi.I.,2013). Invited talk "Organisational Information Security Culture: Case Study UAE e-Government" Homeland Security Summit - Middle East International conference: 27-29 May 2013 Abu Dhabi, United Arab Emirates.

Chapter 2

UAE e-Government

2.1 Introduction

Information technology has enhanced every aspect of life and the way people, businesses and governments interact with each other. The rapid growth in the domain of technology has also contributed to improving government structures. Governments all around the world are incorporating the e-Government element in their strategy to cope up with the global dynamics. E-government has proved to be one of the building blocks of the current government structures. In the context of United Arab Emirates, e-Government has facilitated the governments operations and distribution structures. From the government perspective, e-Government has played a vital role in the effective synchronization of processes, leading to enhanced and fast services. The core objective of the UAE government is to enable an increased portfolio of public services, improving the delivery time and cost factors. In the traditional approach, the processes took place manually and within the office. Now, with the employment of e-Government, the citizens of UAE can avail numerous government services via online

mediums.

e-Government also refers to a communication system between individuals, private, and public agencies. Technology has improved the data processing, and played a major contribution in establishing backend structures. The concept of e-Government is contributing to the government in a broader perspective. The government can carry out operations more effectively and efficiently. Moreover, the introduction to e-Government by the government of UAE has provided improvement in the exchange of communications between the government, businesses and citizens. The aim is not limited to decreasing the cost and time of the government services, but to also providing user-friendly and easy processes for the citizens.

The e-Government is further split into four functions: e-Organisations, e-Services, e-Partnering, and e-Democracy, which serve multiple domains of the government processes. The emphasis has been on a statement "one-window, one-click or one stop government", which reflects the goal of the UAE government. To add more efficiency to the e-Government processes, the government has ensured collaborations with the best technology brands. This is ultimately providing the desired structures and coping up with the latest technology.

2.2 e-Government

Previously, the communication between the citizens, businesses or government agencies took place in government offices. The concept of e-Government was initiated after the rise of information technology and communications, as the government started to adopt technological elements in the government operations. Information technologies have supported in creating both front-end and back-end supporting systems with im-

proved data processing, but for the first stage till now mainframes are used by some organisations. In the 1980, downsized mini-computers were introduced, which were later on replaced by personal computers. These facilitated both front-end and back-end government services. Late on, in the 1990s, after the Internet era, the government agencies incorporated internet based services, leading to interactive online systems. e-Government and the internet created a strong connection between the end users (citizen) and government. In the literature, there are numerous definitions prescribed by scholars for e-Government interaction with citizens. As an example, Weihrich (21) explains the concept of e-Government by presenting his case in a broader sense. He explains that as e-Governance is linked to computer applications and the Internet, but extends to include other ICT applications, such as cellular telephone, satellite communication and geographical information systems in it's support apparatus. e-Government can either be used to execute tasks inside the government or to facilitate the public at large by expanding the reach of the government to the masses. These centres may be comprised of an unattended booth within the government agency to assist in providing the services this kiosk or booth can be close to the client.

Furthermore, personal computers, palms, smart phones can all be used to avail these services from home. It provides means through which the government can carry out its functions in an effective and transparent manner, it also enables the government to facilitate provision of greater information and improved services to the general public. It allows participation of individuals, businesses and groups within a society in order to improve the state of governance within communities or countries (22).

As shown in figure 2.1, e-Government is basically away for governments either via web-based technologies or another system enabled by ICT, to makes it easier for individuals and businesses to reach out to the government or avail the services. These

services are provided by the government for the purpose of increased participation and progress for the benefit of governments and citizenry.

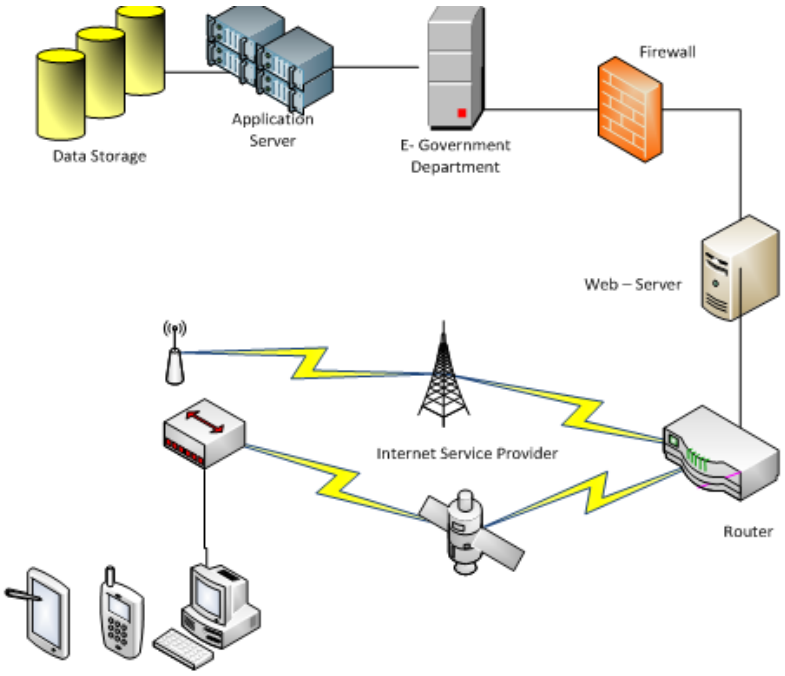

Figure 2.1: e-Government Infrastructure (Source:Abu Dhabi e-Government annual report 2014).

2.3 e-Government Services

Almost all definitions emphasise one aspect, which is the best result of using information and communication technologies to facilitate processes exchanged between the government, businesses and citizens. One of the main contributions made by e-Government is the revolution in traditional government structures, which have been renewed or reinvented. Many governments have already implemented electronic service initiatives. In the previous years the government services and functions were operated by traditional approaches, mainly manual. The communication structure among

the government, businesses, and individuals was comparatively slow. The introduction of information technology has massively replaced manual processing, and now everything has been shifted under the umbrella of information technology. The information technology revolution has enabled evolution towards more dynamic and intelligent processing techniques. It is possible to trace the desired service centres, close to the clients. They can also avail these services from their homes, using online technology. These technologies have the potential to serve a diverse range of services and deal with different ends: better relationships between citizens and their government through access to information, cost-effective delivery of government services with higher standards of quality, and better communications with business and industry. This has created the need for new method of implementation, which utilise public and internet infrastructures. Information technology has revolutionised the government structures, and has highly supported the delivery of services in all domains. The e-Government services have not only supported communication at the corporate level, but at all communications levels. From the individuals to the private sector, everyone can establish a communication network with government agencies. They can avail numerous services like taxpaying, online registrations, identity card, and various other aspects. Moreover, e-Government has established a cost and time saving structure.

Kolsaker (23) states that the aims and objectives of governments and related agencies have developed from offering public services online by means of information technology, to aspirations such as strengthening relationship between the public and the government through increased participation in processes which are critical to democracy. The literature suggests that each government which implements e-Government defines its own set of aims and objectives which are tailored to the agenda and game plan of the said governments. As a consensus, the major aims and objectives of ev-

ery e-Government revolves around the notion of enabling safe and secure usage of the internet to provide government services and required information to the general public through efficient methods of communications. These are provided in a convenient manner and support growth of e-Commerce for the benefit of the country and its businesses by providing useful information through websites and web portals. e-Government strategies globally are followed by an aspiration to advance the competence, user-friendliness and efficiency of public service delivery. The main aim of e-Government is to increase transparency between all e-Government elements and make them more user-friendly, convenient and inexpensive, these elements are described below (24):

- G2B: government to business services (external services) i.e. the front office.
- G2C: government to citizens services (external services) i.e. the front office.
- G2G: government to government services (internal services) i.e. the back office.
- G2E: Government to Employee services (internal services) i.e. the back office.

The advantages of e-Government are shown in the reciprocal exchange between government on one side with business and citizens on the other side as shown in figure 2.2.

The operation of e-Government can be characterised into two kinds of services:

- External government services, which means online service delivery to citizens (G2C) and to business (G2B).
- Internal government services, which means government to government services (G2G) and government to their employees (G2E).

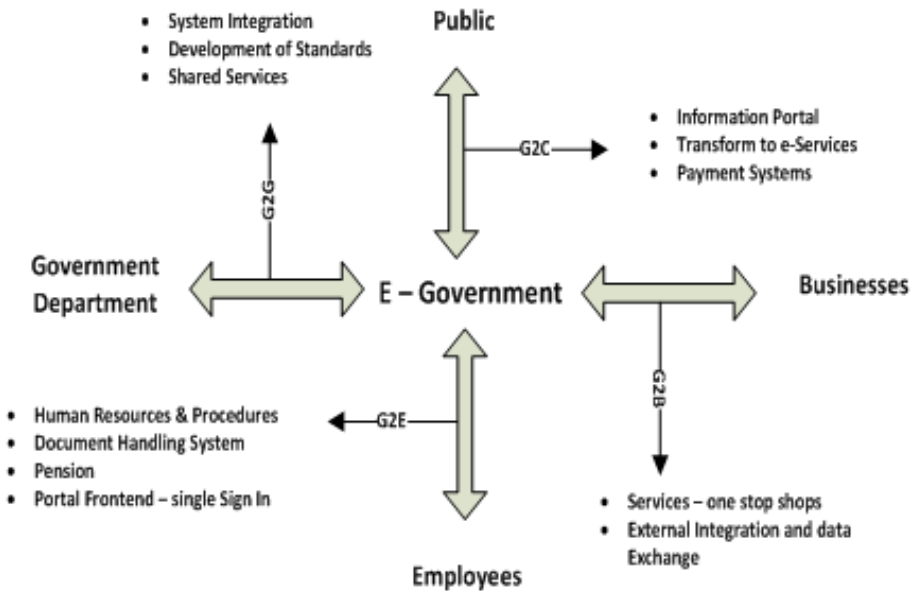

Figure 2.2: e-Government Services.

2.4 e-Government Functions

The different descriptions of e-Government can be reflected in the numerous functions incorporated in the area of e-Governance. Carrizales (25) divided the e-Government into four distinct functions:

- e-Organisation: The leading and foremost purpose of e-Government is to organize its systems electronically. This step is deemed to be the most important step towards setting up an e-Government. Through e-Organisation, the internal processes of a government such as intranets can be used to the benefit of government. It also includes using information technologies to enable communications between agencies and departments through the internet.

- e-Services: This is the second function of e-Government which involves us-

ing technology to provide efficient and effective services to the public. These services include online policy and regulation information, as well as websites allowing public to download government forms, etc. e-Services have evolved over time to provide services like online licenses, online tax payments, and complaints handling.

- e-Partnering: This function identifies various partners of the government and uses technology to strengthen their relationship and improve their efficiency through effective communications. the partners to a government are identified as public and private administrations, including industries, other metropolises, institutes, hospitals, and public and not-for-profit entities. Through this function, it is now possible to arrange online bidding and contract awards for government programmes.

- e-Democracy: The purpose of this function is to encourage citizens to contribute to government judgement or decision making processes. It is argued that e-democracy does miracles in curbing government access as it promotes greater transparency and openness. This allows the public to be well-informed and reminds governments that they are accountable in regard of their conduct. It is possible to make available budget information and voter registration forms online through the e-Democracy function of e-Government.

2.5 e-Government Development

Based on technical, organisational and managerial and feasibilities, layne (26) suggests that e-Government is an evolutionary phenomenon and therefore e-Government

initiatives should be accordingly derived and implemented. It suggests four stages of a growth model for e-Government: cataloguing, transaction, vertical integration and horizontal integration. These four stages are explained below in terms of the complexity involved and the different levels of integration.

- Cataloguing: Government creates a web-site to gain 'online presence'. The information is normally presented to citizens and usually organised into different sections. The web-site primary function consists of a search facility to answer user queries.

- Transaction: Online interfaces for the purpose of conducting transactions. These are typically characterised by direct connections to live databases that require minimal interaction from government staff.

- Vertical integration: The implementation of a seamless link between local and national databases that share a common information source, thus reducing redundancies and inconsistencies in the information stored about individual citizens. This must be accompanied by organisational and process change.

- Horizontal integration (across functions): This type of system integration means that a transaction in one agency can lead to checks against data in other functional agencies. This stage of integration will support true 'one stop shopping.

An e-Government structure that makes it possible for citizens to avail "one-window, one-click or one stop government" is one which is placed at the top slot in terms of its efficiency and effectiveness. For achieving this crowned status, e-Governments have to meet certain requirements which allow them to achieve their goals. The first and foremost requirement is the provision of understandable, accurate, and complete

information. The second requirement involves the availability of services provided by government in electronic form which can be easily accessed by each citizen and overcomes the hurdle of providing services in remote hard to reach locations. Another requirement of e-Government is to ensure the security of information provided online so as to be able to provide services to the public in tragic times akin to the terrorist attacks of 9/11 and natural disasters, such as hurricane Katrina, in which the timely response of government can either make or break the government's reputation.

2.6 Overview of the e-Government Structure of UAE

United Arab Emirates was established in the year 1971, in comparison with other countries that were established thousands of years ago, UAE seems like a new born country; but that did not hold it back, it was an encouraging factor for UAE to prove that hard working and a government hand in hand with the people can establish a powerful country in a short space of time and that is a force to be reckoned with. UAE is the third largest state in the Arabian Peninsula occupies a geographical area of 83,600 sq km (30,000 sq. mi.). The close proximity of UAE to the sea has many advantages as a strategic passage to Strait of Hormuz which is a transit route for the world's oil, petroleum and natural gas. Less than 15% of the UAE population are Emirati, from a total 8.9 million residents. Its native language is Arabic and the main religion is Islam. Dirham is the current currency. UAE is a part of the Arab world with much in common in accordance to religion, language and background. It comprise of seven Emirates; Abu Dhabi; Dubai, Sharjah, Ajman, Umm Al Quwain, Ras Al Khaimah and Fujairah as shown in figure 2.3. Four-fifths of the UAE is desert, yet it is a country of contrasting landscapes, from awe-inspiring dunes to rich oases, precipitous rocky mountains

to fertile plains.

Figure 2.3: UAE Map (Source: Ministry of Interior UAE).

UAE in many aspects is an up to date country which focuses on its ability to reduce its dependence on the oil sector, and become one of the world's most leading and fastest growing tourist destinations and a safe and welcoming environment. Educational standards are rising rapidly. Citizens and residents have taken advantage of higher education facilities throughout the country. The government aims to compete with first world countries. Such perseverance means establishing new standard in economy, education, IT, legal regulations and health care. United Arab Emirates is one of the fastest adopters of technology. In the year 1995, the internet was introduced in UAE, and since then the country has been progressing rapidly. The UAE like any other country in 2012 has noticed the increasing need and use of electronic interactions. This is due to people's awareness of technology, these days, citizens are not looking for any old service. They are looking for quality and excellence in a service, and they want to advance service delivery, build up accountability, increase the concept of transparency

and increase government efficiency.

The key emphasis of the of UAE 2021 Vision (27), is to constantly evolving ICT tools to enable the federal government entities and the public to use e-Services in a safe and effective way to achieve better delivery and good governance, bringing more competitive advantages to UAE. By establishing outstanding information and communication technology infrastructures, the UAE networks businesses together giving them a competitive edge when they interact and transact with the world. For the citizens, they will also gain the benefits of efficient inter-connections in their digital lives as well as the service from the government.

The UAE government has the prestige of having one of the highest quality broadband connections in the world. Its e-Government enables authentication of transactions through its smart ID cards issued under the initiative of the national ID program which supports secure authentication even from remote places. The federal public key infrastructure initiative by UAE e-Government increases trust by allowing identity management and privacy of data. Federated identity management ensures provision of a single sign-on service which facilitates federal and local government sectors to offer services through their websites. The UAE e-Government can increase its chances of success by enhancing the quality of life of the public through providing equal e-services to all and by investing in resource and capacity building.

2.6.1 UAE e-Government

The UAE has been at the forefront of accepting and adopting the latest technology and communication mediums, for the purpose of enhancing the government processes. The central government of the country has introduced numerous services and e-Government

programs to facilitate the citizens. These elements have been incorporated in the governmental strategies with core focus on the improvement of structures. The emphasis of the UAE government is to bring these elements in line with other countries, and comply with the international standards. This will also enhance the academic, justice and associated spheres. The e-Government programme in United Arab Emirates began when the government started to introduce technological mediums in its operations. In the year 2010 it was ranked 99th and now has moved up to 7th, which is a dramatic change and worthy of note. This is a huge accomplishment for the government of UAE. The country has jumped a big gap and taken the first position among the Arab world and GCC region. There is no doubt the government has made huge efforts to set all these standards and is now leading to the Arab world in the growth of its e-Government strategy. The government of UAE has made considerable progress towards adopting a state-of-the-art e-Government implementation.

UAE e-Government strategy is a core part of the incorporated information systems in the government organisations. These information systems have been integrated with the government organisation to form a potential structure to provide enhanced public services. The key is that e-Government is an innovative strategy which can provide with innovative outcomes. It is a well-developed program which has a list of strengths such as the establishment of sound economic strategies, political enthusiasm for the government, and a stronger academic system. Therefore the future e-Government plan of the UAE's government is to raise its rank and profile internationally. They want to make UAE a provider of government services to fully associated residents by offering the desired infrastructure to enable full communication between government units, the private sector and citizens. The principles of the UAE e-Government strategy are summarised as follows (28):

- Maintain cooperation between federal and local authorities.
- Revitalise the regulatory and policy making role of the ministries, and improve decision making mechanisms.
- Increase the efficiency of governmental bodies, and upgrade the level of services by focusing on citizen's needs.
- Develop civil service regulations and human resources, by focusing on competence, effective leadership training.
- Ministries are to manage their activities in line with public and joint policies.
- Review and upgrade legislations, policies and regulations.

2.6.2 Current States of UAE e-Government

Currently there are national websites, the country's national central portal, e-Participation portal and e-Services portal, also these are websites of the ministries (E.g. education, social service, labour, finance, health, and environment). Through these websites are tested its accessibility, described by the World Wide Web consortium under the supervision of web content accessibility guidance. Westland et al. (29) describes the notion of e-Government by giving an interesting brief about the actions of the UAE government. In early 2001, the UAE initiated the e-Dirham services proposed by the Ministry of Finance. The e-Dirham was designed to assist in collecting incomes and returns and also for delivering the administration and community with a safe and expedient payment instrument. The e-Dirham card has different versions; the first is the fixed value card which comprises of fixed value denominations ranging from Dhs 100 to 5000. The other is the government client card, proposed for those consumers e-Government

consume the government's services quite regularly. In 2005 the UAE launched UAE's first ever e-Government portal; "www.government.ae", a portal projected to syndicate all e-Services provided by both national and local administration bodies under one roof. The portal permits an increase in communication between consumers and government agents and also offers diverse services such as e-Services which allow people to contact government amenities without leaving their households, it permits them to download a link to the portal on their smart-phones and e-Participation, a survey related feature which helps in combining various social networking platforms together.

Al-Khouri (28) further provides an e-Services profile of the UAE which shows that online citizen transactions are 23%, intake processes of citizen interactions are 20% and the web presence for publishing information is 57%. In terms of e-Government services in all of the Emirates, Abu Dhabi ranks the highest and Dubai, Sharjah and Fujairah rank after it.

In the current scenario of UAE, there are around 560 e-Government services available for the citizens which can be accessed from the national portal. These e-Services were taken into consideration after analysing a range of around 3000 government services being offered by the federal, as well as the local government agencies.

The central government has allocated a huge fund of 150.35 million dirhams to be invested in the e-Government operations during the period of 2012-2014. This is another huge initiative, and an intelligent approach adopted by the government of UAE. The telecommunication authority in the UAE is solely responsible for dealing with all these operations. Additionally, the government has encouraged the local authorities to speed up the processes so that the funds can be utilised effectively. The electronic transformation strategy opted by the government of UAE will not only provide contemporary benefits, but will create a huge benefits for the coming future for the country.

The introduction of broadband services is another opportunity for its e-Government as it will support speedy connections for users and increase usage of e-Services. The UAE boasts one of the highest quality broadband connections in the world. In the global ranking, 36 countries were members with UAE captivating leading position among other nations like South Korea, which is the closest competitor at 57% of residence subscription of FTTH. The other countries close in this competition are USA, Japan, Russian and France.

Average of five indicators show the development index of telecommunication infrastructure components and those indicators are:

- Estimated number of internet users per 100 people.
- Fixed phone lines per 100 people.
- Mobile subscriptions per 100 people.
- Number of fixed internet user per 100 people.
- The number of fixed broadband facility per 100 people.

The UAE Vision 2021 goes beyond technology education. There has been the launch of 'smart classes' that will provide every student with an electronic tablet and access to high speed 4G networks and the smart learning initiative, which was launched by H.H. Sheikh Mohammed Bin Rashid, for the schools and later for the Colleges of Higher Education and Zayed University. According to the UN report in 2012 (30), the United Nations Public Administration Network conducted a detailed survey and published a report based on e-Government developments and proposed an index based on categories comprising of telecommunication infrastructure, human capital, participation and online services. The results of the United Nations survey put UAE in 28th

position in terms of the e-Government development index. With respect to the results the UN survey broke down these for Arab countries and ranked them with respect to e-Government readiness. In these results Bahrain stood on the first position, UAE on the second, Kuwait third, Jordan fourth, Saudi Arabia fifth and Qatar sixth. Interestingly apart from Jordan, all the rest of the countries are proud members of the Gulf Cooperation Council.

With respect to the general results of international countries and their readiness in terms of e-Government, it was seen that the Republic of Korea was in first position and the United States of America came second, Canada came third, United Kingdom fourth followed by Netherlands, Norway, Denmark, Australia, Spain and France, showing that nearly all of the European continent was focusing strongly on the adoption and implementation of e-Government processes.

2.7 e-Government Challenges

Fang (31) conducted an assessment of e-Government in different countries around the world. The paper stated that the benefits and strengths of e-Government are clearly visible in form of making government affordable by reducing the cost of service provision. Another achievement of e-Government is the creation of government data bases and archives which can be very valuable for decision makers which has only been possible due to e-Government. The usage of e-Government services in education has yielded great signs of efficiency and effectiveness. e-Government reduces hassles of shuttling from one government department to the other by providing a one-stop service to public and business alike. Ndou (32) states that e-Governments in developing countries have been partly unsuccessful in motivating public-private partnerships which causes

lackluster. Governments have been urged to understand the basics of IT in absence of which large IT projects undertaken by governments for setting up e-Governments will eventually fail. The opportunities available to developing countries by setting up e-Government are cost reductions and improvement in efficiency. Another set of opportunity lies in the form of increased transparency and accountability and low levels of corruption. The threat to the survival of e-Governments in developing countries comes in the form of privacy issues. Given the fragile nature of data available online, security breaches and terror attacks can be initiated in no time and damage systems and the public.

Avny (33) states that e-Government strength lies in its ability to increase efficiency and decrease cost by reducing labour expenses. It supports less reliance of public on civil servants as they avail e-services by themselves. The weakness of e-Government is that it creates distance between civil servants and public. e-Governments around the world can establish computerised administration automated centres as it will increase their chances of providing services to the people. The major threat to e-Government lies in the fact that it violates the principle of equality since not everyone is computer literate and cannot use the e-Services as a result.

Sinawong (34) attempts to explain the influencing factors, issues and challenges which lie ahead of Cambodian e-Government's "Government Administration Information System" (GAIS). He explains that the design and execution GAIS project was made possible through effective management and participation of each individual ministry, the state secretariats and the Phnom Penh municipality by working in groups. In the process of implementation, many conflicts related to design, role, technology, and participation sprang up but the management effectively resolved these conflicts. The weaknesses identified in the paper include wavering support from the leaderships for,

and a lack in prioritizing the development and up-gradation of, e-Government services in Cambodia. The opportunities which lie ahead for Cambodian e-Government include the presence of political leadership and will to a develop fully functional e-Government and an ICT policy which lays emphasis on the capacity building in terms of communication and information technology. The paper reports that according to a survey by the United Nations, Cambodia ranks very low on the readiness index, which is a major threat to effective implementation and usage of e-Government systems and services. The higher turnover rate of skilled IT staff due to inadequate pay also seems to be a major threat as the flight of skilled human resource is a grave concern for organisations as its hampers progress and reduces efficiency and requiring a lot of time in training new sets of employees which is expensive.

A survey of network readiness index carried out by multilateral agencies revealed that due to the dedication of the Jordanian government towards its e-Government programme, the promotion of ICT has been made possible and significant investment in infrastructure in the form of new telephone lines has been made. Mohammad et al. (35) identifies opportunities for the Jordanian e-Government by pointing out that a survey of households revealed a 29% increase in internet connections over the previous year and concluded that households were willing to access e-Government services and had impressive knowledge of services offered by the e-Government. A snapshot of the barriers and challenges being braved by the Jordanian e-Government has been provided by Btoush (36). The research states that there has been a lack of attention towards beefing up the security of data being made available or gathered through e-Government websites. Inadequate measures have been taken to ensure the privacy of data which can prove to be very inconvenient for government departments and the public as cyber crimes and cyber terrorism is on rise. Another threat comes in the form of

resistance on part of current employees e-Government fear losing jobs to ICT trained employees. The research highlights that the financial resources required for effective and efficient progress of e-Government in Jordan are also unavailable which is the main hindrance to setting up an e-Government. It has been found that there is very low internet penetration rate in Jordan. If internet is inaccessible to public, there is no way the country's e-Government can flourish or achieve its objectives. Another weakness hinted at by the paper is a lack of human resource specialising in ICT. There is need to invest in training programs so as to enable the workforce to undertake effective execution of the e-Government initiative in Jordan.

Rokhman (37) states that e-Government in Indonesia can flourish to unprecedented levels if the opportunity present to it in form of 45 million internet users e-Government are willing and awaiting to use its services. He states that the low global and regional ranking of of Indonesia on readiness in terms of infrastructure development and ICT skilled human resources is a major threat to its survival. Across the board, governments globally have invested significant resources developing e-Government strategies of varying levels of sophistication, while these initiatives are intended to bring in benefits such as increased responsiveness to citizens' needs, increased domestic revenue growth, and cost savings (38), (39),(40) it should be noted that it is not uncommon for these efforts to fail to yield the intended benefits. Various studies (41) and (42) indicate that the gains from developing an e-Government prove to be an "elusive dream" for many countries. Indeed, Heeks (43) carried out a study in the context of the developing world which showed a surprising 35% of e-Government initiatives were "total failures," where the initiative was either not successfully implemented or abandoned immediately on implementation. Furthermore, 50% of e-Government initiatives were considered " partial failures " due to yielding undesirable outcomes.

2.8 Conclusion

In the current era of information technology and communications, governments are investing heavily in the implementation and adoption of information technology and incorporate it into the governmental strategies. United Arab Emirates is considered as the highest investing governments in the implementation and adoption of information technology. The UAE government has a remarkable reputation and achievement in the domain of e-Government. The best practice of the government is the collaboration with top technological brands, which are a way itself to a potential e-Government structure. These aspects have improved the government processes by adding time-efficiency, cost-efficiency, and such associated factors. Moreover, the government has maintained a strong security structure for the exchange of information among the individuals, businesses and government. There is no doubt in the fact that the incorporation of information technology in the government strategy has provided with effective results. This has assisted in coping with the general global dynamics, and also contributes to various other functions of the UAE government.

The overall government processes have been shifted on information systems, and the services are being provided via innovative channels. The role of e-Government play a part in the political structure, economic development, and academic system. From the security perceptive, the government has to ensure maximum security standard, as the biggest threat of e-Government is cybercrime. Currently, this is an uncontrollable activity which has affected numerous domains, but can be dealt with effectively using powerful technological infrastructures.

Chapter 3

Information Security Systems and Standards

3.1 Introduction

Before the information age, organisations stored their most valuable physical resources in a secure location, such as a safe, organisational workers adopted a secure system and their employees were well aware of the threats to this system. With the transition to information driven economies, many significant threats to information resources now occur. With increasing numbers of frameworks and standard of information security now available in the market, choosing the right one is difficult task. This chapter provides background information and evaluation of four international standards or frameworks that deal with information security.

Information is an asset which, like other important business assets, is valuable to an organisation and consequently needs to be protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post

or by electronic means, shown on films or spoken in conversations. Information is different from data; data is the raw material for processing. Data relates to facts, events and transactions, i.e. is unprocessed information. While information is data that has been processed in such a way as to be meaningful to the person e-Government receives it. It is anything that is communicated.

Whatever form information takes, or by whatever means it is shared or stored; it should always be appropriately protected. However, there are continuous threats of information being lost, stolen, accessed (physically or otherwise), blocked or misused or destroyed by people, viruses, malwares, natural disasters (e.g. earthquake, tsunami), man-made disasters (e.g. 9/11 attacks) and sudden failures (e.g. U.S. blackout in 2003).

Thus, information security protects information and information systems. From a wide range of threats in order to ensure business continuity, minimise damage to businesses and maximise return. Information technology (IT) security is a subset of information security, and it is concerned with the security of electronic systems, including computer, voice and data networks.

Information security is the preservation of information and information systems and it can be characterised as:

(a) Confidentiality: Ensuring that information is accessible only to those authorised to have access on both a physical and logical levels.

(b) Integrity: Safeguarding the accuracy and completeness of information and processing methods, for example control for Input/output data validation.

(c) Availability: Ensuring that authorised users have access to information and associated assets when required, for example business continuity procedures.

Information security encompasses all infrastructures that facilitate its use: processes, systems, services and technology. Securing solutions from unauthorised access, unauthorised modification and denial of authorised access are achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organisation are met.

3.1.1 Security Requirements of e-Government

3.1.1.1 Importance of Security for e-Government

A specific goal of the UAE e-Government is that, by February 2014, networks and internet technologies will be integral to the delivery of government information, services and processes. To meet this goal, the UAE government is making substantial investments in putting its services online. However, security over the internet will always be a challenge. Technology will continue to improve, and practices conducted over the internet will become more secure. Security processes must be as secure as technology will allow, and the users must follow the policies set to make their own actions safe.

As a e-Governmentle, e-Government comprises of three important components:

- Online services.
- Information & Communication Technology (ICT) infrastructure.
- The literacy of end users/citizens.

Information security is relevant to the top two tiers, which are the online services and the ICT structure security. "There may well be sound reasoning for governments taking a more cautious and gradual approach than their private sector counterparts,

much of it security-related. The political risks of security breaches in government are often perceived to be far more serious than proportionally similar risks in the private sector context, a comparison most often attributed to the significantly greater holdings of personal and sensitive information" (44). Another requirement of e-Government is to ensure the security of information provided online in order to provide services to the public in tragic times and natural disasters, e.g. terrorist attacks of 9/11 and Hurricane Katrina. In these situations a timely response can either make or break governments.

The principles of information security for e-Government are defined in Figure 3.1, as discussed earlier there are three principles of security. Two are information integrity and availability. However, for government services, citizen confidentiality is the third, e.g. health records, insurance information, etc. When dealing with government services, privacy protection should be taken into consideration as a fourth principle.

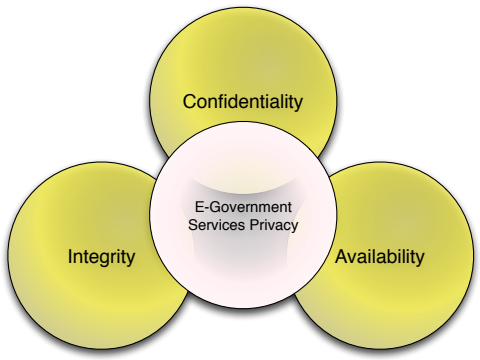

Figure 3.1: CIA Security Triad.

3.2 Information Security Management System

The information security management system (ISMS) is specifically designed for information security, and it could be utilised by an organisation to establish a robust control system for information security management. There are several definitions of ISMS. The ISO 27001 standard defined it as: 'The part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security' (45). The ISMS can be defined as: "A management system that embraces all the policies pertaining to supervision and management for the purpose of achieving the institution's objectives". The part of the management system dealing with information security is referred to as the information security management system. The ISMS specifies the instruments and methods that the management should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security (46).

No matter which definition is adopted, organisations use ISMS as a tool and a guideline to establish their information security. Organisations invest substantial amounts of money in protecting their companies from threats by using firewalls, intrusion detection systems, antiviruses, DMZ (perimeter network) and other methods. It is assumed that the security of information can be ensured by adopting these solutions. These assumptions are incorrect because security management deals with end-to-end systems. ISMS have many components including people, policies procedures, processes and technology (47). Development of information security is not an easy task. Such systems should cover components including a combination of people, hardware, software, communication devices, network and data resources that processes (for example, storing, retrieving, transforming information) data and information for a specific purpose.

Policies and procedures establish e-Government will do what, how to prevent threats, detect threats and take corrective action to combat the threat.

There should be a culture change within employees of organisation with regards to dealing with information security in general. For example, employees should not handover their password to a colleague to speed up an operation. Additionally, employees should not store sensitive information on portable devices without encryption. Every member of the organisation should be aware and accept the importance of Information Security and follows the rules described in the organisation policy.

To implement ISMS systems within an organisation guarantees all aspects of information security in the current system, as well as future developments. It is important to adopt the best practices available, and there are several well established and widely recognised standards that could be used.

3.2.1 ISMS Development Criteria

In this section, a discussion of how to measure the effectiveness of the ISMS in an organisation is presented. One major concern when developing ISMS is to identify suitable criteria for the design of the system. The following summary needs to be considered when developing such a system.

3.2.1.1 Achieve Information Security Objectives

For a management system to achieve security objectives, a clearly defined objective should be in place, and the objective of the business should be defined and supported by the top management of the business. Business requirements, such as the legislations and regulatory requirements, contractual obligations business goals and cus-

tomer expectations, should be met. The ISMS objectives should be well understood and achievable by the organisation. The objectives should also be communicated and integrated into the process and measurement system, then the achievements of all objectives should be documented periodically to ensure objectives are met. A good management system of information security can help the organisation to achieve the objectives it defines and align resources with its focus.

3.2.1.2 Identify and Mitigate the Risk

As ISMS is the system organisations use to deal with risk, all the controls and improvement will be based on the risks identified from the risk assessment process. Therefore, a good methodology of risk assessment can help the organisation to clearly and thoroughly identify the risks relevant to the organisation.

A good risk assessment methodology could be defined as (48) a method that delivers reproducible and comparable results of risk assessment. The management system should have a clear definition of the acceptable level of risk, and the organisation should take this into consideration in terms of risk, impact, the cost of implementing controls, the cost of inaction an the identified risk and the capabilities of the organisation.

It is also crucial that a follow up treatment plan contains identifiable management actions, resources for implementation controls, defined management personnel roles and responsibilities and management priorities in terms of information security risks.

3.2.1.3 Effectiveness and Efficiency in Operations

To obtain a good performance from the ISMS, measurements of operations and key index/factors should be defined and monitored. The result of the monitoring should

be evaluated against the performance requirements and feedback of the management review. Corrective action or preventive action should be in place to eliminate any discrepancy between performance and expectations.

3.2.1.4 Meets the Requirements of the Information Security Standard

The international standard of information security chosen by an organisation should reflect the common acceptance of a good management system. Therefore, being certified by information security standard is an objective way to prove that an organisation has a good management system. In order to pass the certification, an organisation is required to meet all the mandatory requirements in an information security management system, such as ISO 27001, while providing appropriate evidence of an execution record in the management system.

3.2.1.5 Fit in the Culture of an Organisation

A management system should fit in the culture of an organisation. If the management system does not fit into the culture of an organisation, it is assumed to have some integration problem, especially for management solutions. If the management system takes organisational culture into consideration and adopts a style suitable for the size, capacity, applied technology and the culture in the organisation, then this synergy can be added to the operations.

3.2.2 Components of a ISMS

An ISMS comprises several important components, which are referred to as requirements in most security standards. An organisation should fulfil all the requirements

to demonstrate compliance with the standard that leads to good management and results. According to the ISO 27001 standard (49), a management system for managing information security should contain:

- Documentation: Procedures, forms, and necessary documents to support the management of information security. Two different document categories are defined in management systems: document and record. The essential documents are: ISMS policy, objectives and scope of ISMS, required procedures for planning and operating ISMS, methodology of risk assessment, report of risk assessment and finally the treatment plan for reducing risk. The second category of documentation is the record. A record is important because it is evidence of the execution the ISMS. The record also could help the management system to improve. By evaluating the record the system can gain efficiency and effectiveness. The ISMS record can be characterised as follows: identification, storage, protection, retrieval, retention time and nature of the record. Records are required in most ISMS operations and security controls to keep the ISMS traceable and to allow control measurements to be implemented and improved.

- Awareness/training and competence: A management system relies on skilled employees to operate. Therefore, the competence and knowledge of managing information security as well as the knowledge of using and operating the management system is crucial to the successful managing of information security in an organisation. Typical skills and knowledge required are; risk management and treatment, security control, security technologies, audit knowledge and skills and training.

- Internal audit: A management system can be seen as a machine in the organisa-

tion. The internal audit plays the role of checking the machine periodically to make sure everything is on the right track. An internal audit is required for these purposes:

  - Check the compliance of the standard used;
  - Check conformance with legislation and regulation requirements;
  - Check implementation and whether operations are effective;
  - Check that the results of the ISMS operation are in line with expectations of management.

- Management review: Support from the management level of an organisation plays an important role in the operation of an ISMS. A management review provides an opportunity for management to review the operation outcomes while giving clear instructions and support to operations. The management system, beside the legal and regulatory requirements, business objectives and the requirements from the management level lead the organisation towards its business goals. Hence, a periodic management review is necessary to align the ISMS operation with the business and management objectives. During the management review, the below items should be assessed:

  - The result of the e-Governmentle ISMS operation;
  - Relevant parties feedback;
  - Resources and technologies required to improve the ISMS;
  - The result of improvement activities (for example corrective and preventive actions);
  - The result of measurement of ISMS operations;

  - The result of risk assessments;
  - Vulnerabilities of the ISMS or the organisation operations.

- Continual improvement: Continual improvement is an ongoing activity needed for the management system to improve. Corrective actions are raised and applied to the organisation when non-conformities are found. The following are required corrective actions:

  - Identify the root cause of the non-conformance;
  - Determine the action to correct the non-conformity and prevent it happening again;
  - Implement the corrective actions;
  - Review and evaluate the effectiveness of actions.

  Preventive actions are applied to the management system to prevent unwanted results or remove the potential causes for non-conformity.

3.3 Development of ISMS

A management system is characterised by its 'continual improvement cycle' or 'Deming PDCA' (plan - do - check - act) cycle, which are the key controls in all management behaviours. The PDCA cycle has proven to drive management towards continual improvement and has formalised the way people manage. By implementing the cycle, consistent results are guaranteed by checking against the defined target/objectives in the planning stage (50). The cycle shown in Figure 3.2, ends with 'action', which

means continual improvement of the management system. Corrective action and Preventive action are two actions often used in management systems. This section will introduce how to follow a PDCA cycle to establish the Information Security Management System.

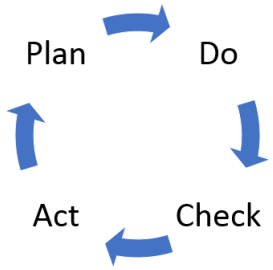

Figure 3.2: PDCA Cycle.

3.3.1 Planning Stage

During this stage of establishing the ISMS, the organisation should initially analyse the requirements, then determine the scope and the boundaries of ISMS. The characteristics of business, locations, assets, organisation structure and the technologies used by the organisation should also be considered. The policy should include the following:

- Setting of objectives and the direction of management;
- Establishing principles for information security management;
- Establishing principles for action with regard to information security;
- Establishing legislation and regulation requirements;
- Establishing contractual obligations;

- Aligning with business strategy and objectives;
- ISMS maintenance;
- Setting the criteria for risk evaluation.

The risk assessment methodology for the organisation needs to also be defined and then the risks need to be identified. These risks need to be evaluated so a risk acceptance level can be determined. A plan should be put in place to deal with these risks, and the outstanding risks of the organisation need to be evaluated.

3.3.2 Implementation (Do) Stage

The main focus of this stage will be the implementation of the previous stage's requirements, and the following actions should be carried out to achieve this:

- Define a risk treatment plan identifying appropriate management actions and resources;
- Define management responsibilities and set up the priorities for security risk reduction;
- Set the objectives for control actions and implement the risk treatment plan to achieve the objectives, including obtaining funding for the actions and the roles and responsibilities of the assignment;
- Implement all the controls in the treatment plan to achieve its objectives;
- Define the method of measuring the effectiveness of control actions and specify how to use these measurements;

- Implement relevant training and awareness requirements;
- Determine operation and resource management of ISMS;
- Security events, incidents detection and response.

3.3.3 Checking Stage

During this stage, the implementation of the ISMS is monitored, and actions need to detect possible errors in the processing of ISMS and any security breaches or incidents. The results of the execution of security activities are subsequently compared with the plan to establish their performance. Regular reviews are conducted on the ISMS effectiveness, which covers the policy and objectives, should be conducted. The results of the risk assessment, residual risks and the acceptable level of risks are reviewed. The organisation's internal auditor is required to monitor the operations of ISMS and periodically check on the system at planned intervals. The organisation's management is required to review the scope of the ISMS periodically to ensure that it is still adequate and determine whether there is room for improvement. Feedback from the findings should be added to the security plan.

3.3.4 Action Stage

During this stage, any improvement to the ISMS should be implemented. This process includes identifying the requirements then implementing them. The next step is to communicate with all relevant parties about the improvements and agree on how to proceed. Finally, the results of improvements should be reviewed and, if necessary, the plan for improvements should be reviewed to ensure the objectives of improvement actions are met.

3.4 ISMS Validation

There are three different ways to ensure that the organisation is complying with the information security standard used to implement ISMS (51):

- Internal audit: The internal audit is conducted by the organisation. For impartiality, the person or team that conducts the audit should be different to the team being audited. The result of the internal audit could be referenced by the organisation itself, but normally there is a special objective of the first party validation defined by the organisation. This method differs from the other two methods of auditing.

- External audit (customer audit): The second party audit is conducted either by the customer, buyer or the partners where the second party conducts the audit to ensure the requirements are fulfilled from their viewpoint. For example, Dell Computers send out second party auditors to the outsourcing vendors to make sure that the information security of their product or the details of production have been secured by the outsourcing vendors. For the purposes of validation, second party audits are normally more subjective, and any possible damage to the rights of the second party could be seen as non-conformity to the second party validation, though the same standard of information security is applied in the audit. Despite the subjective viewpoint, second party audits are considered efficient compared to other ways of validation because the second party tends to be subjective and leave no room for grey areas. Second party auditors also tend to have clear criteria defined by themselves under their own objectives.

- External audit, independent party audit, or third party audit: These audits are

a method of validation supported by international standards. A limitation of second party audits is that it may be necessary to send out an audit team with a different culture or language in order to understand and complete the tasks of second party's validation. The characteristics of the third party are impartiality and independence of the auditee's business. However, a weakness of the third party audit is that the auditors have the least depth of business understanding.

3.5 e-Government Information Security Management Standard Selection Criteria

There is variety of standards for information security, many developed by international organisations and adopted by worldwide organisations. It is important to make the right decision with regards to which standards to adopt in the case of e-Government. A certificate is a way of increase the confidence of citizens in UAE e-Government security management. For standard selection, if the standard can be certified and an impartial certificate obtained this can help the UAE e-Government to increase confidence in the minds of civilians. Certification will be taken into consideration where a certificate assists society in understanding that government departments have passed an internationally recognised standard which guarantees the quality of the security management. Therefore, a set of criteria was chosen to aid with the selection process, these are described in the next section.

3.5.1 Implementation

The implementation requirements will influence the choice of standard for a government agency, as there are always budget and resource limitations, but this is not the case for the UAE e-Government. In choosing a standard, four aspects must be considered for ease of implementation by UAE e-Government:

- Easy understanding of the standards.
- Guidance for implementation provided by the standard.
- The requirements of expertise in the standard.
- Resources requirements of this standard.

3.5.2 Maintenance

After implementation of the standard, maintenance is a long-term requirement. Hence, evaluating the maintenance of a standard plays an important role in selecting a proper standard. Four maintenance related aspects have been defined as:

- The resources requirements in the maintenance stage.
- The loading of maintenance stage, e.g. how many man-days should be invested to maintain the standard.
- How easily is the skill of maintenance transferred to other workers in the organisation?
- Will the requirements of standard change very often?

3.5.3 Risk Management Methodology

When selecting a security management standard, a risk assessment framework plays a key role in the discovery stage for security risks to e- Government. These organisations, which do need a good risk assessment framework to help identify the risk and the result of the risk assessment, should be reproducible and comparable. Three aspects need to be considered when choosing a risk assessment framework:

- The result should be comparable and reproducible.
- The risk assessment should at least identify threat, vulnerability, impact and likelihood parameters, which are often seen in risk assessment theories.
- Supporting material/guidance should be provided by the standard.

3.5.4 IT Security Specific Standards

The main purpose for using standards is to enhance IT security management for the UAE e-Government project; therefore, choosing an IT specific standard is crucial. The IT specific standard should address the IT security specific methodology of risk assessment and protection or controls. A pure risk assessment or quality management methodology will not have a comprehensive view or detailed view of IT security problems. Key points for evaluating the IT specific standard are:

1. Standards clearly identify the IT problems or risk.
2. Framework provides IT protection concepts, theories or controls in detail.
3. Experience of other companies or organisations about IT security are shared/included in this standard.

3.5.5 Service Process Management

As a government business can be divided into many integrated service processes, security management is required in every service processes. A good government process management should also increase customer satisfaction and increase management expectation of security (52). A standard that considers service process management architecture, which can help to instil security management into the service process architecture, should be considered.

3.6 Security Standards

This section describes the different international standards considered for implementation; four standards were considered which are described in detail below.

3.6.1 ISO 27001 Standard

The ISO 27001 was developed in 1995 as BS7799 and revised by the British Standards Institute in 2000 as BS7799 Part 1 and Part 2. Part 1 is the Code of Practice (best practice or guidance) and became ISO17799 in 2000. ISO 27001 evolved from a British government research program that surveyed the experience of the petroleum industry and other big organisations in handing the information security. The ISO 27001 standard provides a high level framework for establishing the foundation of the ISMS. It governs the management controls surrounding the design, implementation, monitoring, maintenance, continuous improvements, and the certification of the ISMS. It also measures the ability of a risk assessment to identify risk areas and provide solution to mitigate such risks (53).

3.6.1.1 Control Domains

Beside the management PDCA cycle required by ISO organisation management systems, the management responsibility, internal ISMS audits, management review of the ISMS, and ISMS improvement need to be implemented before the information security specific requirements outlined in Figure 3.3.

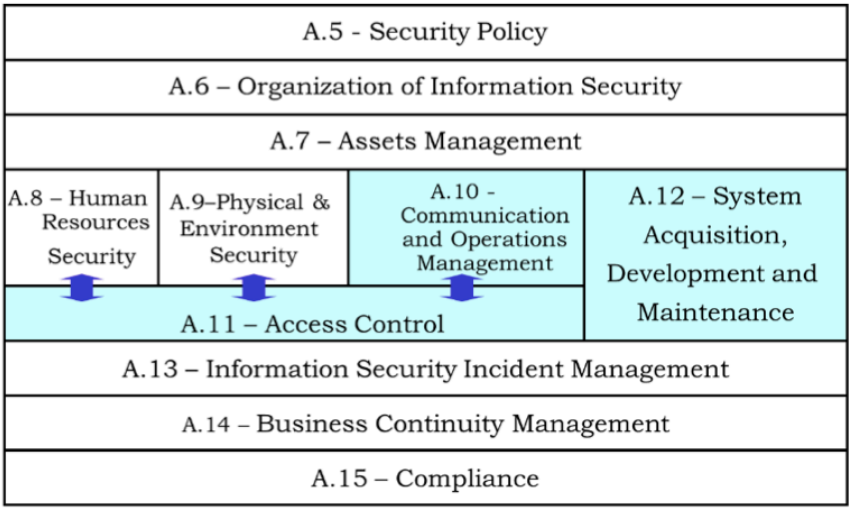

Figure 3.3: ISO 27001 Security Domains (Source: BSI ISO 27001 editor training course documentation).

The ISMS is classified into 11 domains of information security management. According to ISO Organisation (54) these are:

- A5. Security Policy: The security policy is the top tier principle for an organisation to follow, it is the core guidance for all procedures and the controls. A periodic security policy review is required by the standard to keep it updated and effective.

- A6. Organisation of Information Security: This control requires an integrated internal and external organisation, which enables effectively operations in information security management.

- A7. Asset Management: The management of information assets include the inventory of assets and the classification and labelling of assets. The purpose of the controls is to implement proper protection of the assets.

- A8. Human Resource Security: This covers the human resource security prior to employment, during employment and after employment. This enables full protection of human resource security.

- A9. Physical and Environmental Security: The security of the environment the perimeter and equipment are important aspects in security management; they are the basis for all access controls and system protection (hardware).

- A10. Operations and Communication: The IT/IS management and service room operations are crucial in maintaining the availability and integrity of information and IT systems. Backups, antivirus, communication/network policies are required, as are monitoring and change management.

- A11. Access Control: Physical, application, system (OS), and data access controls are required, as is user responsibility for access control.

- A12. Information systems acquisition, development and maintenance: This chapter defines all the requirements for information systems. Security of acquisitions, development and maintenance are all included.

- A13. Information Security Incident Management: This domain requires the reporting of the information security events, the handling of the information security incidents and the protection of evidence about the incidents.

- A14. Business Continuity Plan: Five controls are required in this domain to reinforce higher security by implementing the business continuity plan.

- A15. Compliance: Policy, regulations and other contractual obligations all require compliance; technical standards and audit technologies are also the focus here.

3.6.1.2 ISO 27001 Discussion

This section will discuss advantage and disadvantages of implementing the ISO 27001, Fenz (55) summarises the following advantages:

- It is main focus is on securing information by preserving the confidentiality, integrity and availability criteria thereof, and thereby protecting the business information assets.

- ISO 27001 is a risk conscious environment by acknowledging the security risks involved and implementing effective risk management procedures to mitigate such risks. One of the main drawbacks of the ISO 27001 is that it does not deal financial issues, corporate governance, ethical conduct, or trust issues. The standards only address information security risk management matters (56) and (57).

3.6.2 COBIT Standard

Control Objectives for Information and Related Technologies (COBIT) framework is published by the ISACA organisation and references the different information system control standards of different countries, government organisations and academies. It concludes with a series of control objectives about information and relevant technologies, to ensure that a reliable IT system is put in place (58). The IT governance institute, established in 1998, aims to advance international thinking and standards in directing and controlling an enterprise's IT.

Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT and appropriately manages IT-related risks and opportunities. IT Governance Institute (ITGI) offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

In 1996, the first version of COBIT was published and is still evolving. The 5.0 version will be published in 2012. COBIT is a framework of IT governance, which provides a management methodology by implementing objective controls to enhance the management, users, system manager, system/security auditors and reference model using the guidance provided by ITGI to assistant organisations in implementing effective IT governance. Thus, COBIT supports IT governance by providing a framework to ensure that (59):

- IT is aligned with the business.
- IT enables the business and maximises benefits.
- IT resources are used responsibly.

- IT risks are managed appropriately.

COBIT strategic alignment focuses on ensuring the linkage of business and IT plans by defining, maintaining and validating the IT value proposition and aligning IT operations with enterprise operations. It also values delivery as it executes the value proposition throughout the delivery cycle, ensuring that IT delivers the benefits promised by the strategy, concentrates on optimising costs and provides the intrinsic value.

- Resource management is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. There are key issues related to the optimisation of knowledge and infrastructure.

- Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities in the organisation.

- Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, e.g. balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

3.6.2.1 The Basic Principles of COBIT

The basic COBIT principle requires an organisation start its IT management by setting up business requirements as the goal of IT management. In order to achieve or fulfil

the goal and requirements, organisations need to invest in IT resources by using a set of structured processes and managing the IT resources. The organisation can then provide enough enterprise information to meet business requirements and achieve the organisation's goal. COBIT meets business needs in four ways: business focused, process oriented, control-based and measurement driven.

- Business focused: COBIT is provided to IT service providers, users, auditors, and the management of business and the process owner. COBIT provides business with the information required to achieve business's objectives. To satisfy business objectives, information is necessary to follow the information criteria defined by COBIT. The Information delivered to the core business process has to fulfill certain criteria such as quality, security, compliance and reliability.

- Process oriented: COBIT divides IT governance into 34 processes grouped into four domains (57). Theses domains are plan & organise, acquire & implement, deliver & support and Monitor & evaluate.

- Control-based: COBIT defines controls objectives for all 34 processes. Control is defined as the policies, processes, practices and organisational structures. Measurement driven: COBIT requires enterprise to define what level of management and control the enterprise should provide.

3.6.2.2 COBIT Discussion

This section will discuss advantage and disadvantages of implementing the COBIT framework. The main advantages as surmised by Lainhart (60) are that the cost of implementation is relatively low as COBIT is an open standard and freely available. It can easily align with other international standards. It provides strong IT control

guidelines and uniform approach to all IT areas. The main drawback to the COBIT framework is that how it deals with security matters, only one process out of 34 deals with security issues. The framework focus on which controls should be implemented without providing technical guidelines.

3.6.3 COSO Standard

The Committee of Sponsoring Organisations (COSO) defined an enterprise risk management framework. It provides a comprehensive framework and guidance on risk management and internal control and fraud deterrence. The aim is to improve organisational performance and governance and to reduce the extent of fraud in organisations (61). The main focus of COSO is on risk management to help organisations effectively identify, assess and manage risks. It is a tool for organisational risk management and an internal control and fraud deterrence system that helps a corporation manage enterprise-wide risk. COSO believes its framework fills the need of most organisations and expects it will become widely accepted by companies, organisations, stakeholders and other interested parties.

COSO was organised in 1985 to work with the National Commission on Fraudulent Financial Reporting. COSO collaborated with an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. The recommendations for public companies, their independent auditors, other regulators and educational institutions were published. COSO's goal is to provide thought leadership dealing with three interrelated subjects; enterprise risk management, internal control and fraud deterrence.

3.6.3.1 Content of COSO Frameworks

COSO defines four objectives that an enterprise has to achieve (61):

- Strategic: High-level goals, aligned and supporting with its mission.
- Operations: Effective and efficient use of its resources.
- Reporting: Reliability of reporting.
- Compliance: Compliance with applicable law and regulations.

The following eight components are key implementation controls in the COSO frameworks:

- Internal environment: this component covers, risk management philosophy, integrity & ethical values, commitments to competence, and assignments of authority and responsibility.
- Objective setting: deals with strategic/related/selected objectives and risk tolerance.
- Event identification: this component deals with event identification techniques, characterisations and distinguishing risks and opportunities.
- Risk assessment: here the risk is identified, likelihood of occurrence is established and impact
- Risk response: here the responses are evaluated and appropriate responses are chosen.
- Control activities: this component covers the policies & procedures and controls over information systems.

- Information and communication
- Monitoring: on-going monitoring activities and reporting

3.6.3.2 COSO Discussion

The main benefits of the framework are outlined below:

- It provides a completed risk assessment framework, which includes setting policy, communication and monitoring objectives, a completed framework for risk handling and risk control.
- It fits different purposes; there is no pre-defined category for this framework, so the framework might fit many different categories. This framework, not only can be applied to IT security but also to other categories of risk; hence, easier integration with other management categories is expected.
- It links to the internal control and fraud deterrence. This framework has many supports for integration with internal controls and fraud management, and those frameworks can be integrated more efficiently.

The drawbacks of the framework are highlighted below:

- For risk management only: Beside risk identification, assessing and managing, there is no specific instruction for IT security.
- Not a management system: There is no structure or requirement for a management system; it only covers the methodology of risk management, and it is not easy to use to sustain IT security.

- Not technical or security oriented: The framework evolved from fraud management and financial control practices and does not have much content or many controls for technology or IT security. From the viewpoint of IT security requirements, this framework is not specific enough.

3.6.4 ITIL

Information Technology Infrastructure Library (ITIL) is one of the most widely adopted frameworks for identifying, planning, delivering and supporting IT service in businesses. It was published between 1989 and 1995 by Her Majesty's Stationery Office in Britain on behalf of the Central Communications and Telecommunications Agency, which is now subsumed within the Office of Government Commerce (OGC). Its early use was principally confined to Britain and the Netherlands. ITIL focuses on the continual measurement and improvement of the quality of IT services delivered, from both a business and a customer perspective (62), (63). It also provides a framework following the lifecycle of IT, which starts with the IT strategy, followed by service design, service transition, service operation, and a continual service improvement process, to drive the improvement of services (64). The ITIL framework consists of the following five categories (57):

- Service Strategy: The service strategy of any service provider must be grounded upon a fundamental acknowledgment that its customers do not buy products; they buy the satisfaction of particular needs.

- Service Design: Service design is a stage within the overall service lifecycle and an important element within the business change process. The role of service design within the business change process can be defined as: the design of

appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements.

- Service Transition: The role of service transition is to put services that are required by the business into operational use. Service transition delivers this by receiving the service design package from the service design stage and delivering every necessary element required for ongoing operation and support of that service into the operational stage. If business circumstances, assumptions or requirements have changed since the design stage, then modifications may well be required during the service transition stage in order to deliver the required service.

- Service Operation: The purpose of service operation is to deliver agreed levels of service to users and customers, and to manage the applications, technology and infrastructure that support delivery of the services. It is only during this stage of the lifecycle that services actually deliver value to the business, and it is the responsibility of service operation staff to ensure that this value is delivered.

- Continual Service Improvement (CSI): Concerned with maintaining value for customers through the continual evaluation and improvement of the quality of services and the overall maturity of the ITSM service lifecycle and underlying processes. CSI combines principles, practices and methods from quality management, change management and capability improvement, and it works to improve each stage in the service lifecycle, as well as current services, processes, and related activities and technology.

3.6.4.1 ITIL Discussion

ITIL advocates that IT services must align to the needs of the business and underpin core business processes. The benefits of implementing ITIL include:

- Provides a good starting point for improving service management processes.
- Improves business productivity levels due to the delivery of higher quality IT services, resulting in improved decision making processes, business profits and revenues.
- Reduces incident handling times.
- Improves customer satisfaction and customer relationships.
- Highlight the importance of creating business value, rather than simply just executing processes.

The drawbacks of the framework are highlighted below:

- ITIL V3.0 has five books and each is more than 400 pages long, totally more than 2000 pages. This is a detailed dictionary of IT service management guidance, which is a useful reference during implementation. It is not a framework; therefore, the upper-tier framework of IT service management should be included.
- Although IT security topics are covered in the framework however, ITIL focuses on IT services instead of the IT security or information security.

Table 3.1: Evaluation of Security Standard

Criterion	Score	COSO	ISO 27001	ITIL	COBIT
Implementation the system	0-very difficult to implement (self), 10-very easy to implement	3	9	3	4
Maintenance of the system	0-very difficult to maintain (self), 10-very easy to maintain	10	5	3	4
Risk management methodology	0-none, 3-partial, 5-completely	5	5	0	3
IT security specific standard	0-non-it, 3-partial, 5-IT security specific	0	5	2	3
Service process management	0-not included, 3-partial, 5-completely	0	3	5	5
Management system	0-non-mgmt system, 5-mgmt system	0	5	0	2
Support Guidance (e.g implementation)	0-no supporting guidance, 3-partial, 5-completed supporting	2	5	3	5
Risk assessment	0-not covered, 5-completely covered	5	5	0	2
Vulnerability management/guidance	0-not covered, 5-completely covered	2	5	2	3
Technical protection	0-not covered, 5-completely covered	1	3	3	3
Human resource security	0-not covered, 5-completely covered	0	3	3	3
Data/information management	0-not covered, 5-completely covered	0	3	3	3
Physical protections	0-not covered, 5-completely covered	0	3	3	3
Measurement/evaluation	0-no measurement, 5-with completed measurement in the standard	3	3	3	5
Audit scheme	0-no audit scheme provided, 5-audit scheme provided	0	5	0	5
Recognition of the standard	1-industrial standard, 3-national standard, 5-international standard	2	5	0	0
		33	72	33	35

3.7 Evaluation of Standards

To evaluate the standards presented in section 3.6, a survey was conducted and sent to consultants and specialists in the area of information security. The result of the survey is shown in table 3.1, which show that ISO 27001 scored the highest and as a result it was chosen to be used as standards to implement the ISMS for the UAE e-Government. Figure 3.4, shows the landscape and overviews of the frameworks of security management system used. It is obvious that ISO 27001 standard offer certification and it is IT specific standard which is important to enhance the e-Government security.

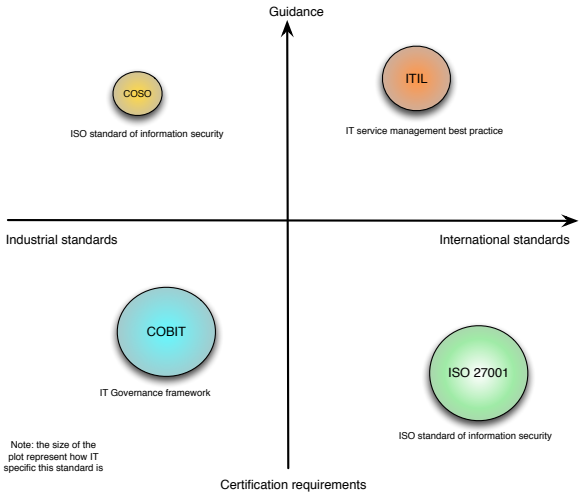

Figure 3.4: Overview Security Standards Framework.

3.8 Conclusion

Information security is not limited to technical issues; it is the management of problems. While there has been a number of standards in the area of organisational security and how it should be selected, most only focus on certain aspects of security and not

on how these aspects should be taken in to consideration within the entire framework of the organisation's culture.

Four standards or frameworks about information security are evaluated in this chapter. The study outlined the requirements of a government organisation, i.e the UAE e-Government, evaluated the standards based on these requirements to and finds the best standard to implement.

Although all the standards or frameworks evaluated in this chapter are IT or information security relevant, these standards or frameworks could be classified by positioning the nature or the purpose of the standard; these may include framework for management and their requirements and best practice/guidance.

After the evaluation, it is possible to conclude that COSO is a framework for enterprise risk management that meets the highest tier requirements in our study. Organisations could use it as a top tier framework to build the structure of information security in an organisation.

COBIT could be the second highest tier in the management, as it helps organisations to define the objectives of information security management, and those objectives could be the goals of security control implementation.

ISO 27001 can be positioned in the middle tier of security management, representing the requirement and minimum requirements of a good information security management. ISO 27001, including 11 domains, 34 control objectives (which could be mapped to COBIT objectives) and 133 controls, is based on past experiences of information security management. In the study and the evaluation of the standards, ISO 27001 has the highest quantitative value, and best meets the requirements of the UAE e-Government. The reason it is a good fit for the requirements could be its right tier and right detail level. The implementation of certification standard ISO 27001 will

help UAE e-Government win the trust of citizens and customers.

ITIL is the lowest tier in security management. It provides the most detailed guidance on IT management and can be used when people would like to know how to implement a control. The conclusion of this evaluation is that the best fit UAE e-Government requirement is ISO 27001.

Chapter 4

SWOT and TOWS Analysis

4.1 Introduction

The development of the e-Government initiative is facing challenges that need to be addressed in order to achieve its objectives. This chapter highlights the issues affecting the development of e-Government initiative and evaluates the current status of UAE's e-Government department with an eye to the future. The SWOT analysis is a tool used to analyse the various aspects essential to penetrate in the market, and can assist it to improve the strategies and cater the gap accordingly. It was applied to identify the internal strengths, weaknesses and external opportunities and threats on UAE e-Government. Based on the results of SWOT analysis, a TOWS Matrix was constructed to develop strategies that use the e-Government strengths to take advantages of opportunities in the external environment and also to mitigate the external threats.

4.2 SWOT Analysis

The aim of SWOT analysis is to identify the strengths, weaknesses, opportunities, and threats related to any organisation, or government considering this scenario. The identifications of these elements can lead to the development of effective strategies. The government can identify the strengths, cope up with the weaknesses and explore opportunities. These strengths and weaknesses have internal associations, whereas the opportunities and threat have external association (65).

Mansar (66) presented a paper on the impact of e-Government in UAE. In the review, she published her views on the impact of the e-Government practices on businesses all over the United Arab Emirates. Moreover, in the article she suggested a number of risks inherent in the implementation of the e-Government practices. These risks included the: the degree of user involvement in the systems, the commitment to be fulfilled from the levels of the government, the proper maintenance of the information systems, specifically the websites associated with government agencies. The reason for identifying the risk in the articles was the confidential or sensitive data present on the online platforms, which can be subject to various security threats. In this regard, the government can implement various laws and regulations that can effectively deal with this matter.

Anvy (33) addressed the problems encountered in the administration of e-Government, specifically in the scenario of the 21st century. As per the analysis, e-Governance provides with enormous strength to the government, as it simplifies the operational processes, and makes them more efficient (synchronised). The concept of e-Government has been threatened by numerous socio-cultural deficiencies. Many of these issues are associated with the incongruity among the fast paced technological advancements tak-

ing palce globally (67). In this article, a consultation process was carried out on each of the four components, considering all the e-Government departments, which led to the following outcomes:

4.2.1 Strengths

Strengths are associated with internal factors in any organisation or business, (i.e. the e-Government in this research). These strengths can be used effectively to achieve the core objectives of the UAE Government.

1- The programs dedicated for the e-Government development have a strong leadership structure, and have the involvement of high profile individuals. This is an essential element for coordinating the adoption of e-services, in all the sectors. The most essential factor is the support from the government, in terms of funds, which are also available for the recruitment of the foreign consultants.

2- e-Government operations are part of the daily activities of both individuals and businesses. The citizens use the online government portals for numerous activities on a daily basis. A strength is the availability of around 560 e-Government services, thought out the nation for the citizens of UAE. The selection of these e-services was made from more than 3000 government services, including the federal, as well as local government entities.

3- The services under the e-Government assist in abolishing bureaucracy, which provides a better communication structure between citizens and the federal government of the UAE. The best feature of the e-Government is in reduced paper work and high dependence on certain entities. Around 8000 shipping consignments are catered daily by e-Government in Dubai customs.

4- The e-Government structure in UAE has been incorporated using the latest technologies. From the software perspective, the technologies include open source software that reduces the security threat, and is also supported by powerful information systems and databases.

4.2.2 Weaknesses

In the context of internal limitations and errors, weaknesses have been highlighted:

1- The adoption of e-Government can result in cultural resistance within the government departments, like adopting information security practices. Surveys conducted in the year 2010 and 2011 identified the challenges which might take place in making the government employees follow the proper guidelines.

2- The lack of standardisation and consistency among different service providers.

3- It is difficult to join all the sectors and create a single effective technology structure.

4- Needs for business continuity system to be in place.

5- A single big data centre with a centralised approach.

6- The integration of dissimilar legacy services and systems in place into a single repository.

4.2.3 Opportunities

Opportunities are factors that exist in the external environment.

1- The UAE government operates with a futuristic approach, and a broad vision. The internet has high penetration and this has a high impact on e-Government processes.

2- The strong economic position of the UAE provides it with financial security. The government of the country is highly supportive and has invested huge funds in development projects. The federal government allocated around 150 million dirham for the e-Government and communication structures.

3- The youth of the UAE takes part in the advancement of the e-Government and the human capital in the country is highly skilled, educated, and aware of the importance of technology.

4- The government of UAE has always encouraged its citizens in learning to utilise internet services, which has led to the high adaptation rate of social media and e-Commerce.

5- There is high acceptance of new technologies like smart phones, automated devices, etc.

6- The dedication and strong support from the government and political leadership is an opportunity in itself.

4.2.4 Threats

Threats are referred to as un-favourable circumstances that exist in the external environment:

1- One of the major threats to any e-Government structure are cyber-attacks. The consistent denial of service, and other such associated threats can weaken the systems.

2- Other elements that represents a serious threat are social engineering, legal exploitations, and phishing attacks.

3- The introduction of e-Government can lead to the rise in cyber related crimes, including the credit card fraud and other serious crimes

4.3 TOWS Matrix

The TOWS matrix is a conceptual framework that combines the external factors and those internal to the enterprise, and develops strategies based on these variables (21). There are four types of strategy:

- SO strategy (Maxi - Maxi) - maximize e-Government strengths by taking advantage of external opportunities.
- WO (Mini - Maxi) strategy-is aimed to minimize the weaknesses by taking advantage of external opportunities.
- ST strategy (Maxi - Mini) -use the e-Government strengths to avoid or reduce the impact of external threats.
- WT strategy (Mini - Mini)-are defensive tactics directed at reducing internal weaknesses and avoiding external threats.

The result of the TOWS matrix for the UAE e-Government is presented below, which summaries the strategies and course of action required to achieve the e-Government mission.

4.3.1 Strength and Opportunity

1. Citizen centred strategy: The Government has introduced Vision 2021, an educational plan that focuses on enhancing technological understanding and operation.

For example the smart learning initiative, this was launched by H.H. Sheilh Mohammed Bin Rashid, for schools and later for the Colleges of Higher Education and Zayed University. These educational programmes will encourage citizens to use e-Government services in UAE.

2. The strong e-Government leadership and its high calibre individuals can utilise a forward-thinking government to propose and implement futuristic solutions that will leverage advanced ICT infrastructure and will fit the needs of the loyal highly skilled young population.

3. As the UAE economy is stable and has many multinational organisations, it can design a programme for or give incentives to ICT, specialist from around the world to consider. The UAE is a profitable area to live in, and has many job opportunities for internationals which could be used to train current local employees.

4.3.2 Strength and Threads

1. The establishment of a computer network security and privacy protection unit with protects e-Government services from a broad range of possible cyber-attacks.

2. The implementation of information security standards such as ISO will assist in the implementation of best practices.

3. Protecting the database of the critical national infrastructure.

4. Many government departments are collaborating with the private sector to be the channel, through their outlets, for those e-Government cannot use, or would rather not use, the available e-Services.

5. The strength measured up against these on-going threats would be the well skilled and experienced young info sec professionals in the government. The degree of their experience will lower the probability of an attack taking places.

4.3.3 Weaknesses and Opportunities

1. The young educated population is ready to adopt a sophisticated system of e-Government and adopt a culture of best practice regarding information security policies that will ensure the widespread uptake of e-Government and e-Payment systems.

2. Utilise highly skilled ICT sector to employ the latest theory of user interface design and web technologies and develop user friendly web and mobile services.

3. Development of employee awareness strategies, within each organisation.

4. Human-machine interface strategy, to improve the e-Services user interface.

4.3.4 Weaknesses and Threats

1. Increase the utilisation and ease of use of e-Government systems for elderly and foreign workers.

2. This can be attained by providing a government mediator service that will manage the e-Government system on behalf of residents at designated kiosks. This approach can assist in minimising the threats.

3. Integration of many different security technologies in a single government platform will provide a multi layered security approach which it will make it more difficult for an attack to take place.

4.4 Conclusion

The best way to maintain the e-Government structure is to implement continuous evaluation and monitoring systems, which can effectively deal with the internal and external environment dynamics. The UAE government has granted permission to the government agencies having a control access on the resources. It will increase the level and communication and collaboration among different government agencies.

The result of the analysis shows that UAE e-Government departments are lacking a comprehensive information security framework and policy for exchange of information between departments and citizens that are using the services. A successful implementation of e-Government requires a continuous evaluation, as the external and internal environments are dynamic, some factor changes dramatically overtime while others experience little changes.

Chapter 5

Gap Analysis

5.1 Introduction

This chapter describes the initial step toward developing information security management system for the UAE e-Government. To achieve this goal it was decided to obtain the ISO 27001 certification, which is the leading standard of information security. Gap Analysis was performed to determine the status of the organisation against the ISO 27001 standard, and to identify the weaknesses in the existing system. The analysis highlights the potential risks associated with the UAE e-Government. A Management, Technical and Operational (MTO) model is also presented. This model gives greater focus and provides a framework, which is more aligned to the organisational structure and responsibilities.

Information security is critical for today's organisations; global exposure to threats means that they must protect themselves from external and internal threats. Wiander (68) describes the importance of building an information security management system based on ISO 17799 standards. The study concludes that there was internal

resistance to change and this was due to lack of information available to the employees within the organisation. Valdevit et al. (69) show that there is growing interest from SMEs to be ISO 27001 certified in order to improve their IT security, and to achieve this, a suitable Gap Analysis tool was developed. In his paper, Dey (47) describes the development of an information security system, and shows that there should be proper analysis and design, involving the entire organisation, starting from the senior management down to the end users. The conclusion was that they should all take appropriate roles in the establishment and implementation of an information security system within the organisation. Technology solutions need to be implemented appropriately to fight against threats and risks, or to automate certain processes. Policies and procedures need to be established in order to define e-Government will do what, when and how, in order to prevent the threats. A detection mechanism is required and once a thread is detected, corrective measures will be taken to fix any damages.

Gap Analysis is widely used in many fields, as a way of finding out the gap between the current status and a specific standard or requirement. Applying a Gap Analysis to an information security management systems means finding out the difference between the actual performance of security management in an organisation and the requirements of the ISO 27001 standard in our case. There are many reasons why Gap Analyses might be conducted by an organisation; for organisations that would like to adopt and be certified by the ISO 27001 standard, it normally plays a role in finding out the distance to be covered before certification by ISO 27001 would be possible. When the distance is understood, organisations can therefore make a plan of improvement to achieve their goal of getting certified by ISMS (70).

Gap Analysis can help organisations to understand their position in the market as evaluated by means of information security management, and then consider the direc-

tion of their market, product or service strategies. No matter the purpose for doing the analysis, the results will lead to the positioning of the organisation, finding out the improvement requirements, and finding out the differences between current practices and the specific standards or requirements. In other words, Gap Analysis helps organisations to realise the difference between "where we are" and "where we want to be". Compliance is the process of comparing the applied controls of an organisation with those in ISO 27001 in this case.

There should also be a cultural change within the organisation, to deal with information and its security in general. The concept of an e-Government is to provide access to government services to the public and private sector (citizens and businesses) at any time over open networks. This leads to issues of security and privacy in the management of the information systems. To develop a secure e-Government system, the organisations involved are required to have an ISMS. The reason behind developing the ISMS for the UAE e-Government was a strategic decision agreed by the management board, to meet the following organisational requirements:

- The desire to meet various regularity requirements, particularly around computer misuse, data protection and personal privacy.
- The desire to manage information more effectively for each organisation within the e-Government.

5.2 Gap Analysis / ISO 27001

Most organisations, in order to ensure compliance with the various regulations and corporate governance rules around securing key information, adopt the ISO 27001

standard. The objectives of the standard itself is to provide a model for establishing, implementing, operating, monitoring, reviewing and maintaining the information system, based on a business risk approach. The compliance assessments evaluate 133 controls of the requirements that are designed to achieve the 39 objectives of the standard, within 11 key domains (54). The objective of this work is to prepare the groundwork for the development of the ISMS for the UAE e-Government.

For those using Gap Analysis as a benchmarking tool, the timing is flexible or should be on demand. Organisations pursuing a certification for an ISMS perform Gap Analyses within two different timings with different purposes, as shown in Figure 5.1.

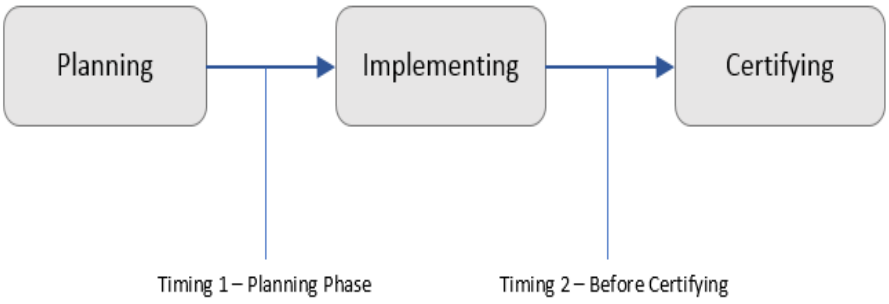

Figure 5.1: Gap Analysis Activities.

Initially during the planning stage and before the start of the implementation, the analysis is conducted to help the organisation to understand the requirements of the standard and compare it to the existing security controls. This reveals the gap, meaning the difference that should be implemented in the implementation stage. This is done by an internal team and is led by a qualified auditor (71).

The second timing for Gap Analysis is normally before the certification audit process; the function of this is similar to a mock test of the certification. Sometime also

called a Preliminary Audit (Pre-audit), this kind of Gap Analysis helps organisations understand if they could pass the Certification Audit and achieve certification for the ISMS. Following this Gap Analysis, the organisations make corrective actions to their management systems and then accept the final audit of the ISMS.

5.3 Gap Analysis Implementation

There are many different ways of implementing Gap Analyses. Basically, the components of the analysis include a standard or a specific requirement set, which define the objectives of the Gap Analysis, and a methodology which defines the processes of evaluation against the objectives. Meanwhile, the quality control of a Gap Analysis defines the process of getting a reliable and reproducible results. Figure 5.2 shows these activities.

The first step is to define the standard or requirements target; this is used by the evaluator to check the organisation's actual performance and generate the analysis report. Normally an international standard or industrial standard fulfils this role; in some case, customer requirements, government regulations/requirements or organisation management requirements can be the standard to define the objectives of the Gap Analysis. When the report is released, the standard used to check the actual performance will also be included as part of the report, to clearly convey the meaning of the results of analysis.

The second step is to select an evaluation team, procedures and objectives. The evaluator e-Government conducts the check is usually chosen to be impartial, and the qualification of evaluators should be considered when selecting evaluators.

The procedure of Gap Analysis is important; procedure should define the method-

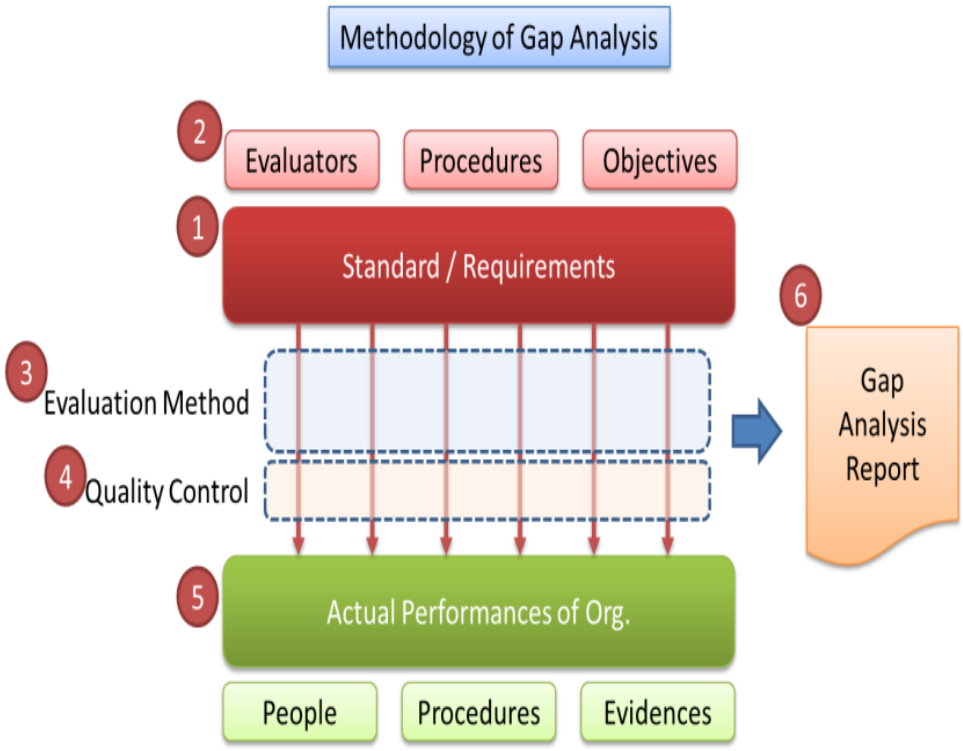

Figure 5.2: Gap Analysis Activities (Source: BSI ISO 27001 editor training course documentation).

ology used, the evaluation activities, sample rules, and the schedule/time requirement of the Gap Analysis. The procedure should also contain all the steps and activities to complete the analysis. Sometimes procedures also defines the reporting format and the items that should be included in the report.

The evaluation method could be defined in the procedure of the analysis or defined separately; there are many types of evaluation, e.g. qualitative or quantitative, and different methods lead to different results or understandings. A formal procedure commonly includes a checklist, which includes all the items and should be checked during the Gap Analysis. The checklist also contains the methods that both parties agreed and that met the objectives of the analysis. For the Gap Analysis of the UAE

e-Government, a quantitative method was chosen in terms of quantity of compliance; choosing an appropriate method plays a key role in the success of a Gap Analysis. Experienced teams or evaluators can contribute to appropriate methods used in Gap Analysis activities. Further considerations of methodology also include the culture of the organisations and the reality of the organisation management processes. The analysis should also include the technologies used in evaluation, e.g. computerised evaluation or remote evaluation, videoconference interviews, etc. Due to the nature of information security management, in which most data and evidence is stored computer systems, the different methods or technologies chosen to evaluate an ISMS system will result in different resolutions of evaluation and precision of the results.

Finally, analysis reports are very important and are used in decision-making, especially in the implementation plans, which influence the investment in people or resources. Also, in some customer-required Gap Analyses, the result could lead to purchasing decisions. No matter from which viewpoint, the quality of the Gap Analysis process should be emphasised from the beginning of the analysis. The quality control section defines the quality that the Gap Analysis activities should maintain, from the people quality and the process quality, to the report quality.

5.4 The UAE e-Government Gap Analysis Case Study

This Gap Analysis should be performed widely enough to cover all departments that could represent the UAE e-Government security control current status. Therefore, this process could be involved with many different departments and different processes. Defining a methodology before performing the analysis could facilitate the implementation of Gap Analysis, and help both the evaluator and the UAE e-Government's rel-

evant departments understand the method of implementing Gap Analysis and the criteria and the judgements of the result. Furthermore, the methodology should maintain consistency and guarantee reproducibility of results.

In order to meet the requirements of the UAE e-Government and the requirements of Gap Analysis, the methodology should contain at least the items listed below:

1. Define the scope of the analysis: the methodology should clearly define the scope of the analysis process, which should adequately represent the result of the target of analysis;

2. Determine the method of conducting the analysis: for example, the sampling rule of analysis, interviewing people and reviewing documents, or on-site/off-site;

3. Evaluation of the results: the methods by which the evaluator interprets the findings and how the final results are presented or classified.

Four different organisations within the UAE e-Government were used as case studies. All these organisations manage and operate their own information security, which implies that they are running an implicit information security management system without a systematic risk assessment according to ISO 27001. The gap assessment was initially carried out on the information that had been shared with section managers on a sample basis. Sample cases were taken in each of the areas to check their compliance to the standard. The next step was to assess the compliance of all the sections within the chosen departments. This was achieved by interviewing the relevant managers and their teams to obtain a clear picture of the business, reproducible results and consistency, together with the review of documentary evidence, in order to verify the compliance level. Table 5.1 Shows the list of the 11 key areas and the people responsible for each one.

Table 5.1: List of Interviewees for each Domain

Domain	Interviewee
A-5 Security Policy	Director & All Teams
A-6 Organisation of Information Security	Head of Electronic Audit
A-7 Asset Management	Head of Quality Management
A-8 Human Resources Security	Head of Network & Operations
A-9 Physical and Environmental Security	Head of Cyber Crimes Section
A-10 Communication and Operation Management	Local Branch
A-11 Access Control	Head of Information Security
A-12 Information System Acquisition, Development and Maintenance	Consultant
A-13 Information Security Incident Management	Database Specialist
A-14 Business Continuity Management	Management Team
A-15 Compliance	Management Team

The interviewee also included H. E. Salem Khamis Al Shair Al Suwaidi, the Telecommunications Regulatory Authority (TRA)'s Deputy Director General for Information and e-Government Sector. He leads the team responsible for developing the UAE federal e-Government, to provide all the federal government services electronically. Senior managers were selected for the survey as they are key practitioners responsible for a variety of security domains within the organisation and therefore have extensive experience and knowledge of e-Government security, challenges and issues.

A list of questions was used to establish the maturity level and to capture the compliance of the organisation to different scenarios. The questions were designed using the ISO 27001 standard controls. Each staff member was interviewed individually, and answered the questions related to their domain which are listed in detail in Appendix A.

5.5 Management, Technical and Operational (MTO) Model

The ISO 27001 eleven security domains do not provide insight into which group in the organisation is responsible for the activities associated with each domain. Thus, as part of this research, a model based on the organisation's structure was developed (72) . This model provides greater focus and a better understanding of where the organisational responsibility lies for each domain. The security domains are grouped into three categories based on organisational responsibility:

1. Management Controls, which include the following domains: A-5 Security Policy, A-6 Organisation of Information Security, and A-15 Compliance;

2. Technical Controls, which include the following domains: A-7 Asset Management, A-9 Physical and Environmental Security, and A-10 Communications & Operations Management;

3. Operational Controls, which include the following domains: A-12 Information Security Acquisition, Development & Maintenance, A-11 Access Control, Information Security Incident Management, and A-14 Business Continuity Management.

This model provides a common language for all to view and manage information security activities. It could be considered as a framework for measuring and monitoring performance and integrating better management practices, which are more aligned to traditional organisational structure and responsibilities.

5.6 Maturity Model

The concept of maturity models is regularly being applied within the field of Information Systems as an approach for organisational assessment. Any systematic framework for carrying out benchmarking and performance improvement, if it has a continuous improvement processes, can be considered a maturity model. Generally, in the constituent literature, maturity implies a perfect or explicitly defined, managed, measured and controlled system (73),(17),(74). It is also a progression in the demonstration of a specific ability, or in the accomplishment of a target, from an initial to a desired end stage.

There are common mature modules available, these being: NIST, CITI-ISEM, COBIT, SSE/CM and CERT/CSO. All of these have between 5-6 levels of maturity; for the purpose of this study it was decided to use the COBIT model, because it is focus toward auditing specific procedures, awareness and adaptation (75). The COBIT maturity model is an IT governance tool used to measure how well the management processes are developed with respect to internal controls. Such capabilities can be exploited by auditors to help management fulfil their IT governance responsibilities.

A fundamental feature of the model is that it allows the organisation to measure its current maturity level against a specific standard, in this case ISO 27001. As a result, the organisation can discover practical improvements to the internal controls of an IT system. The maturity levels are not goals; rather they are a means to evaluate the adequacy of the internal controls with respect to the e-Government business objectives. The model focuses on auditing specific procedures. This definition of maturity has several important characteristics:

1. It provides the blueprint for a complete security program;

2. It informs the management of the order in which to implement security elements;

3. It leads toward the use of best practice standards.

This approach toward a detailed security maturity model (Security Program Maturity Model) takes a management systems approach. It involves the existence or non-existence of the eleven controls (domains). A list of questions was used to establish the maturity level for each of the eleven controls, and these were intended to capture the compliance of the organisation in different scenarios.

The maturity values are determined according to the security requirements of the organisation. During implementation, two issues needed to be addressed regarding the questions and their maturity values. This was resolved by designing the questions using the ISO 27001 standard controls and carefully determining and agreeing on their maturity values (weight). Below is the list of agreed maturity values and their description:

1. Nonexistence (value 0): there is no recognition of the need for internal control;

2. Ad-hoc (value 1): there is some recognition of the need for internal control;

3. Reputable but initiative (value 2): controls are in place but are not documented;

4. Defined (value 3): controls are in place and are adequately documented;

5. Managed and measurable (value 4): there is an effective internal control and risk management environment;

6. Optimised (value 5): An organisation-wide risk and control program provides continuous and effective control and risk issues resolution.

To establish the organisation's initial maturity benchmark, the relevant staff were contacted from the four departments. They were then interviewed individually, and answered the questions related to their domain.

5.7 Results and Analysis

5.7.1 Gap Analysis Results

To assess the current levels of compliance of the e-Government department that was used as case study against the principle of code of practice. The results of the analysis have been categorised using the following definitions:

1. Compliant: The organisation and process operations are fully compliant with the specific area of ISO 27001;

2. Partially compliant: The organisation and process operations has gone some way to being compliant, but still requires additional work to be undertaken;

3. Non-compliant: The organisation and process operations do not have the controls in place to satisfy the requirements of ISO 27001.

The results shown in Figure 5.3 indicate that some of the controls are more developed than others; it is evidence that control A-5 show 100% non-compliance. This is due to the nonexistence of an approved security policy. In A-6 Security Organisation, and A-7 Asset Management, the high ratio of non-compliance indicates that the operations in security organisation and asset management in the UAE have high deviation levels from the international best practice in security management, and once again this is due to the lack of implementation of an effective security policy within these

two controls. The lack of policies will affect the other controls by increasing their non-compliant response. Therefore, the first recommendation to improve the organisations' ISMS is to write comprehensive security policies (this is described in detail in Chapter 9).

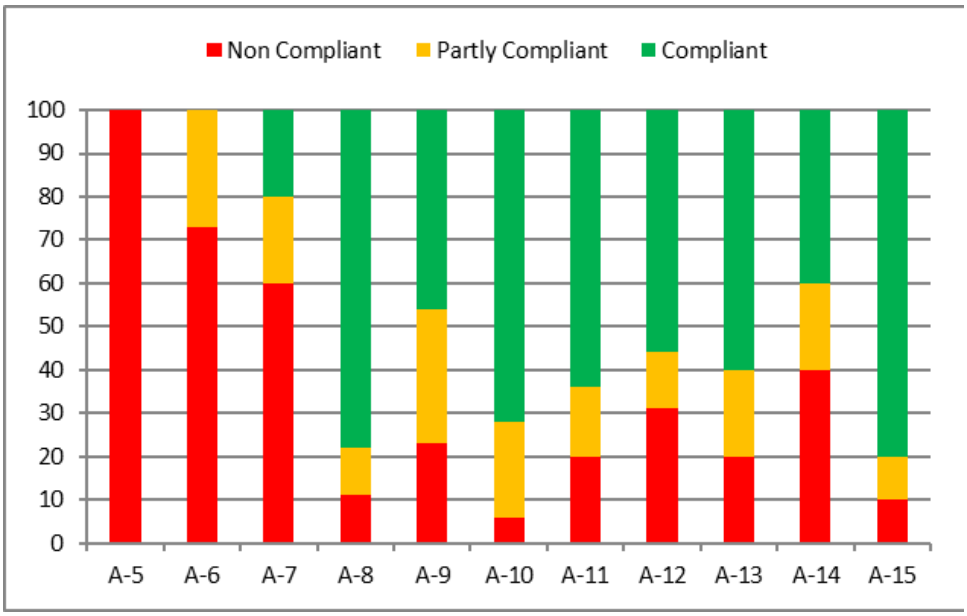

Figure 5.3: Gap Analysis Compliance Levels.

The lowest gap in compliance falls on A-10 Communication and Operation Management; this gap indicates that the communication and operations of the UAE e-Government project is the closest one to the international information security standard. Therefore, this gap diagram, suggests that the information security management in the UAE e-Government are good in operations but not up to standard in those management domains. The rest of the controls seem to have a higher percentage of compliance and this is due to internal security procedures being put in place by the teams responsible for each section.

Table 5.2, shows the compliance levels for all the 133 requirement controls for the

Table 5.2: Compliance Score

Domain	Req.	Compliant	Partly Compliant	Non-Compliant
A-5 Security Policy	2	0	0	2
A-6 Organisation of Information Security	11	0	3	8
A-7 Asset Management	5	1	1	3
A-8 Human Resources Security	9	7	1	1
A-9 Physical and Environmental Security	13	6	4	3
A-10 Communications & Operation Management	32	23	7	2
A-11 Access Control	25	16	4	5
A-12 Information Security Acquisition, Development and Management	16	9	3	5
A-13 Information Security Incident Management	5	3	1	1
A-14 Business Continuity Management	5	2	1	2
A-15 Compliance	10	8	1	1
Total	**133**	**75**	**25**	**33**

organisation, and it can be seen that:

1. 56.4% of the controls that were reviewed were found out to be compliant with ISO 27001 standard;

2. 18.8% of the controls that were reviewed were found out to be partly compliant with ISO 27001 standard;

3. 24.8% of the controls that were reviewed were found out to be non-compliant with ISO 27001 standard.

This indicates that the organisation has a large number of controls that meet the standard required. Bearing in mind that this was the first attempt to test the organisation's compliance, this is quite an encouraging outcome.

5.7.2 MTO Model Analysis

The next analysis carried out was to identify the compliance of each section of the organisation based on the MTO model. The model categorises the information security management domains into three major categories: management, technical and operations. The results are shown in Figure 5.4; it is clear that management shows more than 60% of non-compliance. From here, it is easy to conclude that, where management is concerned, the UAE e-Government protection controls are not even close to being in the right track, as required by the ISO 27001 standard. This is primarily due to the lack of an information security policy. Meanwhile the technical and operations sectors have higher percentages of compliance and this is due to internal security measures put in place internally. The technical domain shows around 32% non-compliance, while the operations sector shows 22% non-compliance. Both domains are better fit to the standard than the management domain. The result shows that improvements should be emphasised on management's part rather than on operations' part, and once again this is related to non-availability of comprehensive information security policy.

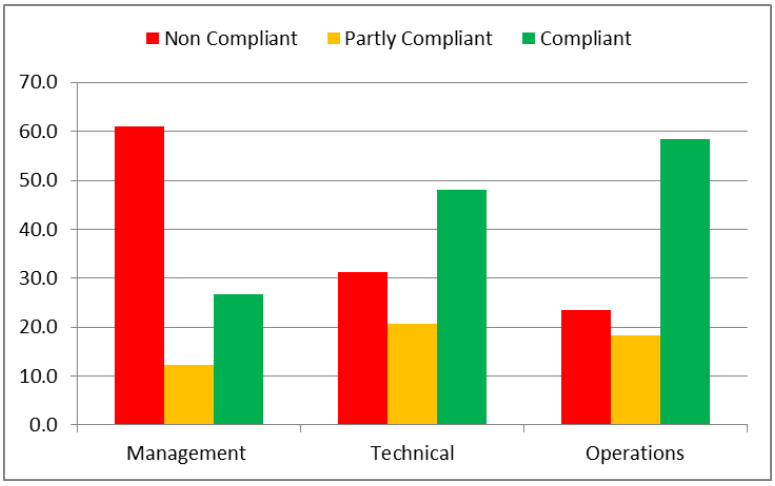

Figure 5.4: MTO Model Results.

5.7.3 Maturity Model Assessment

The next analysis carried out was to identify the compliance of each section of the organisation based on the MTO model. This was conducted by interviewing the manager of each section; a list of questions was used to establish the maturity level for each of the eleven controls, and they were intended to capture the compliance of the organisation to different scenarios. Table 5.3 shows a detailed explanation of the scores used for benchmarking against the ISO 27001 standard.

Table 5.3: Maturity Score

Maturity Rating	Description
Score < 33%	The organisation should start implementation of overall security measures
Score 34% - 65%	The organisation has taken significant steps to enhance security
Score > 66%	The organisation fulfils defined measures, thus the probability of high risks is marginal

The maturity benchmarking against ISO 27001 is shown in Figure 5.5; at a glance, it clearly shows that the average maturity is low, around 35.5%. It is obvious that some of the controls are more mature than others; for example, the Compliance, Communications, Human Resources, Security, and Asset Management scores lie between 34% - 63%. This implies that work has been done to improve the security of the organisation but that further improvement is required. In the meantime, there are some controls lying in the region below 33%, which implies that the operation is dependent

on knowledge and motivation of individuals, and that many control weaknesses exist and are not adequately addressed.

Employees may not be aware of their responsibilities. Action is required to improve the security of these controls. The results demonstrate the need for development of comprehensive information security policy (control A-5 with maturity of 18%) and also the need to develop information security incident management (control A-13 with maturity of 24%). There is rule of thumb that management system requirements equate to maturity level 3, and this gap analysis concluded that in its current state, the UAE e-Government will fail in the ISO 27001 management system certification.

Figure 5.5: Gap Analysis Maturity Results.

5.8 Control A-13 Information Security Incident Management

A management system is a method that an organisation chooses to operate, in order to achieve the business goal. During operations, some mistakes or errors in the system or personnel management could cause unexpected deviations; these could be referred to as information security incidents. An incident is something sudden and unpredicted; therefore, resilience in handling an information security incident will be the key management issue beyond the procedure expectation. Organisations should develop security incident management, which is important not only to the management system itself, and to the objectives of the organisation, but is also important to the national security and government stability. The incident management system is a tool for organising pre-identified resources to respond to an emergency or disaster. It is useful when employees and resources from the e-Government organisation are required to manage incidents successfully (76).

It is essential to establish the type of incident management system put in place to deal with information security in the UAE e-Government. To achieve this, further study during Gap Analysis was conducted into the A-13 control (Information Security Incident Management), to ensure a consistent and effective approach was applied to the management of information security incidents. The study was conducted by interviewing the senior management in the department for information security and checking the security reports within the department for the previous three-month period. The findings are shown on Tables 5.4 and 5.5, which compile the findings and recommendations based on the ISO 27001 standards.

For the e-Government incident management as a whole, most requirements of ISO

Table 5.4: Findings within the Planning Phase of the Handling of Security Incidents

Safeguard	Implementation	Comments
Establishment of a management system for handling security incidents	Partly implemented	There is no written security incident management system in place. Only for network-related events, the e-Government employees are following internal not documented procedures.
Specification of responsibilities for dealing with security incidents	Partly implemented	Responsibilities for dealing with security incidents are documented in the job description and approved by the manager for most e-Government employees.
Procedural rules and reporting channels for security incidents	Partly implemented	There is no written policy including procedural rules and reporting channels for security incidents. There is a standard procedure, in which the person on duty informs the security engineer and, in case of a security incident, informs the Manager in charge.
Escalation strategy for security incidents	Partly implemented	There is no written policy including the escalation strategy for security incidents. It is the decision of the Manager in charge to inform the head of the department. The head of the department can inform the general on the incident.
Specifying priorities for handling security incidents	Partly implemented	There is no written policy including priorities for the handling of security incidents. The priorities that e-Government employees work with are derived from the handbooks of the systems they work with (e.g. CISCO MARS). Security incidents are then reported to the management where a decision on further action is made.

Table 5.5: Findings within the Operational Phase of the Handling of Security Incidents

Safeguard	Implementation	Comments
Investigation and assessment of a security incident	Partly implemented	There is no written policy that describes actions for the investigation and assessment of any security incident that is detected. The course taken depends on the management decision and the skill of the security engineer.
Remedial actions in connection with security incidents	Partly implemented	There is no written policy documenting remedial actions in connection with security incidents. All actions are discussed in the meeting with the security engineer and the manager in charge, and a decision is taken.
Notification of parties affected	Partly implemented	There is no written policy specifying parties that have to be informed of a security event of a specific type. The parties that were contacted will be identified in the meeting with security engineer and management.
Evaluation of security incidents	Partly implemented	There is no written policy outlining the evaluation of security incidents. The evaluation should be done by a skilled engineer with specialist knowledge of the system.
Use of detection measures for security incidents	Partly implemented	There is no written policy focusing on measuring and improving the effectiveness of the management system for the handling of security incidents. There are monthly reports that are generated from the responsible security engineer and sent to the management. There is no proof that the management approves these reports.

27001 in planning and operation stages are not completely implemented. From the top of the management system, policy is not clearly defined and documented. Job descriptions and important procedures are not implemented.

The handling of information security incidents is not mature, lacking a documented procedure, although there are monthly reports. Therefore, the effectiveness of the incident handling and the improvement of the management system in incident handling are below the requirements of the international standard.

5.9 Conclusion

An information security management system is an integral part of the organisation management, required to monitor, review and improve the information security of the organisation. It is a continuous process that deals with security policy development, and puts procedures in place to deal with security threats. The Gap Analysis is initially used to identify the weaknesses in the organisation's procedures. This should be a continuous process, as the organisation is required to reassessed to update the Gap Analysis. This is carried out to ensure long-term protection against security breaches.

The results could help an organisation to know the direction of improvements and make decisions on the allocation and prioritisation of resources. In our case study, management is the weakest domain when it comes to compliance with ISO 27001, while maturity level analysis demonstrates a clear direction in the maturity of protection controls, which clearly indicates the priorities and directions to which the UAE e-Government should pay attention and improve.

The security levels that can be achieved through technical means are limited, and should be supported by appropriate policies and procedures. The identification of

which controls should be in place requires careful planning and attention to details. Information security management requires, as a minimum, participation by all stockholders, including employees, suppliers, third parties and other external parties.

Gap Analysis is an important tool for the implementation of information security management systems. This study uses a case study to show the effectiveness of Gap Analysis, by interpreting the results of the UAE e-Government. In the initial stage, it helped to find the gap between its security levels and the ISO 27001 best practices for information security. The first thing that should be defined in the methodology is the scope of analysis and the standard to be compared against for the evaluation. In our case study, ISO 27001 was chosen as the standard, and the A-5 to A-15 control domains were selected to be evaluated.

Based on the purposes of analysis, a methodology is composed by integrating different methods of analysis. In this case, we used compliance level, MTO Model (also compliance level) and maturity model in the methodology to gain different Gap Analysis results in different aspects.

Chapter 6

Risk Assessment

6.1 Introduction

Having completed the Gap Analysis in the previous chapter, the next stage was to carry out a risk assessment in order to understand the existing and possible risks to the UAE e-Government's information security. Having evaluated the risk we are then able to recommend a series of mitigation measures to manage the risk to the organisation. Performing risk management enables the e-Government to accomplish its objectives of securing the IT systems that store, process, or transmit information, enabling well-informed risk management decisions and assisting in authorising IT systems (77).

An organisation's assets are harnessed by an organisation in order to drive it forward towards fulfilling its objectives. As information systems have transitioned from paper based system to digital information systems, the types and nature of threats to information security have changed and grown substantially (78). Information technologies have become key assets in modern organisations, supporting, controlling, and managing business processes. However as highly as they are valued, these assets are

also often the most vulnerable. As the cyber economy has emerged, it has accelerated these developments, redefining markets, organisational scope, the sources of knowledge and creativity, business logic, and resource criticality (79).

Within paper based information system information system assets were tangible, with threats readily perceived, and the location of information well understood. With digital system's information ubiquity brings new challenges in managing and restricting access to information. Specifically, the growth of information assets has introduced several new management problems requiring new policies, technologies and organisational capabilities (80),(81).

Despite the lack of tangibility, or perhaps because of it, it's increasingly important to insure that the true cost of protecting digital information systems is well understood and met by an organisation. Correctly evaluating these costs necessarily requires deeply understanding the threats and vulnerabilities to the organisation's information systems (82). There are many overheads associated with fully protecting an information systems assets and it is important that these are fully recognised. Implementing the protection creates a diversion of resources from alternative applications. In addition, many tools and procedures used to protect information assets also reduce the throughputs, access and transparency as well as creating new complexities and inflexibilities in resource utilisation. Solutions are often temporary and less than perfect against emerging threats (7).

Despite the inherent cost associated protecting digital systems, no protection can be perfect without crippling the system such that it is no longer useful. For this reasons organisations need to find a balance between the cost and benefits of protecting a system, to do this the organisation need to fully understand the risks. Risk is the possibility of occurrence of an event that would result in the damage to the e-Government

systems and credibility. The technology applied to implement information systems also creates risks; information disclosure, compromising the principle of information confidentiality; inappropriately modification, information integrity is compromised; finally, the information could be lost or destroyed, compromising the availability of information principle (83). The assessment of risks to an asset depends on factors such as the nature & value of the asset, the purpose for which it is used, the environment in which the asset is set and the protection provided by the controls already in place. Within the organisation, there are a number of standard events that should trigger the risk management process. This could be the initiation of a new project, system or business process (84), the discovery of new threats or vulnerabilities, or changes to the asset inventory or operational procedures. In addition a periodic assessment of existing assets should be carried out in conjunction with a risk assessment. The relationship between different risks management concepts are shown in the figure 6.1. The most important relationships are described below (85):

- Threats exploit vulnerabilities of assets, while vulnerabilities in assets increase security risks.
- Assets have values and an associated potential impact.
- Security risks indicate security requirements that are met by introducing security controls.
- Security controls protect assets against threats.

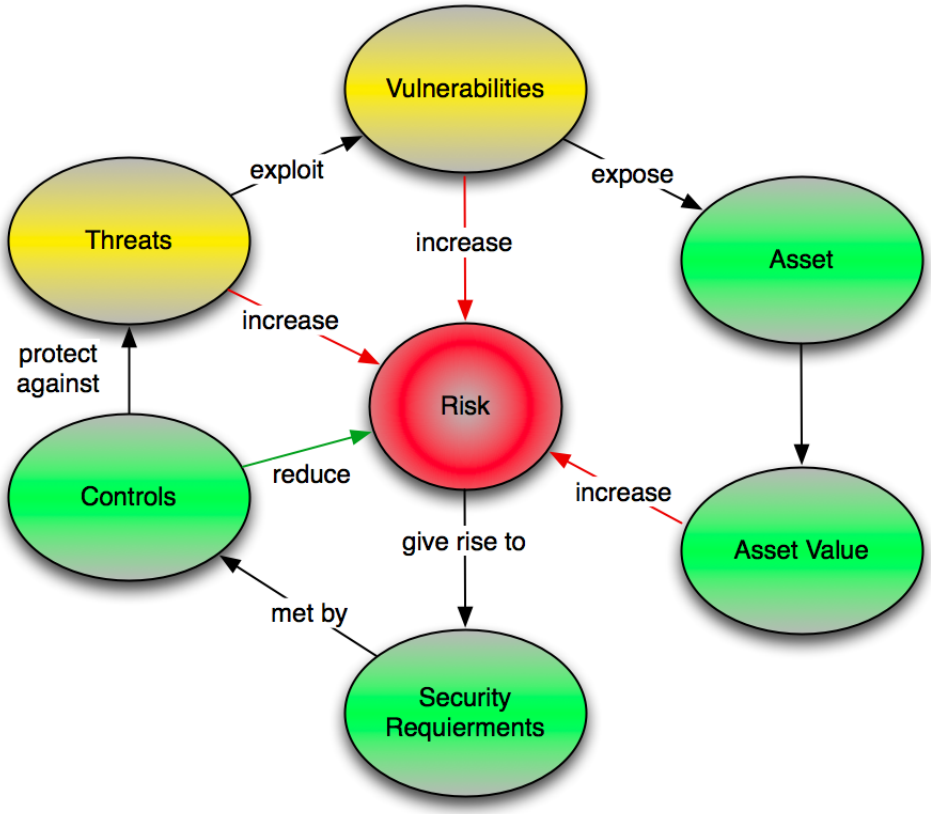

Figure 6.1: Risk Management Concepts (Source: 'Management of Information Security' by Whitman and Mattord, 2010)

6.2 Risk Assessment Methodology

The methodology used to establish the risk assessment consists of both a procedural and a technical dimension. As shown in figure 6.2, the methodology has 2 phases, the documentation phase and the risk determination Phase.

6.2.1 Phase 1: Documentation phase

The process of managing risk starts with the identification and classification of assets. This process obtains knowledge from senior management, section managers, opera-

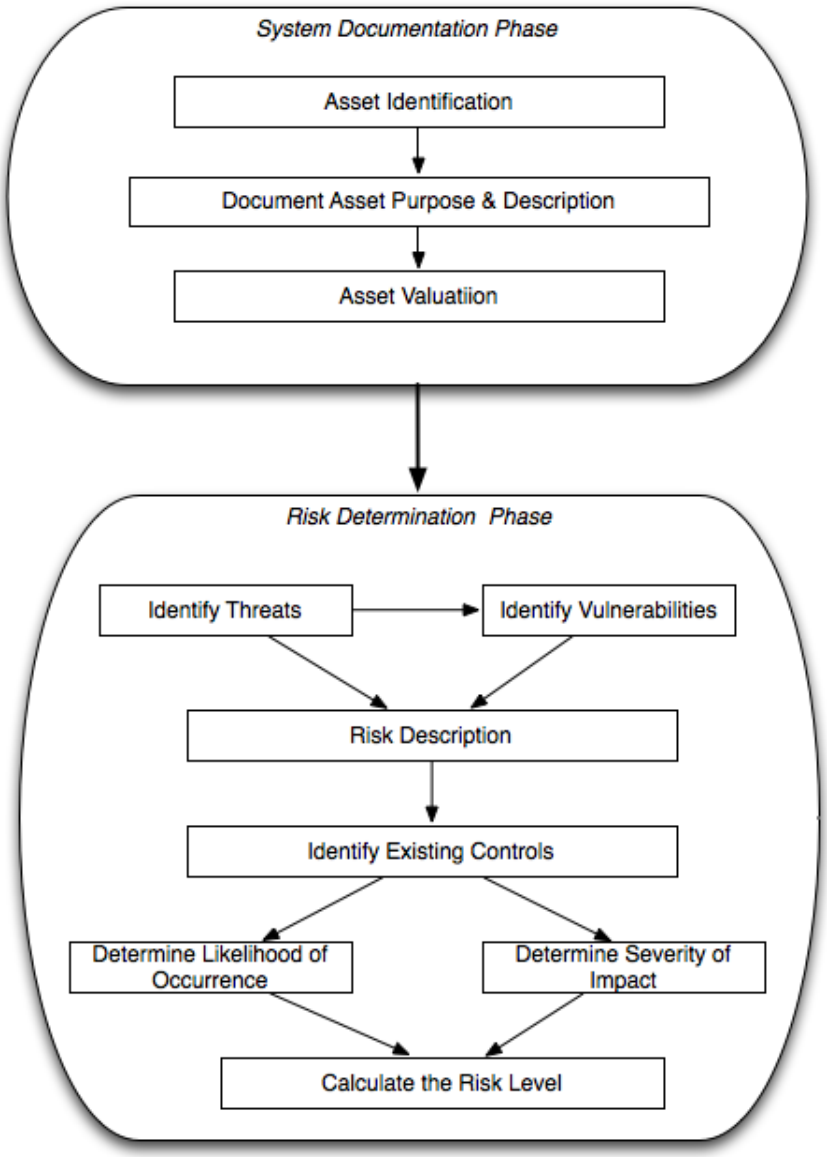

Figure 6.2: Procedural Phases of Risk Assessment

tions and technical staff to identify important assets together with criticality rating, their security requirements and perceived threats. An asset is something that has value or utility for the organisation and for its continuing business operations. Information too is an asset and hence needs protection to ensure uninterrupted business opera-

tions and business continuity. Asset identification and valuation, based on the business needs of an organisation, is a major factor in the risk management process. To correctly identify the asset owners, it helps to assign each asset to one of the following broad categories:

1. Information Assets: These may be understood as digital information such as an e-mail, a worksheet, or a digital document, and hard copy information such as printed documents, memos, agreements, among others.

2. Software Assets: These are operating systems, applications (whether proprietary or third party's), ERP systems, CRM, BI, among others.

3. Physical Assets: This group includes physical environments (data-centre, safe room, management room, etc.) as well as cabling, piping, antennas, hardware, among others.

4. People: This category includes employees, third parties, trainees, among others. In general, a person is indicated as an asset by their office name or the job title.

5. Utilities: The utilities may be defined as all assets depending on third-party's services, such as the electricity, water, ISP connectivity etc.

6. Intangible Assets: Although not valued at all in the asset identification process, this category is, however of great importance. All intangible assets should be identified, and knowledge, competitive advantage, organisational image, and so on, are included in this group. These assets are generally associated with processes where, for instance, the company's brand trustworthiness and perception are essential for the company to perform their activities.

Note that some of the above assets are infrastructure components that service a wide range of business applications and do not necessarily have a single business owner. For the purpose of managing risk, these pooled assets will be considered as owned by a particular business unit. In order to identify the appropriate protection for assets, it is necessary to assess their value in terms of their importance to the business. These values are derived based on potential business impact in terms of loss of Confidentiality, Integrity and Availability of the assets resulting in a loss to the organisation. The asset owners are responsible for identification, classification and valuation of their assets. The sensitivity and confidentiality of assets must be identified so that suitable protection levels can be applied. All information assets classified will be labelled and handled as per the Information labelling and handling policy and procedure.

6.2.1.1 Documentation Asset Purpose and Description

For each asset, a clear statement of its role in the business must be documented. This statement is an important indicator of the criticality of the asset. Any interdependency with other assets will also be identified. Each asset must have an owner accountable. Some assets such as business applications may also have information asset administrator (IT) nominated by business owners. Ownership and accountability for assets helps to ensure that adequate care is taken for the asset and information security is maintained. The responsibility for implementing security controls may be delegated but the accountability should remain with the nominated owner of the information asset.

6.2.1.2 Asset Valuation

In order to identify the appropriate protection for assets, it is necessary to assess their value in terms of their importance to the business. These values are derived based on

the potential business impact in terms of loss of Confidentiality, Integrity and Availability of the assets and the resulting loss to the organisation. The asset owners are responsible for identification, classification and valuation of their assets. The sensitivity and confidentiality of assets must be identified so that suitable protection levels can be applied. All information assets classified will be labelled and handled as per the Information labelling and handling policy and procedure. It is not economically viable to afford the highest level of protection of all assets. Asset valuation is an important process that helps to provide appropriate protection to the assets based on their sensitivity and criticality. To facilitate appropriate protection by means of policies, procedures and controls, the values to an asset should be specified in terms of Confidentiality, Integrity and Availability by the asset owners.

The asset valuation/business impact analysis parameters used are as shown in Table 6.1. The value of each asset will be calculated based on the maximum of individual C, I and A values. This is the applicable asset value for the risk management process as it represents the importance of that asset to the UAE e Government. The total value of the asset is equal to the sum of all (attributes * its level).

6.2.2 Phase 2- Risk Determination Phase

6.2.2.1 Creating Threat Profiles

A threat is an undesirable event that could cause harm to an asset by violating its security. Threats are a function of the opportunities and value to an intruder, and the level of sophistication of the user. This process analyses information produced by Phase 1 and selects critical assets, refines their associated security requirements and identifies threats to the assets. The following questions are addressed to decide the

Table 6.1: Asset Valuation Matrix

Asset value	High (3)	Medium (2)	Low (1)
Confidentiality	Unauthorised disclosure of information can lead to major financial loss, violation of confidentiality agreements or loss of competitive advantage and image of the company.	Unauthorised disclosure of information can lead to loss of competitive advantage and disrupt internal operations.	Unauthorised disclosure has minimum or no impact on business or operations.
Integrity	Unauthorised Information alteration may lead to major financial loss, violation of third party agreements or loss of competitive advantage and image of the company.	Unauthorised Information alteration can lead to loss of competitive advantage and disrupt internal operations.	Unauthorised Information alteration has low or minimal impact.
Availability	Non Availability will affect the majority of the critical business functions resulting in major financial loss, violation of SLAs or loss of competitive advantage.	Non Availability will affect many internal critical operations.	Non Availability will not affect or will have negligible business or internal operations.

organisation's threats profile (86):

- What are the threats?
- When and where can a threat occur?
- Who could be the perpetrator of the threat?

- How often has the threat affected the asset?

The output of this process is a threat profile for the organisation. The characteristics of the critical assets and the vulnerabilities of infrastructure components are analysed together in order to identify various threats to the assets. Together with identified vulnerabilities, the threats pose risk to the assets of e-Government.

Each of the threats as shown in table 6.2, have been categorised as High, Medium and Low based on their possible impact on business functions. It is important to remember that the threat ratings can change if there is any change in the business environment.

Table 6.2: Determining the Threat Level

High (3)	Medium (2)	Low (1)
The threat that can cause	The threat that can cause	The threat that may not exist or can cause
a. Complete outage of production environment b. High financial loss c. Loss of customer confidence d. Loss of image and reputation	a. Partial outage or outage of non-critical business functions b. Partial disruption of operations c. Disrupt internal operations and procedures d. A situation to face 'High' level threat in future	a. Partial disruption of internal operations b. Damage to internal processes but can be eliminated c. No or minimum damage by following best practices d. A situation to face 'medium' level threat in future

6.2.2.2 Identify Vulnerabilities

Vulnerability is a weakness in a system, process or procedure that can be exploited to launch an attack on an asset. As mentioned in previous pages, threats and vulnerabilities are linked together because, a threat without an associated vulnerability does not present any risk to the asset. Using vulnerability assessment tools and techniques, key infrastructure components are identified and vulnerabilities are evaluated. Particular attention is given to vulnerabilities that could be exploited by threats that are identified during the threat assessment phase.

During the vulnerability assessment exercise, components of the infrastructure are examined individually to identify weaknesses that could be exploited by the identified threats. The vulnerabilities are identified in selected assets at various instances as part of various assessment exercises carried out. They are rated as High, Medium or Low based on the severity and complexity of exploitation of those vulnerabilities as shown in table 6.3. The sources of vulnerabilities are determined from technical assessment of infrastructure components can reveal security related vulnerabilities. Technical assessments are normally performed using tools, process walk-through, penetration testing and interviews.

6.3 Risk Analysis

Risk assessment process includes evaluation of likelihood and severity of risk actions associated with an asset. The actual risk analysis involves creation of various matrices and tables to arrive at a measurable value of risk. As various information security best practices highlight, there is no right or wrong methodology of conducting the risk analysis. However the risk methodology must be able to provide comparable and re-

Table 6.3: Determining the Vulnerability Level

High (3)	Medium (2)	Low (1)
a. The vulnerability is easy to exploit. b. The vulnerability is easy to exploit due to the availability of resources/tools. c. Vulnerability can be exploited by an unskilled person. d. Exploitation may lead to huge financial loss and disrupt operations. e. Exploitation may lead to loss of image and reputation. f. Vulnerability cannot be mitigated or involve huge investment or change/introduction of major processes.	a. The vulnerability is difficult to exploit. b. The vulnerability is exploitable due to the availability commercial resources/tools. c. Vulnerability can be exploited by an unskilled person with the help of readily available resources. d. Exploitation may lead to disruption of internal operations. e. Exploitation may lead to partial disruption of financial operations. f. Mitigation of vulnerability may involve some investment or change of existing processes.	a. The vulnerability is impossible to exploit b. Vulnerability can be exploited only by a highly skilled person with the help of various commercial resources c. The vulnerability may not require any mitigation d. Exploitation time is very high e. Exploitation may not lead to disruption of operations or financial loss f. The mitigation may be possible with existing processes and by reconfiguration of technological items.

producible results. The risk of an undesired event occurring is a function of asset value and Threat and Vulnerability present in an asset. The basic method for identifying the risks is to address the following questions for each asset:

- What known threats to the asset exist and exploit the known vulnerabilities?
- What can go wrong? The process additionally assesses the identified risks in order to establish the high priority risks in terms of impact. To assess the risks, following questions should be addressed:

- What is the likelihood that the risk will occur?
- What would be the severity if an event did occur?
- What is the Risk Level, given the likelihood and severity?
- What is the priority for the risk in terms of impact on the business?

6.3.1 Determination of Severity

Severity (Exposure Factor) is the result of successful risk action (i.e. A vulnerability being exploited by a threat) against an asset. It is related to the criticality of an asset which is determined by the level of protection e-Government requires for the asset, taking into account the three most important security goals, namely Confidentiality, Integrity and Availability. In simple terms, severity is the worst potential result of an event that has occurred due to a threat\vulnerability pair.

Exposure factor or Severity Values given in the table 6.4. The severity value (threat - vulnerability value) is determined by taking the severity rating of a threat and that of a vulnerability. For example a medium threat (value 2) might exploit a high level vulnerability (value 3), which will result in a severity (EF) value of 6 (Threat * Vulnerability).

Table 6.4: Exposure Factor Matrix

Threat / Vulnerability	Low (1)	Medium (2)	High (3)
Low (1)	1	2	3
Medium (2)	2	4	6
High (3)	3	6	9

6.3.2 Likelihood of Occurrence

The Likelihood of occurrence is defined as the frequency of a threat materialising in the environment under scope. The likelihoods of occurrence are influenced by environmental changes in which the threat exists and major business process changes. The likelihood of occurrence is classified as follows (87):

- Rare (value = 1) has not happened in a long time (the last 3 years)
- Often (value = 2) may happen once a year
- Frequent (value = 3) may happen more than once in a quarter

6.3.3 Calculation of Risk Impact

Risk is the combination of the asset value, the vulnerabilities with respect to the asset, and the threats that can exploit the vulnerabilities. If all are high, then the risk impact is high. If all are low, then the risk impact is low. Conversely, the asset may be very valuable but the vulnerability may be exceedingly low (88). The risk impact for each threat action is calculated based on the following equation:

Risk Impact = Asset Value * Exposure Factor * Likelihood of Occurrence

While finalising an approach to mitigate and treat the risks encountered it is important to have a criteria based on which an informed decision can be taken by the management to suitably treat the risks encountered and decide as to how the organisation should respond to the risks encountered.

6.4 Risk Assessment of UAE e-Government

Four departments the within the e-Government are involved in the risk assessment activities, the methodology describes in section 5.3 was used to determine the asset values in terms of their importance to the business. These values are derived based on potential business impact in terms of loss of Confidentiality, Integrity and Availability of the assets resulting in a loss to the organisation. This was achieved with the assistance of the asset owners. The sensitivity and confidentiality of assets must be identified so that suitable protection levels can be applied. Then a threat profile and the resultant vulnerabilities for the assets was calculated . This was achieved by physical inspection of the assets, investigation of historical occurrences with the security management of each department and the penetration test results described in detail in the in chapter 6. In order to classify the risks, a formal consultation with the management was carried out and the following rules for classification was adopted:

- A risk impact value less than 27 is acceptable. 27 is derived from the multiplication of a highest asset value 9, a low exposure factor 3, and a rare occurrence value of 1. In such circumstances, the management is responsible to ensure that current controls remain enforced and continuous monitoring is in place.

- A risk impact value above 27 and below 36 has to be treated with the proper controls to bring down below 27. The value 36 is derived from the multiplication of a highest asset value 9, a medium exposure factor 4, and a rare occurrence value 1. In such circumstances, the management is responsible for creating a Mitigation plan that needs to be put in place within a span of 6 months.

- The management cannot accept any risk impact value greater than 36, which

requires an immediate and urgent attention. The management require to initiate an action within 1 week of identification and a plan needs to put in place to mitigate the risk within 1 to 3 months unless restricted by specific constraints.

The result of the risk profile of the assets is shown in table 6.5. The total number of assets identified was 30 and based on classification criteria it was found that 11 assets had high risks, 9 assets had medium risks and the remaining 10 assets had low risks. The high risk assets require an immediate and urgent attention from the information security management team. Likewise, there are some assets that are classified as medium risk and need to be treated with the proper controls to bring down below 27.

To manage the risks it is important to know what controls need to be implemented to reduce the identified risks to an acceptable level. Before undertaking the treatment, there should be a process of selection of appropriate controls, taking into account the operational objectives and priorities along with the resources available. The process of implementation of appropriate controls will leave residual risks i.e. risks at a reduced level which needs to be addressed by us appropriately depending upon the risk appetite. While selecting the controls, it is beneficial to identify the function of control in terms of protection, deterrence, detection, response and recovery. It is more cost effective to select protective controls that can serve multiple functions. Risk treatment planning is a process of deciding the steps that need to be taken to reduce threats and take advantage of the opportunities discovered during the risk analysis. Table 6.6 shows the risks and their mitigation plans for the systems under consideration, the management is required to implement these plans in order to reduce the assets risks otherwise it will not be able to obtain the ISO 27001 certification.

Table 6.5: Asset Risk Profile

Asset Name		Asset Value	Threat	Vulnerability	Occurrence	Risk Impact	Classification
Telecom	C	3	1	3	1	28	Medium
	I	1	1	1	1		
	A	3	2	3	1		
Cisco Switch	C	3	2	3	1	42	High
	I	3	2	2	1		
	A	3	2	2	1		
DR	C	3	3	2	1	40	High
	I	3	3	2	1		
	A	2	1	2	1		
CID	C	2	2	3	1	45	High
	I	3	3	3	1		
	A	3	1	2	1		
Immigration	C	3	2	2	1	42	High
	I	3	2	3	1		
	A	3	2	2	1		
E-Services	C	3	2	2	1	34	Medium
	I	3	2	3	1		
	A	2	1	2	1		
E-Border	C	2	2	3	1	26	Low
	I	3	2	2	1		
	A	1	1	2	1		
E-Gate	C	1	2	2	1	20	Low
	I	3	2	2	1		
	A	1	2	2	1		
Maintenance Application	C	1	1	2	1	20	Low
	I	3	1	2	1		
	A	3	2	2	1		
MEMEX	C	3	1	2	1	38	High
	I	3	2	2	2		
	A	2	2	2	1		
Archiving System	C	1	2	3	1	22	Low
	I	3	2	2	1		
	A	2	1	2	1		
Network Management	C	1	2	2	2	28	Medium
	I	1	2	3	2		
	A	2	2	2	1		
Security Infrastructure	C	3	2	2	1	42	High
	I	3	2	2	1		
	A	3	2	3	1		
Dubai Gateway	C	3	2	3	1	44	High
	I	2	2	2	1		
	A	3	2	3	1		
Help Desk	C	1	1	2	2	14	Low
	I	1	2	2	1		
	A	1	2	3	1		
Data Replication SUN	C	3	2	2	1	60	High
	I	3	2	2	1		
	A	3	3	2	2		

Asset Name		Asset Value	Threat	Vulnerability	Occurrence	Risk Impact	Classification
DMZ	C	3	2	3	2	60	High
	I	3	2	2	1		
	A	3	2	2	1		
SSD	C	2	2	2	2	28	Medium
	I	2	2	2	1		
	A	2	1	2	1		
Store System	C	2	2	3	1	34	Medium
	I	3	2	3	1		
	A	2	1	2	1		
Database Monitoring	C	1	1	2	1	13	Low
	I	1	1	2	1		
	A	1	3	3	1		
Time Attendance System	C	1	1	2	1	28	Medium
	I	1	1	2	1		
	A	3	2	2	2		
Inspection System	C	1	2	2	3	26	Low
	I	1	2	2	3		
	A	1	1	2	1		
Finance System	C	1	2	2	2	18	Low
	I	2	2	2	1		
	A	1	1	2	1		
SMS System	C	1	2	2	1	10	Low
	I	1	2	2	1		
	A	1	1	2	1		
UDB	C	3	2	2	3	108	High
	I	3	2	2	3		
	A	3	2	2	3		
MOI	C	3	2	2	3	90	High
	I	3	1	2	3		
	A	3	2	2	3		
Network infrastructure	C	2	2	3	1	36	Medium
	I	3	1	2	1		
	A	3	2	3	1		
e-Mail Exchange	C	2	1	2	1	28	Medium
	I	2	2	2	1		
	A	2	2	2	2		
HR. System	C	2	1	2	1	14	Low
	I	3	1	2	1		
	A	2	1	2	1		
Internet	C	2	1	2	1	32	Medium
	I	2	1	2	1		
	A	2	2	2	3		

Table 6.6: Risks Mitigation Plans

Asset	Risks	Recommendation for managing the risks
Telecom	Cable exposed	Protect cables
	Poor A/C	Improve A/C system
	Fire hazard	Install a Fire Hazard System
	System down	Replication
Cisco Core switch	Unauthorized access	Biometric Physical Access Control system should be established
	data leakage	
	System down	Replication
DR	Tapes theft,	Biometric Physical Access Control system should be established
	Unauthorised access,	Database Encryption
	data leakage	
CID	Eavesdropping,	Implement an encryption system on the database
	Unauthorised access	Biometric Physical Access Control system should be established
	System down	Replication
Immigration	Unauthorized access	Implement an encryption system on the database
	data leakage	Biometric Physical Access Control system should be established
	System down	Replication
E-Services	No cluster	Install cluster the data centre
	Outsourced	Hire new staff e-Government can manage the system
	lack of security and can be hacked	Install special controls like Firewall, IDSISP for E-Services
E-Boarder	No clustering solution	Install cluster
	Unauthorized access	Design Security Architecture
E-gate	No clustering solution	Install cluster
	Unauthorized access	Design Security Architecture
Maintenance Application	No clustering solution	Install the cluster
	Unauthorized access	Design Security Architecture

Asset	Risks	Recommendation for managing the risks
MEMEX	No cluster	Install cluster
	Unauthorized access	Biometric Physical Access Control system should be established
	System down	Replication
Archiving	No cluster	Install the cluster
	Unauthorized access	Design Security Architecture
Network Management	Cables exposed,	Improve the state of the cables
	Easy physical access	Biometric Physical Access Control system should be established
Security Infrastructure	Risk of access from hackers due to open ports	A comprehensive Security Information and Event Management (SIEM) should be implemented
	Easy physical access,	Biometric Physical Access Control system should be established
	Cables exposed	Protect the cables
	System down	Replication
Dubai Gateway	Unauthorized access	Access control: reviews should be done for physical & logical access
	System down	Replication
Help desk	System down	Replication
Replication of Data, SUN	Unauthorized access	Access control: reviews should be done for physical & logical access
	System down	Replication
	Different systems interactions	Design Security Architecture
DMZ	Unauthorized access	Implement an encryption system on the database. Biometric system should be established
SSD	Unauthorized access	Implement an encryption system on the database. Biometric Physical Access Control system should be established
	No cluster	Install the cluster
Time Attendance System	System down	Replication

Asset	Risks	Recommendation for managing the risks
Store System	Unauthorised access	Implement an encryption system on the database. Biometric Physical Access Control system should be established
	No cluster	Install the cluster
DB Monitoring	Shortage of staff	Address by hiring more staff
Inspection System	Unauthorized access	Biometric Physical Access Control system should be established
	No cluster	Install the cluster
Finance System	Unauthorized access	Biometric Physical Access Control system should be established
	No cluster	Install the cluster
SMS System	Unauthorized access	Biometric Physical Access Control system should be established
	No cluster	Install the cluster
UDB	Unauthorized access	Control the user access. Implement an encryption system on the database (Monitoring tool should be installed
	System down	Replication
MOI Active Directory	unauthorized access	Establish a Network Access control solution
	Integrity compromised	Review ICT security manager
Resolution System	System down	Replication
Network Infrastructure	Cables exposed	Better cabling protection
	Easy physical access	Biometric Physical Access Control system should be established. Install RFID based asset management system to trace the assets
	Weak network access control	Establish a Network Access Control Solution
Mail Exchange	No encryption& Email Encryption Gateway including internal	external encryption
	No cluster	Install the cluster
HR System	No cluster	Install cluster
Internet	No proper security architecture in place	Establish Security Architecture for IT Infrastructure
	Can be penetrated, Image damage	Install Web Application Firewall for Portal

6.5 Conclusion

The results of this chapter have highlighted the value of the risk assessment process in identifying key security weaknesses within the organisation's systems. Each asset has an associated risk impact on the organisation therefore it is necessary to define an acceptable level to be used as a threshold in decision making within the organisation. This process must be readily understandable and simple to implement. The result should be comparable and reproducible; it should meet the requirements of business information security, legal and regulatory requirements and define the risk acceptance levels.

In order to ensure the effectiveness of the information risk management framework, the continual improvement of the process is essential. Corrective and preventive action procedures need to be considered along with the information security policy and procedures, security objectives, audit results, analysis of monitoring events and management review. As the organisation matures in terms of risk management, the acceptance levels can be reduced to increase the level of security and to trigger the continual improvement process.

The risk management framework and acceptance levels need to be reviewed at least once a year to ensure the effectiveness of the framework in continuing to reflect the requirements of the e-Government. Reviews should include an assessment of the adequacy and effectiveness of the risk assessment methodology as well as the risk treatment strategies. They should also seek to identify any significant changes within the organisation, changes in technology, changes in organisational objectives and processes, changes to threat profiles and changes in legal and regulatory situation. This information risk management framework shall also be reviewed whenever there is a

major change in infrastructure or whenever a major incident occurs. All risks need to be effectively treated which results in the reduction of the risk to an acceptable level, with minimal adverse impact on the organisation's resources and mission.

Chapter 7

Penetration Test

7.1 Introduction

Having completed the Gap Analysis and the Risk Assessment for the UAE e-Government, this chapter proceeds to describe the next part in the chain, the penetration test. Then it elaborates on the importance of the penetration test as a way of protecting and securing information. This leads on to a list of the different types of penetration test and reveals the best and most accurate way to examine the strength of electronic security systems. The test was carried out on four organisations within the UAE e-Government the result of the test, which includes a list of existing vulnerabilities is presented with suggestions for specific solutions for their elimination.

As information systems become an integral part of government services, one of the main concerns of developing reliable information systems is data security. The growing number of devices connected to e-Government services has increased dramatically, and the variety and complexity of the systems software used by these devices have made information systems security a bigger problem now than in the past (89).

Furthermore, it is vital for businesses to protect an organisation's information assets by following a comprehensive and structured approach, to provide protection from the risks that an organisation might face (90). Security experts have developed a variety of security assurance methods, such as the penetration test, in an attempt to solve these security problems and to comply with the international security standards regulations.

7.2 Penetration Test

A penetration test is a tool and software that detects the vulnerabilities in the security of a computer system and network devices, like firewalls, routers, switches, servers and applications. The test reveals the points of weakness in system configuration hardware and software flaws, and operational weaknesses which could be used by hackers to gain unauthorised access to the system (data) and cause damage to the system. The test can be performed with or without detailed prior knowledge of the environment. When it is performed without prior knowledge additional steps will be taken to enumerate hosts and applications, and to assess the ease with which any outsider could exploit publicly-available information or social engineering to gain unauthorised access.

The penetration test can be defined as the "simulation of a real-world attack against a target network or application, encompassing a wide range of activities and variations" (91). It is a critical step in the development of any secure system, as it not only stresses the operation, but the implementation and design of a system (92).

Penetration testing is the process of trying to reach resources without the acquisition of the required passwords. The test is a way of skipping a certain permitted security level to reach a higher one, which is not supposed to be reached in the first place. It functions as a simulation and a replication of an outsider electronic attack;

such an attack will reveal the failing points that hackers could use to break the entire system by finding hidden loopholes. After the hypothetical attack, an intensive study is conducted and presented to the people in charge of securing the electronic system. A penetration test is a clear-cut tool that exposes loopholes that, in some cases, the whole system may disregard and overlook, or would not consider the cause of any issues in the future. The next step in a correctly conducted penetration test is to set the appropriate recommendations to reduce risks. Penetration testing is preferential to other tests because of its ability to reveal what may be difficult or impossible to be detected with automated network or scanning software; it provides companies with actionable findings and intensive analysis, including both tactical and strategic recommendations. The test will answer such questions as:

- Are the network, firewalls and user application(s) vulnerable to external or internal attacks?
- Is it possible for external intruders to gain access to critical data/resources?
- How effective is the organisational social engineering?
- Are the operational controls implemented effectively?

For a successful penetration test that meets the client's expectations, the clear definition of goals is absolutely essential. If goals cannot be attained or cannot be achieved efficiently, the tester should notify the client in the preparation phase and recommend alternative procedures, such as an IT audit or IT security consulting services. The organisation goals that can be attained by penetration testing can be divided into four categories (93):

i. Improving security of technical systems: Most organisations require a penetration test for the purpose of improving the security of their systems. The main purpose of penetration testing is to find out how possible it is for the systems to be hacked due to technical vulnerability, the management of systems, or a combination of the aforementioned two possibilities. The systems normally include security systems, such as firewalls, routers, switches, and the facing-out systems, such as web servers. Penetration tests can give the organisation a clear list and map for improving the security of technical systems.

ii. Identifying vulnerabilities: In order to achieve the goal of improving the security management of technical systems, the identification of vulnerability is the key objective of the penetration test. Sometimes even when a unit system is fully tested, it is still vulnerable to threat when it is integrated with other systems or vulnerabilities caused by improper configuration. For example, two LANs are all secured separately, however, weaknesses may be found when they are combined. Hence, applying a penetration test to find out the vulnerability and try to reduce the possible external threat could utilise the vulnerability of the systems.

iii. Having IT security confirmed by an external third party: Impartiality is very important to security checking, since the internal staffs are the ones e-Government construct the security mechanism. By utilising the security knowledge, the company budget and due care of internal staff, the security systems are allocated and configured. An external third party is better positioned to check the robustness of a security system because the external third party will test the systems from different viewpoints, with different knowledge and tools, which can help the internal staff in locating their blind-spots, weaknesses in the systems, and sometimes,

mistakes in configuration or system arrangement.

iv. Improving security of organisational and personnel infrastructure: Not all vulnerabilities are from technical weaknesses; weaknesses also stem from the management and people. As APT (Advanced Persistent Threat) attacks are very often seen in government systems, organisational and personnel vulnerabilities are therefore also points that penetration tests would be utilised to identify. Social engineering techniques are commonly used by hackers to break the lines of defence in organisations, and penetration tests simulate the social engineering to test organisational and personnel defence abilities.

7.3 Penetration Test Procedure and Planning

To conduct a successful test, there are certain procedures that need to be put in place. These procedures are shown in Figure 7.1 and should be conducted in the steps shown. The first step is to gather information about the IP addresses of the networks under test; the servers and databases should be freely accessible by the assessing team. Then, a port scan is conducted on the system under test using appropriate software, such as Nmap, Kismet and Nessus. The third step is to identify the type of operating systems used in the system and their versions. In this stage, the types of applications used in the system are also identified; this process is called "fingerprinting" the network. The next step is to use the information gathered to identify the vulnerabilities of the operating system and the applications; the scanning will highlight any unnoticed weaknesses in a system or software. The final step is to exploit the detected vulnerabilities; using the weaknesses to gain unauthorised access to the resources/data, or to prepare an attack on the system does this.

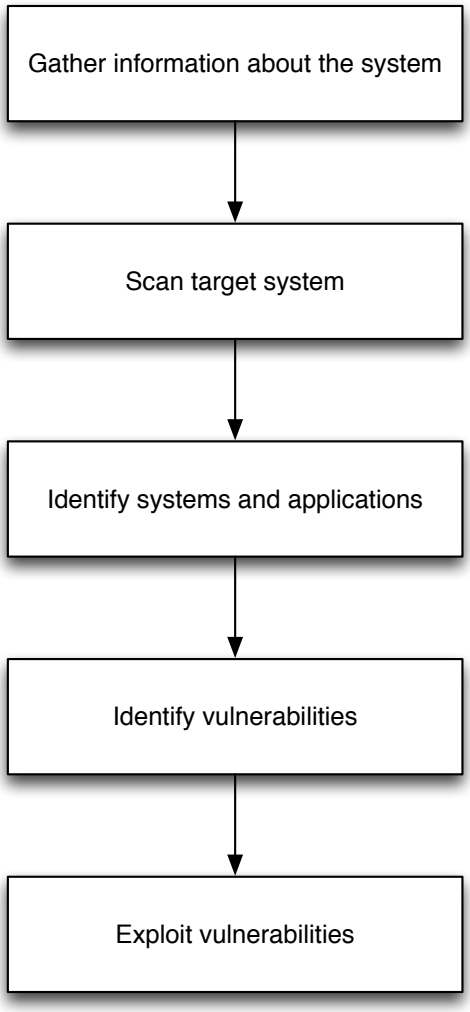

Figure 7.1: Penetration Test Procedure

7.3.1 Classification of Penetration Test

Penetration tests are designed and conducted to meet the organisation's requirements; therefore a criterion needs to be agreed on between both parties (i.e. the organisation's IT security team and the external testers). This should include features such as the aggressiveness of the testing and the scope of the test. Figure 7.2 shows the classification of the penetration test used, and a description of each layer is provided below.

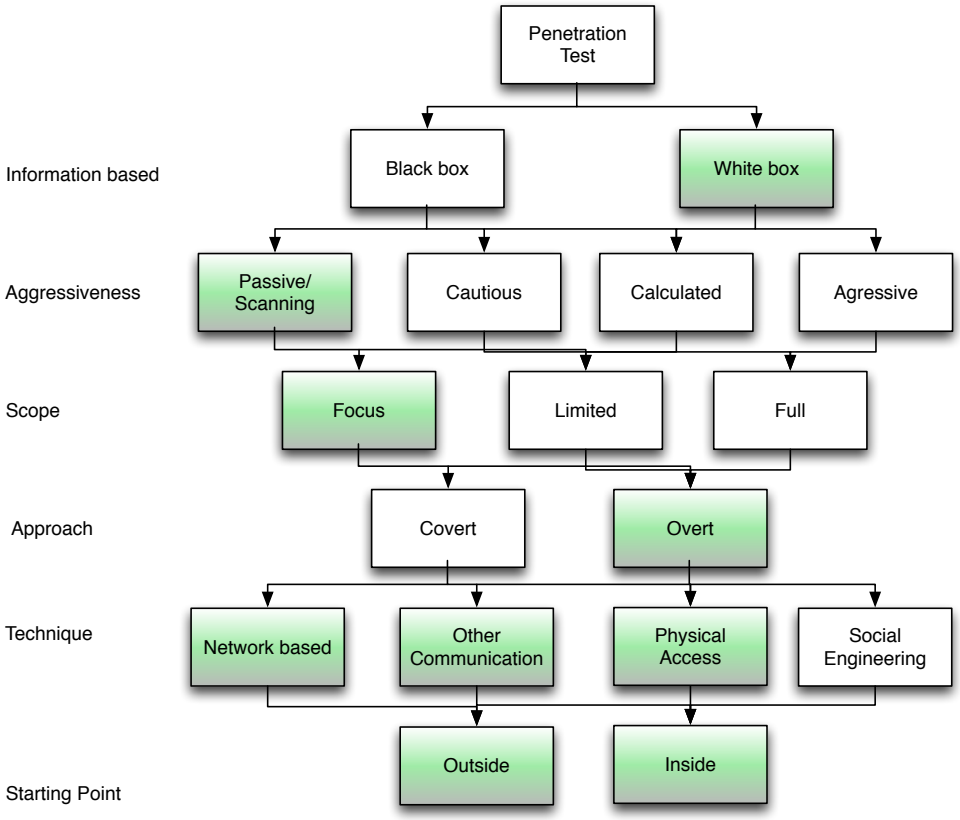

Figure 7.2: Penetration Test Classification

i. Information Based: The penetration test is divided into two categories, where the information of security systems are either provided or not provided. If the penetration test is done after the organisation has disclosed enough information about the system to the tester, for example, the network diagram, structure, IP and the system architecture or even the codes and configurations of systems, it is called a "White Box" penetration test. In contrast, "Black Box" means the tester did not get any information from the organisation, and must penetrate the systems in the same way as external users using the systems. In our case, it was decided to use the white box approach, since prior knowledge about the network was given to the

test team.

ii. Aggressiveness: The aggressiveness amounts to the style of the penetration test, and also the intensity of the penetration; therefore, the aggressiveness will decide the tools and techniques used in the test. From the left-hand side in the diagram, "scanning" is the most passive way of running a penetration test (also called a vulnerability scan). However, the more intensive method of "cautious" testing will be a more detailed penetration; this penetration is not just scanning but also will use some hacking tools to penetrate vulnerabilities. "Calculated" testing is a penetration test which is planned and well-structured, and that utilises specific tools and techniques, along with different techniques for different targets. Most importantly, the data is analysed and plans are revised after new information are gained by the tester. The "aggressive" technique of penetration will fully utilise all the penetration skills of the tester, and apply most of these tools. Combinations of different techniques, social engineering and persistent attacks are often involved in this style of penetration test. In the case of the UAE e-Government, a passive scanning approach was used, due to the sensitive nature of the network under test.

iii. Scope: The scope of a test is the decision of the organisation, based on their requirements and objectives requiring the penetration test. A "focused" scope means the penetration concentrates on some specific targets, purposes, threats and weaknesses. "Limited" indicates a scope that is based on the budget, time or other resources, and sets the scope in limited systems or area. A "full" penetration test normally includes all the security systems, entry into all of the system, across the complete organisation. During the penetration test for UAE e-Government, the scope was focused on specific targets that were agreed with the organisation

management.

iv. Approach: For the organisation's staff, an "overt" penetration test means that the penetration is announced and the methods of attack are known to the staff of the organisation before the penetration. A "covert" penetration, in contrast, involves testing without informing the staff managing the systems when or how the penetration is going to attack their systems. These two methods of testing have different purpose: the overt method can test and let the staff prepare well, and sometimes watch the attack path, so as to let the staff better understand how to prevent or to disable the attack path. The covert method is more straightforward, in that the final result shows the staff the strength of their security management. Since the organisation staff were fully aware of the e-Government test, an overt approach was thus used.

v. Technique: Many different penetration test techniques are known to the market. Network-based penetration is the most common technique, where the network is always the main entry point of a system in the network era. Besides the logical entry, physical access and other communication channels can also be the targets of penetrations. Social engineering is the technique of approaching the staff of security control or internal users to get the passwords or other resources necessary for the penetration of the systems. The social engineering part was not included in this test, as a special extensive questionnaire was conducted to assess the organisation culture (this is described in Chapter 8 of the thesis).

vi. Starting Point: There are two choices of starting points in penetration: outside and inside. These two starting points are directed towards two different situations. From outside, the attacker simulates the external hacker trying to penetrate the

external defence mechanism. From the inside, firewalls and other outward-facing mechanisms are not available, and this penetration test simulates a hacker already inside the organisation, or the event of an attacker coming from internal staff.

7.4 Experiment Setting

In this section, we describe the systems that were tested by the penetration test team. Due to the high security nature of the establishment under test, it was decided to use external specialist consultants to assist with conducting the test. The tools used for this study are listed in Table 7.1, the list describes each tool, their functionality and the type of assessment they could be used for. The assessment was structured into five work packages, which are described below.

7.4.1 Testing of Web Portals

This test is used to analyse the security of the web portals for customers and partners. Two web portals, provided by the UAE e-Government, were tested, as these systems represent a potential risk to all systems and networks of the e-Government.

7.4.2 Testing of Internal Systems

This test considers the security of all internal systems within the four given network ranges. Deeper testing of found systems was agreed by the UAE e-Government. The following networks were analysed.

Table 7.1: Software Used To Conduct the Test

Tool	Platform	Assessment type
BackTrack	Linux	General hacking tool, covering (94): • Information Gathering tools • Vulnerability Assessment tools • Exploitation tools • Maintain Access Right tools • Privilege Escalation tools • Stress Testing tools • Forensics tools
Kismet	Unix	Network sniffer/detector, used in packet detection or sniffing. Any network card with the Raw Monitoring Mode can sniff the network traffic. This tool works passively, and can be used for detecting the signal of Wireless Access Point and Access Client (95).
Nmap	Unix Window	Network scanner, the name coming from Network Mapper. Can be run on many different OSs. This tool is used to discover the host and the services run on the computer (96).
Nessus		Nessus is a comprehensive vulnerability-scanning tool. This tool is used to detect the vulnerability of tested system, by comparing them to patterns of vulnerability. Nessus has some different policies set which cover vulnerabilities allowing a remote hacker to control or access sensitive data on a system due to misconfiguration, people using default passwords or some common passwords, and blank/absent passwords on some system accounts (97).
Nikto2		Web Scanner, tests web servers for malicious file, this tool is used for testing the web server (98).
Netcat		Netcat is a tool for debugging and dependable investigation. By analysing TCP and UDP, and other TCP/IP protocol, it is a very powerful TCP/IP analysing tool (99).
Wireshark		WireShark is a packet analyser. Used for network analysing and software communication analysing (100)
w3af		w3af is a Web Application Attack and Audit Framework, used to detect 200 web server vulnerabilities. This tool is also used for web application vulnerability scanning (101).
Yersinia		Yersinia is a network tool special to network protocols. It covers some special protocols, such as the Spanning Tree Protocol, Cisco Discovery Protocol, Dynamic Trunking Protocol, Dynamic Host Configuration Protocol, etc. (102).
Cain and Abel		Cain and Abel is a password recovery tool for Microsoft. It words by sniffing the network for decryption of the encrypted password string (103).
Burp Suite		Burp Suite is an integrated platform for security testing for Web Application. It includes many different tools, such as proxy, Spider, scanner, intruder, repeater, etc.. This tool is used for detecting the security vulnerabilities of web applications (104).

7.4.3 Enumeration of Class B Network

Before we can gain unauthorised access to a network, it is important to know the topology of the network. The target network is scanned using NMAP software to obtain a list of live hosts, as well as to begin mapping the target to get a sense of its architecture and the kind of traffic (for example, TCP, UDP, IPX, etc.) that is allowed. The goal of discovery is to start with no information and gather as much data as possible about the target network and systems. We then use this information to identify potential exploits.

The process of discovering this information is called network enumeration and is the first step of an external penetration test. This step is performed largely over the Internet, using readily available software and publicly accessible repositories of information. Most of the information we obtain in this step is freely available and legal to obtain. However, many companies monitor e-Government tries to get this information since it may indicate a prelude to an attack.

This network represents all of the important systems in the UAE e-Government. The intention of this scan was to get an overview of all systems available in the e-Government environment. Due to the number of systems found (at least 2286 systems were up and running during the testing period), it was not possible to check all systems in depth. As a result, a subset of systems named by the UAE e-Government was scanned in depth.

7.4.3.1 Firewall Configuration Review

The Firewall rule sets given by the UAE e-Government were analysed and compared to "Best Practice" for configuring a Firewall environment. In addition, documents called "Network Access forms", provided by the organisation, were checked against existing

Firewall rule sets on running systems.

7.4.4 Assessment of WLAN Access Points

Basic analyses of WLAN access points and connected client systems were carried out. The intention of this test was to get a quick overview of WLAN systems online. There was no cracking of encryption at any time; no systems were compromised at all.

7.5 Findings & Results

This section describes the initial findings of the penetration test and presents recommendations as to how to mitigate these vulnerabilities. Each finding was characterised into either High, Medium or Low risk, based on how critical it is to the overall system security. Table 7.2 lists the categories used for prioritisation of vulnerabilities and actions to be taken.

The findings listed in Tables 7.3, 7.4 and 7.5 outline the current security status of the systems investigated. A total of 68 findings were identified; out of these, eighteen findings were rated

Table 7.2: Categories of Findings

Risk	Vulnerability Type	Action
High (H)	Critical	The problem found needs to be countered by immediate action. The systems found are under high risk of being compromised or misused.
Medium (M)	Serious	The problem found needs to be corrected in the foreseeable future. The security of the systems affected could be compromised under certain circumstances. An escalation of risk is possible, especially if environment or common knowledge changes. A re-evaluation is to be performed whenever the systems environment changes.
Low (L)	Non-critical	This probably is more a cosmetic than a function-impeding problem. Any abuse is currently deemed improbable. A re-evaluation is to be performed whenever the systems environment changes.

Table 7.3: Vulnerability Assessment of the Web Server 1

Finding	Level	Impact	Recommendation
Unrestricted access to management services	L	Exposing administrative interfaces to the internet increases the number of possible attack vectors at risk from an attacker.	Administrative access should be limited to the IP ranges needed.
No check against trivial passwords	M	With a working account, a possible attacker has more forms to play with, raising the risk of finding possible vulnerabilities.	Protection against the use of trivial passwords should be enabled. Use the Security policy recommendation (Chapter 8).
Trivial "secret" questions	M	An attacker can try to research or guess the secret question and reset the password, thus probably gain access to customer's accounts.	The secret question should be completed by the customer. As default value, provide a number of ideas (driver license number, current car's chassis number, etc.).
Various wrong references to flat-client setup	L	It is hard for customers (especially those using the Arabic language web page) to find the setup programs.	The web page should be debugged, so all hints and links point to the existing setup downloads.
Minimal error handling in Forgot-Password function	L	Such unhelpful and raw error messages can severely impact the reputation of the web application as a e-Governmentle.	Non-working error messages should be overhauled to display meaningful content instead of "Unknown error" or nothing at all.
Possible User enumeration	L	Valid user names can be enumerated.	It should be checked whether it might be safer to assign user names by the system.
Broken Search functions	L	A user cannot search inquiries by job or code, which leads to bad user experience.	The search functionality should be fixed, or references to it should be hidden.
Survey probably not working	L	The survey is not or only partially working.	The survey function should be tested and verified for proper functionality.

Table 7.4: Vulnerability Assessment of Web Server 2

Finding	Level	Impact	Recommendation
SQL blind injection	H	An attacker can delete or modify the database without need for authentication - see "SQL-Injection" section for explanation and background.	The search function should be updated to guard against SQL injection.
Parameter overflow with information disclosure	L	The information disclosure makes path traversal attacks easier.	Error-handling routines should be enhanced to be able to cope with integer overflows and negative values.
Non-deterministic use of URL capitalisation and HTML escaping	L	While the web application itself does not seem to be affected too much from the strange re-encoding (content check due to missing translator not possible), links referencing from outside might result in problems. The additional possibilities of writing/linking to the same resulting URL will probably decrease visibility to search engines and cause additional load onto the server.	The application should be checked why/where this random capitalisation and escaping results from, and be corrected accordingly.

Table 7.5: Vulnerability Assessment of the Server Systems and Applications

Finding	Level	Impact	Recommendation
Window NT 4.0 System still in use	H	This operating system is known to be vulnerable, since no patches and updates are available and the system is not supported by the manufacturer any more.	If this system is not used in the production environment any more, it should be switched off. Otherwise it should be migrated to a supported platform like Windows 2003 or 2008 as soon as possible.
Virus Infection of at least two server systems	H	Even if the server did not seem to infect other systems, it is possible that this system is acting as an infector for other systems.	All systems should be provided with Anti-Virus Scanner software and current (at least daily) pattern updates. The responsibilities and owner of all systems must be provided.
Default installation of server systems	H	As a result of this installation, several unnecessary services are running. Those services increase the attack surface of the system.	Only minimised system installations should be allowed. Create default installation scripts. Group policies for Windows server should be used for system hardening; UNIX servers should be hardened based on scripts.
Use of clear text protocols	H	Passwords and user credentials could be sniffed. There are automated filters available, which can extract credentials automatically from network traffic. Since even administrative logins are sent unencrypted, attackers or non-authorised users can obtain those credentials and gain administrator access.	Only encrypted protocols like SSH, HTTPS or SCP should be used. If protocols like XDMCP or X server are used, they should be used via SSH tunneling only.
Oracle web configuration without authentication	H	Reconfiguration or destruction of Database could be possible (Not tested!) by unauthorised users.	Restrict access to website by using encryption and authentication. Appropriate user rights should be given to configure the server systems.

Finding	Level	Impact	Recommendation
IBM Tivoli Storage Manager Client Multiple Vulnerabilities	H	The remote host is running an IBM Tivoli Storage Manager (TSM) client. The version of the TSM client installed on the remote host reportedly contains buffer overflow vulnerability in its Client Acceptor Daemon (CAD) service. Using an HTTP request with a long Host header, a remote attacker may be able to exploit this issue to crash the affected host or to execute arbitrary commands with administrative privileges.	Upgrade to Tivoli Storage Manager version 5.4.1.2 / 5.3.5.3 / 5.2.5.2 / 5.1.8.1 backup-archive client or the Tivoli Storage Manager Express 5.3.5.3 Client.
Use of old and unpatched Apache Web Servers	H	Systems can be attacked from remote by gaining access to server.	Update to the latest version available or disable service if not used.
Missing Windows Patches and Updates	H	Systems can be attacked from remote. In some cases, direct access as user âĂIJsystemâĂİ is possible.	All systems must be controlled if provided with latest patches. For verifying, for example, Microsoft Security Baseline Analyser could be used (MBSA).
DB2 Multiple high critical vulnerabilities	H	System access will be possible by exploiting one of the vulnerabilities.	Install all available updates provided by the vendor.
Multiple Oracle Vulnerabilities	H	All databases could be compromised, exploiting the vulnerable software.	Install all available updates provided by the vendor. All default passwords should be changed; if no password is set, a strong password should be set.
Old MS-Exchange is prone to Remote Buffer Overflow	H	This flaw can be used to completely crash Exchange 5.5, or to execute arbitrary code on Exchange 2000.	If no update is available, Exchange should be upgraded to latest version available.

Finding	Level	Impact	Recommendation
DB2admin with trivial password	H	Local user can escalate privileges by using DB account.	Default password should be changed to strong password. All passwords should be changed at least every 90 days.
DameWare Mini Remote Control Pre-Authentication Username Remote Overflow	H	An attacker could exploit this flaw by sending a specially crafted packet to the remote host. Successful exploitation of this vulnerability would result in remote code execution.	Upgrade to version 4.9.0.0 or later.
VNC Security Type Enforcement Failure Remote Authentication Bypass	H	Attacker can access VNC Server without authentication and thus control the server if a user is logged in.	Remove service if not needed. A screen saver with locking feature enabled and short timeout should be enabled on all servers.
FTP Server with Read and Write Access	M	Everyone (only access to network is necessary) can write and delete files or folders to these servers affected without authorisation.	Anonymous access to all FTP servers should be disabled.
Multiple Tomcat vulnerabilities	M	The remote web server includes an example JSP application that fails to sanitise user-supplied input before using it to generate dynamic content in an error page. An unauthenticated remote attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser, to be executed within the security context of the affected site.	Either remove the Tomcat examples web application, use appropriate patch referenced in the vendor advisory, or upgrade to Tomcat 6.0.20 / 5.5.28 / 4.1.40 when they become available.

Finding	Level	Impact	Recommendation
OpenSSL Multiple Vulnerabilities	M	An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks.	Update to the latest OpenSSL version.
DNS Server Zone Transfer Information Disclosure (AXFR)	M	A zone transfer lets a remote attacker instantly populate a list of potential targets. In addition, companies often use a naming convention that can give hints as to a serverâĂŹs primary application (for instance, proxy.example.com, payroll.example.com, b2b.example.com, etc.). As such, this information is of great use to an attacker, e-Government may use it to gain information about the topology of the network and spot new targets.	Limit DNS zone transfers to only the servers that need the information.
Windows Remote Desktop Protocol Server Man in the Middle Weakness	M	An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.	Use TLS encryption for the RDP session.
Unsupported, outdated AIX	M	Updates and security fixes are no longer available.	Update to newer version should be done as soon as possible.
Finger	M	An attacker could get information about systems and valid usernames, and their usage frequency, without being authorised.	Disable finger service.

Finding	Level	Impact	Recommendation
SNMP Access with known community strings	M	Everyone with network access can at least read vital system information. Where write access is enabled on "private" community string, system configuration can be changed remotely effectively without authentication.	Where SNMP service is enabled, other community strings than "public" or "private" should be used. Where SNMP write access is not absolutely needed, it should be disabled as SNMP authentication is cleartext and easily brute-forced in SNMP v1 and v2.
Multiple SSL vulnerabilities	M	User cannot use encryption anymore (for expired certificates). Weak algorithms (SSLv2) and ciphers (Anonymous, export, DES, RC*, MD5). Can be broken trivially or with moderate effort.	As for the expired certificate: purchase or generate a new SSL certificate to replace the existing one. Disable all weak ciphers and protocols.
MS-SQL administrator account "sa" with password "sa"	M	Even if a remote connection to system using MSSQL connection is not possible, any local user will be granted full database administrator access.	Change default password to strong password.
HTTP TRACE / TRACK Methods Allowed	M	TRACE and TRACK are HTTP methods that are used to debug web server connections. As they mirror the request provided, they can be misused for XSS/CSRF attacks by circumventing the protective same-domain policy used for JavaScript.	Disable these methods.
NFS Vulnerabilities	M	Data stored in these files can be downloaded without information, probably leaking data or giving away information about infrastructure and configuration of the database.	The NFS share should be disabled or at least limited to the client IP addresses needed.

Finding	Level	Impact	Recommendation
Multiple Mail Server EXPN/VRFY Information Disclosure	M	The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account. Your mailer should not allow remote users to use any of these commands, because it gives them too much information.	On Sendmail, add the option: O PrivacyOptions=goaway in /etc/sendmail.cf.
HP Ignite-UX TFTP File Access Information Disclosure	M	The remote host has a TFTP server installed that is serving one or more HP Ignite-UX files. These files may contain sensitive information. A remote attacker could use this information to mount further attacks.	Disable the TFTP service if it is not being used. Otherwise, restrict access to trusted sources only.
Sendmail Redirection Relaying Allowed	M	The remote MTA is vulnerable to a redirection attack. That is, if a mail is sent to: user@hostname1@victim Then the remote SMTP server (victim) will send the mail to: user@hostname1 Using this flaw, an attacker may route a message through your firewall, in order to exploit other SMTP servers that cannot be reached from the outside.	In sendmail.cf, at the top of ruleset 98, in /etc/sendmail.cf, insert the following statement: R$$$ $#error $ 5.7.1 $: '551 Sorry, no redirections.'
RPC rusers Remote Information Disclosure	M	It provides attacker interesting information, such as how often the system is being used, the names of the users, etc. Using rusers, we could determine that the following users are logged in: oracle (pts/4) from 172.17.2.157 oracle (pts/2) from 172.17.2.157	Disable this service if not needed.

Finding	Level	Impact	Recommendation
Accessing File Server over Null Session, showing user or services	M	An attacker can gain valuable knowledge enabling further attacks.	Login without credential should be disabled, see e.g. http://support.microsoft.com/support/kb/articles /Q143/4/74.ASP http://support.microsoft.com/support/kb/articles /Q246/2/61.ASP
LDAP anonymous access	M	This allows information to be retrieved without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user may be able to query your LDAP server.	If the remote LDAP server supports a version of the LDAP protocol before v3, consider whether to disable NULL BASE queries on your LDAP server.
pam_ssh Login Prompt Remote Username Enumeration	M	The remote host is running a SSH server that responds differently to login attempts depending on whether or not a valid username is given. This is likely due to a vulnerable version of pam_ssh. A remote attacker could use this to enumerate valid usernames, which could be used to mount further attacks.	Install fixed version of pam_ssh.
MTA Open Mail Relaying Allowed	M	Mails can be sent as arbitrary user without authentication.	Reconfigure your SMTP server so that it cannot be used as a relay any more.
SSH Protocol 1 supported	M	The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe, so they should not be used.	Disable compatibility with version 1 of the protocol.

Finding	Level	Impact	Recommendation
TFTP Traversal Arbitrary File Access	M	The TFTP (Trivial File Transfer Protocol) server running on the remote host is vulnerable to a directory traversal attack that allows an attacker to read arbitrary files on the remote host, by pretending their names with directory traversal sequences. ("pretending their names" DOESN'T SEEM TO MAKE SENSE)	Disable the TFTP service if it is not being used. Otherwise, restrict access to trusted sources only.
Multiple Web Server Vulnerabilities.	M	The remote web server is vulnerable to a cross-site scripting attack. The remote web server fails to sanitise the contents of an 'Expect' request header before using it to generate dynamic web content. An unauthenticated remote attacker may be able to leverage this issue to launch cross-site scripting attacks against the affected service, perhaps through specially- crafted ShockWave (SWF) files.	Check with the vendor for an update to the web server. For Apache, the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2; for IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1; for IBM WebSphere Application Server, upgrade to 5.1.1.17.
Central RZ switches trivial DoS	H	It is possible to DoS the complete central UAE e-Government data center without authentication or much effort, even accidentally (as was the case when the network scan started).	The two instable (OR âĂIJunstableâĂİ?) switches should be replaced with the two replacement models which already were ordered and are in store, awaiting exchange since autumn 2009.

Finding	Level	Impact	Recommendation
Multiple Cisco IOS remote exploits	H	An attacker may exploit one of the vulnerabilities in old IOS firmware, trying to crash the remote device or to execute arbitrary code remotely.	The systems should be updated to current firmware. A patch management for network devices should be established.
Sybase ASA Client Connection Broadcast Remote Information Disclosure	M	The remote Sybase SQL Anywhere / Adaptive Server Anywhere database is configured to listen for client connection broadcasts, which allows an attacker to see the name and port that the Sybase SQL Anywhere / Adaptive Server Anywhere server is running on.	Switch off broadcast listening via the '-sb' switch when starting Sybase.
Different software versions on network devices	M	Unstable release might crash systems. The huge variety of different software version makes it more difficult for administration. A patch management process for network devices should be established.	Only stable releases of Firmware or Software should be used in production environment. The official recommendation of Cisco is to use stable maintenance releases as soon as they are available.
Incomplete firewall rule process & documentation	M	It is practically impossible to perform a nominal/actual comparison, as only a small subset of nominal rules is available. It is not possible to tell whether the existing rule base contains rules unapproved or no longer needed.	As the firewall permissions are required to be restricted to a strict as-needed base, all needed connections should be documented accordingly.

Finding	Level	Impact	Recommendation
Impractical references to/from firewall rule documentation	L	It is unnecessarily hard to perform an actual/nominal comparison, to review rule sets (and, e.g., find orphaned rules) or to assign responsibility for firewall rules.	It is more practical to express changes to existing rule sets (adding/removing servers from the same application) as changes of existing Network Access Forms, than to add change request upon change request to the original one. It makes comparison and status reviews much easier. A simple numbering scheme for forms and consistent documentation of these numbers in the configuration can greatly enhance searching for references.
Misleading object names	L	The rule sets are unnecessarily hard to read and understand, which can lead to misunderstandings and security risks.	Groups should be used to group applications and service specific services or servers in a way that enhances a fast understanding of the rules. (GROUPS USED TO GROUP? AND TO SERVICE SERVICES? SEEMS ODD)
Long connection timeouts allow resource exhaustion	L	Long session timings can lead to resource exhaustion if many connections are opened but not properly closed again (e.g. by network disconnection).	The firewalls' connection resources should be monitored for possible exhaustion. If problems are detected, the timings should be adjusted accordingly.
Low limit for DNS fixup	L	DNS-TCP answers are not completely covered by this limit on the DNS fixup. This is especially true for TXT-records or DNSSEC-related answers (see, e.g., RfC 3226 section 2.3 for discussion).	Set message-length maximum to 4000 as recommended in RfC 3226, section 3.
Unused WLAN access points with weak encryption	L	If used, the WPA-TKIP encryption can be broken in moderate time using readily available tools, like AIRCRACK-NG (tkiptun-ng).	The WLAN should either be shut down or updated/reconfigured to use WPA2 (with a strong PSK or certificate).

Finding	Level	Impact	Recommendation
The firewall is not filtering any packets	H	While there is a firewall, it does not filter any traffic (except for a small, one-digit number of systems). The firewall protects neither internal nor external systems from unwanted network traffic.	A valid firewall rule set should be constructed from the ground up with a default- deny rule, allowing only the necessary, approved network traffic.
Firewall firmware not current	L	There may be bugs in the older version that might impact security of the system. Unfortunately the release documentation was not available to the testers, thus the impact cannot be properly estimated.	It should be tested whether a more current version is available and whether critical bug fixes or recommend an update (Cisco support contract needed).
Default inter-interface rule allows unrestricted VPN ==> VPN traffic	M	Traffic between the VPN partners is not restricted. The UAE e-Government -VPN-ASA is working as non-filtering proxy between them. Even if this may expose VPN partners against each other, the risk is set to âĂIJMediumâĂİ as they can probably filter on their own VPN devices. (NOT âĂIJexpose against each otherâĂİ. âĂIJexpose to each otherâĂİ OR âĂIJpit against each otherâĂŹ?) Additionally this poses no direct risk to the UAE e-Government (only to their partners).	If network traffic between VPNs is needed, it is better to explicitly allow the needed traffic with explicit filtering rules. Disable the default behaviour with no same-security-traffic permit inter-interface
OSPF enabled on Firewall	M	External systems can force routing changes into the firewall, with the possibility of redirecting or breaking traffic.	OSPF should be disabled on a firewall, and static routing should be used instead.

Finding	Level	Impact	Recommendation
Weak and re-used VPN Pre-Shared Secrets	M	At least two VPNs can trivially be broken by dictionary attacks against the guessable PSK. In the event that the PSK becomes known publicly, all VPNs must be changed, and similarly when one partner leaves. Considered "Medium" as the VPN is being used via a restricted network not connected to the internet.	Individual, strictly nontrivial passphrases should be used as PSKs. All VPNs should be migrated to using such individual, strong PSKs.
Unrestricted outgoing traffic for dedicated network	M	As there is no requirement document, it cannot be judged whether unrestricted access into all other networks is intended or needed. Completely unrestricted access usually is an indication for missing analysis of needs and risks.	The traffic should be limited to protocols and targets needed.
Incoming traffic without source limitation	M	The services on the servers "ven" are accessible from any (even outside) network.	The traffic should be limited to the source servers and networks needed.
Old temporary firewall rules	L	Handling and disabling of temporary firewall rules does not seem to be working properly.	For the rules given, the need should be checked. Rules needed no longer should be disabled.Enabling and disabling firewall rules should be handled via a proper rule management process.
Outdated ASDM version	L	An outdated version of the firewall management web interface is currently installed.	Before ever enabling the web console, the ASDM should be updated to a current version.
Actively used WLAN with weak encryption	M	The WPA-TKIP encryption can be broken in moderate time using readily available tools, like AIRCRACK-NG (tkiptun-ng).	The WLAN should either be shut down or updated/reconfigured to use WPA2 (with a strong PSK or certificate).

7.6 Conclusion

Penetration testing plays an important role in information security management, by identifying the weaknesses of the whole management system, from technical to organisational or personnel vulnerabilities. Almost all security management is about the access controls of information, and penetration tests check the gatekeepers of the management system of an organisation, logically or physically, where they help the organisation to have a secured zone concept. There are many aspects relevant to the penetration test, of which the most important are networks, applications, physical environments and infrastructures. Both theoretically and practically, many different techniques and styles of penetration tests exist in the market, but they all serve the same objectives for the organisation applying them. The final goal of the penetration test is to improve the security management; in order to achieve this goal, different tools and techniques should be implemented to find out the deficit of security protection, and the result of the penetration test is the starting point for security management improvement.

The organisation benefited from the test, as it was able to use our recommendation to improve the information security of the department being tested. There is a plan to repeat the test in the near future on the same environment, to ensure that all the vulnerabilities discovered are eliminated and to find out whether there are any new vulnerabilities in the system. The government is planning to carry out this test in other departments, to ensure the security of the network.

Chapter 8

Evaluation of e-Government Information Security Culture

8.1 Introduction

Controlling the spread of information has been essential to the provision of all kinds of human security since the dawn of civilisation. The dissemination of information is essential for organisations of any scale to function effectively, yet at the boundaries there has always been the need to prevent the dissemination of some information in order to safe guard an organisation from it's malicious use. Creating systems that allow efficient communication of secure information within an organisation yet preventing its leakage to the outside is a central challenge to organisation management.

Information security systems are a set of systems, policies and procedures put in place to protect information and ensure access to information is only available to sanctioned users of the system. Whilst hardware and software components are always essential in the safe-guarding access to digital information, in evaluating the security

of an information system is it essential to consider the behaviour of human users e-Government form an integral component of the system. The information security culture of an organisation reflects the set of behaviours of human operators where these behaviours may impact on the security of an organisations information.

In previous chapters a full analysis explored different aspects of security systems to discover how these might be improved. A Gap Analysis, Penetration Test and Risk Assessments were carried out in order to identify any vulnerability within the systems. Solutions to mitigate these were implemented. To complete a holistic analysis of organisations information security, in this chapter we address the final and arguably most challenging yet important aspect of organisational information security, namely evaluating the organisations information security culture.

8.2 Information Security Culture

As information technology has progressed from paper based to digital systems the amount of information being managed by organisations, as well as the need to secure it, continues to rise exponentially. Despite the huge amount of work that has been done to create secure hardware and software systems, the behaviour of human users; the user's culture is much less readily altered. Any information security system layer is only as strong as its weakest component and very often it is the behaviour of human operators that represent the weakest part. When an individual's behaviour does not adhere to the security policies abject weaknesses in security are created. Whilst a strong set of policies and practices is therefore essential to the information security of an organisation, they are not in themselves sufficient and it is only when these practices have be adopted and permeated deeply in to the organisations information security

culture that organisations information may be considered secure.

Government is the administration of a society and to be effective it needs to have information which malicious members of society cannot utilise to the detriment of society. To be more effective, governments have adopted digital information systems, the e-Government, to deliver administrative services to society via digital networks. e-Government enables digital interaction and information transfer between citizens, business, and public sector organisations. The majority of national governments have introduced some form of e-Government program ranging from a minimal informational web system to advanced implementations providing a suite of interactive services of ever increasing sophistication and scope. Improving the efficiency, accessibility and effectiveness of public service delivery is a driving challenge of e-Government strategy the world over (105).

Though often intangible, the culture of an organisation can sometimes be its most valued resource, the final free variable in a global competitive marketplace that can lead to an organisation's success or downfall. Within the e-Government human users administer digital information systems and their behaviour is a key factor determining the information security of the e-Government. Whether positive or negative, we collectively term all behaviours, attitudes and perceptions of users with regard to information security as the information security culture of the organisation.

Generally, when working under a direct and readily perceivable physical threat, an organisation will respond by readily adopting a strong culture of security. In a militarised situation for instance, an organisation will install defences and adopt behaviours such as sentry duty so long as a threat is perceived. However as many economies rapidly transform into information-driven, knowledge-based economies, the types of primary threat change faster than the established security culture adapts. Prior to the in-

formation age, organisations would have stored their most valuable physical resources in a secure location such as a safe, and organisational workers would have adopted a culture which was well aware of the threats to this system. In the transition to information driven economies, many workers have yet to fully perceive the significant threats to their information resources and are yet to adopt a strong culture of information security (106).

There is a danger that information security policies may not be disregarded where they appear to be in conflict with social expectations of politeness or trust, in such cases an information security culture has yet to be fully adopted and is in conflict with traditional social culture. Social engineers will exploit these situations to maximum effect, leveraging the full weight of cultural expectation in order to shame, humiliate or extract sympathy from an organisation worker, so as to persuade them to depart from the correct information security policy (107). In some case workers may develop an attitude of resistance or deliberate disregard for security policies if they perceive them as being unnecessarily draconian, or feel they do not grant room for common sense or rational judgement on the part of the worker, or where they present an excessive overhead on their workload in order to comply. This situation can be very dangerous as it can become endemic. It is only when workers are educated as to the Information Security threats that are the motivation for security policies that they make every effort to follow the prescribed protocols leading to the adoption of a new working culture (108).

Chia et al (109) describe three types of relationship between the information security culture and general organisational culture, and the effectively correspond to three stages on improved information security that must be proceeded along in order for an organisation to have fully adopted an information secure culture. In the first stage any

information security culture is completely independent of the organisational culture, reflecting the fact that the general workers in an organisation have no awareness of information security. An improvement on this stage is when the information security culture can be considered a subculture of the organisation culture. In the second stage, some workers are aware of the information security and significantly management are beginning to understand it's importance. The final stage occurs when information security culture can be considered to be integral to and embedded within the organisational culture. At this stage, all members have an awareness of the information security and new members will quickly assimilate information security practices.

The UAE government has made a concerted effort to implement an ambitious e-Government strategy, which has seen it rise rapidly in the UN survey results (110) and be able to claim the most sophisticated e-Government services in the Arab and GCC worlds. Whilst UAE initiative have made considerable progress towards excellent e-Government implementation, previous work has identified some areas within the information security culture of organisations that requires some redress in order to guarantee a trouble free transition to a secure system (111). In order to go further and a become a global leader in e-Government the UAE must address certain aspects of it's organisational culture by fully transitioning to the final stage where information security culture is fully embedded within all government organisations.

8.3 Research Methodology

In order to evaluate organisational information security culture it becomes necessary to evaluate the differing attitudes, behaviours and perceptions among the organisations employees. To do this we develop a questionnaire to capture the opinions of the or-

ganisations employees. We first identify 8 different aspects into which we can loosely group attitudes, behaviours and perceptions, as shown in figure 8.1.

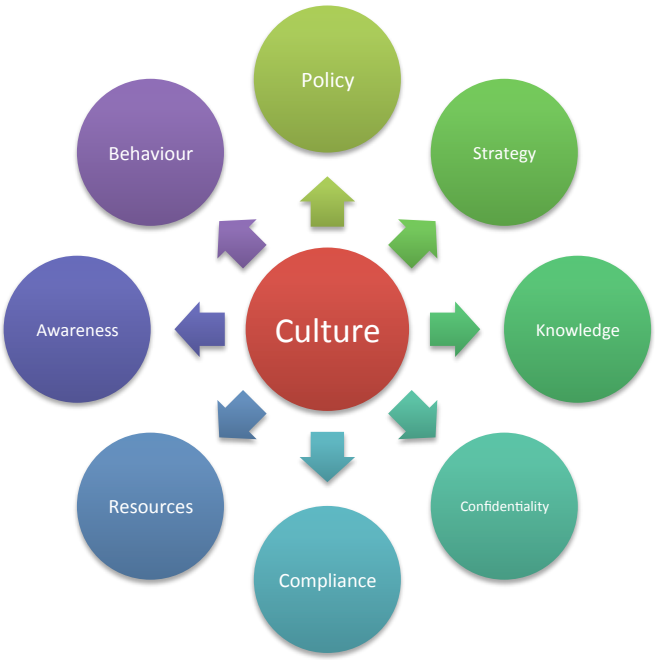

Figure 8.1: Information Security Culture Aspects.

For each aspect we chose a series of questions to be answered by a sample of the organisations workers. Answers to the questions were scored on a likert scale graded 1-5. For any question we take a score of 3 on the scale to be the minimum satisfactory score; a mean result below 3 from the sample indicates an area of significant concern. For each aspect we are able to produce an average mean across all questions providing a heuristic of the security of the organisations culture in this aspect. We describe each aspect and the associated questions in the section below.

8.3.1 Policy

The first step of establishing a robust government security environment is to define the policy, which is an essential part of security practices within organisation and can substantially influence organisational security. As Higgins (112) notes, " Without a policy, security practices will be developed without clear demarcation of objectives and responsibilities ". The organisation will face major difficulties when implementing ISM System. The primary objective of the information security policy is to define the users' rights and responsibilities regarding information within an organisation. Effective information security policies will help users understand what is acceptable and responsible behaviour regarding information resources and will assist in establishing a safe information environment (113). Policy is on the top of the management structure and plays the role of setting up the guiding principles for the rest of the organisation. Policy is also an essential part of leading people in an organisation. Clear policy defines roles and responsibilities of the team. Hence policy can also help in the efficiency of the operations of information security protections. Below is a list of questions used to address the organisation policy:

1. The organisation security policy covers all part and is complete.
2. The security policy needs to be modified completely.
3. There are formal and specific procedures to report security violations.
4. We have rules on how to report information security violations.
5. I know the person in charge of reporting cases of abuse or damages related to electronic resources of the organisation.

6. Attention and consideration of employees (Feedback) expressed by the staff are the best method to improve information security.

8.3.2 Strategy

After defining the policy, the security strategy should be selected to indicate the approach for government to reach their information security protection goals. There are many different ways to complete the tasks of security protection, an overall security strategy with many sub-strategies enables the organisation complete the security protection tasks effectively, efficiently, economically and then meet the strategic goals of information security. To define a strategy, an overall goal and strategic goals should be raised first by the management. The security strategy should align with the Policy toward the goals of government security management. The questions used to evaluate this section are listed below:

1. I know there exists an information security policy in my organisation.
2. Information security policy covers the goals and objectives of the organisation.
3. Information security policy covers all the information security previsions required within my department.
4. The security policy goals need substantial modification.
5. Information security policy covers and clarifies the duties and responsibilities of users efficiently.
6. Management involvement and participation of all staff and taking their suggestions ensures. optimal security deployment and application.

7. The management conduct periodical update of information security policy.

8.3.3 Knowledge

Knowledge is a corner stone of the successful administration of information systems. Understanding the technical nature of some information security issues require in depth knowledge of the relevant technology in order to understand how weaknesses can occur. In addition, users need to understand the deployed security technology, as well as be able to make risk assessments, risk treatments and implement the relevant information protection techniques. For e-Government the knowledge of security management must be acquired maintained and transferred to the security management teams. This knowledge may be acquired from external resources or researched and developed by the security team. 3rd parties, vendors of security solutions and the national security agencies may all provide knowledge. A knowledge management mechanism, database or tools should be implemented for better security management. The questions used to evaluate this section are listed below:

1. Information security is the confidentiality of information.

2. Information security is the integrity of information.

3. Information security is the availability of information as requested by the authorised person.

4. Employee training on the optimal use of his own tasks, especially in terms of security, reduces lots of risks and gaps, and eliminate professional and security related faults.

5. The training courses attended were enough to make use/provide the e-Services in secure.

6. I can make an important contribution to the improvement of information security and the observation of the confidentiality of customer data.

8.3.4 Confidentiality

Confidentiality of government information is the first priority of security management, it is important to the security management because most government information need to be protected to protect the rights of civilians or the operations of government. In order to keep a secure environment, Confidentiality should be defined and implemented by establishing policy, regulation and procedures. It regulates the government users to keep the information secure and should be base on, and supported by, the overall policy. The questions used to evaluate this section are listed below:

1. We have clear policies on how password in term of length and use must be handled.

2. Use of weak password or indifference to the protection of the password may endanger the safety and confidentiality of the contents and systems.

3. In case of subcontracting with a 3rd party company in charge of e-Government systems and devices maintenance, the safest way is to create a temporary account for them, and then delete it when contract finishes.

8.3.5 Compliance

Compliance helps an organisation to meet its internal and external requirements. For information security, the compliance process pushes the staff to follow the internal security management requirement and on the other hand, guiding the organisation to meet the legislation and regulation requirements. In a P-D-C-A cycle (the Deming Cycle of management), information security policy is established in the Plan stage and aims to be the top tier of guidance for the whole management system. Information security compliance utilises compliance checking in form of audits or reviews and checking to assure the planned policy and procedure of management system are all executed effectively, as well as the requirements that come from partners or governments. These two tools of management should be integrated and operated seamlessly to ensure an effective information security management.

Compliance processes help organisations compare their actual information security operations with international standards. Compliance evaluates and audits the difference between the expected standards of organisational situations, and the reality in the organisation. Evaluating the degree of compliance helps organisations determine their conformity to the controls listed in the standards, and delivers useful outputs to the certification process for the next stage of certification (70). Compliance with internationally recognised standards is growing in importance, because it has become popular as a common basis for information security measurement. The questions used to evaluate this section are listed below:

1. The management is committed to comply with information security policy.

2. My organisation does enough to implement information security.

3. Staff are totally committed to achieve the organisation's information security goals.

4. I adhere literally to the policy in working to achieve the goals of the organisation information security policy.

5. I know where to find the relevant information security policies, standards and guidelines.

6. The user is responsible about maintaining own user name and password.

7. In case of doubt that there is a leakage of the password or viewed by others I do immediately change it.

8. It is not a good practise to give your password to colleagues to speed up the response.

9. There are consequences when I don't adhere to our information security instructions.

8.3.6 Resources

In implementing it's security strategy a organisation will always be ultimately limited by the resources that are available. Appropriate policies cannot be implemented where resources are available and insufficient resources can represent a critical flaw in an organisations security. Security resources maybe physical hardware such as firewalls or network switches, or they may software, staff or financial resources. As resources are always ultimately limited, an organisation will always need to prioritise in order to achieve the most cost effective approach to security. Purchasing, for instance, the latest

network hardware may not be an effective use of the available financial resources if there are staff e-Government are insufficiently trained constituting a much more serious security weakness. The questions used to evaluate this section are listed below:

1. The number of current technical staff is sufficient to address any security issue.
2. Individuals and technical staff were prepared and made aware of security threats and risks they may face.
3. Problems concerning information security in our organisation are always solved at their roots.

8.3.7 Awareness

A rigorous and comprehensive information security policy is only of real value when it is correctly implemented by all staff. The staff can only be expected to follow the policy if they are aware off it, otherwise their behaviour will only be governed by their personal interpretation of appropriate behaviour. For this reason we attempt to measure this awareness by attempting to quantify the degree to which workers are aware of the policy and also of the general importance of information security as a whole. The questions used to evaluate this section are listed below:

1. I have/keep a copy of information security policy.
2. I have full knowledge of the security policy requirements within my department.
3. Information security is relevant to business and not only a technical function.
4. The user is solely responsible for the safety of the devices used by him.

5. Lack of information security training would NOT be an excuse for me to avoid taking. responsibility and accountability in case of any security breach or leakage.

8.3.8 Behaviour

We term the employees' perceptions and attitudes, value and behaviour regarding information systems. Behaviour measures the collective values, norms and security awareness of users. In some case workers may develop an attitude of disregard for security policies if they perceive them as being unnecessarily draconian, or feel they do not grant room for common sense or rational judgement on the part of the worker, or where they present an excessive overhead on an employee's workload. It is only when workers are educated as to the information security threats that are the motivation for security policies that they make every effort to follow the prescribed protocols, which leads to the adoption of this new working culture (114). The questions used to evaluate this section are listed below:

1. I DO report to security authorised personal for security violation by colleagues /staff within my department.

2. The security policies are strictly implemented without any exceptions.

3. The computer and electronic communications systems should be used for UAE's business activities only use work equipment to perform. personal use, such as sending personal email or send SMS or access to news.

4. Under no circumstances, for example not even when I am away on vacation, am I allowed to pass my password on to someone else. If necessary, password can

be given over the phone to information security officer to measure its strength.

5. In case of subcontracting with a 3rd party company in charge of e-Government systems and devices maintenance, the safest way is to create a temporary account for them, and then delete it when contract finishes.

8.4 Results

To evaluate an organisation information security culture, the entire population needs to be included in the audit process. The population can be seen as all employees e-Government are working in the organisation and have access to its information. This is necessary since the culture of one office to the next and one department to the next could be different. By getting all employees to participate, comparisons can be made between offices, departments and job levels. It is often unrealistic to involve all employees if the organisation has a large workforce, in which case a sample that is representative of the overall workforce demographic can then be used to participate in the audit. In this study four sectors of UAE e-Government were chosen, and 71 employees participated in the survey. This represents 30% of the work force within that department [5]. To ensure confidentiality, the questionnaires were answered anonymously, employees feel more confident giving honest and accurate opinions if they know they cannot be identified. The first section of the survey was developed to gather the participant demographic data relation to their position within the organisation. The majority of the respondents were consultants 39.4% and management 31.4%, as shown in figure 8.2.

Having gathered the survey results, the next step was to apply statistical analysis to identify trends in the employee's perceptions. We examine the survey results from

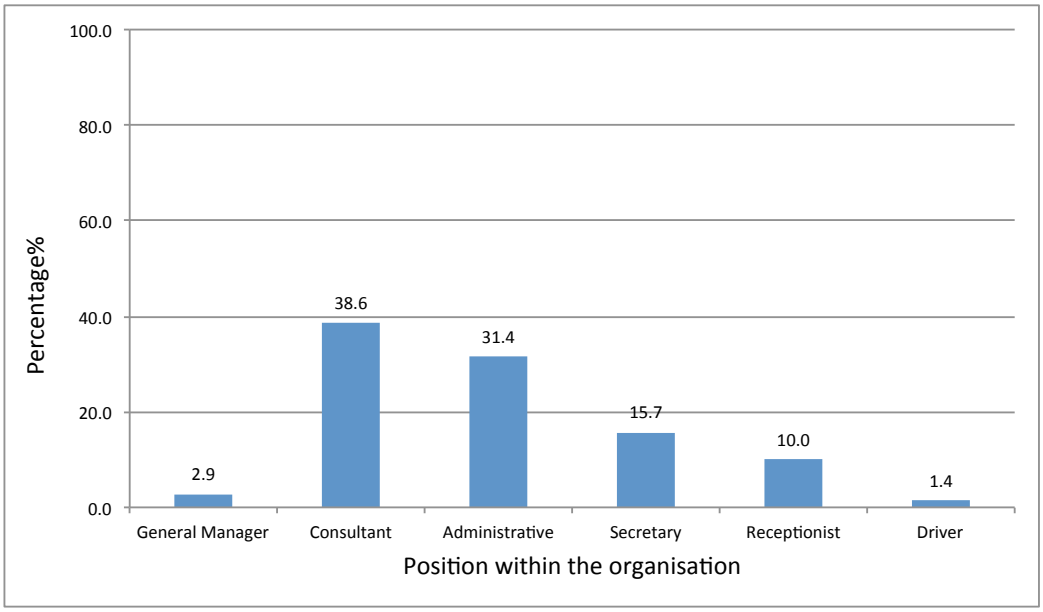

Figure 8.2: Demographic Data.

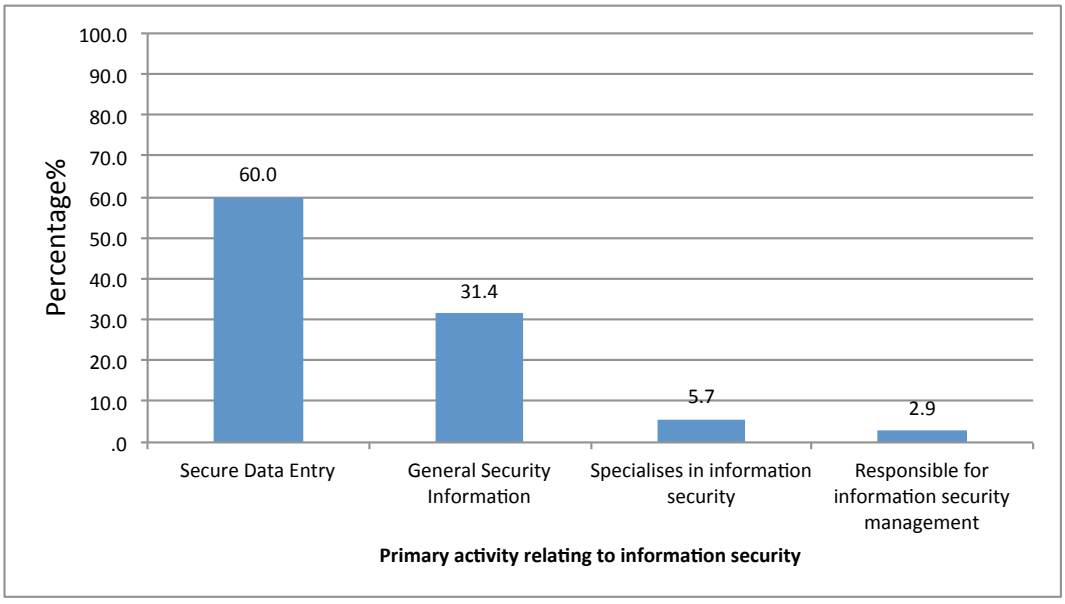

Figure 8.3: Field of Work.

each aspect individually and produce a table of results with the mean Likert score for each question along with the standard deviation of the results. Table 8.1 shows the results from the question on policy. It can be seen that all questions have a mean score

above of 3, implying that overall trend is towards the right side of the scale (good practice). However for a high degree of information security a target mean of 4 is required, this is to ensure that participant responses of 'uncertain' is not sufficient for a secure information security culture. This implies that some work is required to improve the information security policy and employee attitudes towards it.

Table 8.1: Policy Analysis

Question No.	Mean	STD
1	3.19	0.692
2	3.03	0.602
3	3.36	0.95
4	3.00	0.7588
5	3.51	0.901
6	3.34	1.141

Table 8.2 shows the results from the questions on strategy. It can be see that all questions have a mean score above of 3, with one question scoring above 4 (management listen to employee suggestion for improvement). Overall the scores are higher than those for policy however there is still work to do to obtain a target mean of 4 as required.

Table 8.2: Strategy Analysis

Question No.	Mean	STD
1	3.72	0.873
2	3.4	0.71
3	3.42	0.695
4	3.14	0.772
5	3.37	0.82
6	4.06	0.961
7	3.29	1.105

Table 8.3 shows the results from the questions on knowledge. It can be seen that almost all questions have a mean score above 4 indicating a strong information security

culture in this aspect. However one question scored and average below 3, this question concerned the provision of training courses pertaining to the use of secure systems where many participants felt these were insufficient. This issue requires urgent attentions from the organisations management, regular employee training programmes are essential to sustaining a culture of information security. During the course of this research an intervention was carried out to deliver information security training to 1500 employees within the UAE e-Government. We will discuss this further, later in this chapter.

Table 8.3: Knowledge Analysis

Question No.	Mean	STD
1	4.4	0.875
2	4.09	1.025
3	4.00	1.007
4	4.49	0.756
5	2.93	1.146
6	4.11	0.860

Table 8.4 shows the results from the questions on confidentiality. Here again all questions scored above 3 and the majority above 4 indicating over all a good culture of security relating to confidentially with one area (question 1, password policy) requiring some work to bring the question's mean score above 4. This matter is addressed in the next chapter where a comprehensive security policy is developed which includes a policy on passwords.

Table 8.4: Confidentiality Analysis

Question No.	Mean	STD
1	3.54	1.183
2	4.47	0.775
3	4.13	0.916

Table 8.5 shows the results from the questions on compliance. Here again all questions had a mean score above 3 and almost half above 4. This indicated that some good work on compliance is being done by individual departments, however there is still some work to be done in some areas to bring all questions up above 4 and achieve a strong culture with regard to compliance.

Table 8.5: Compliance Analysis

Question No.	Mean	STD
1	3.50	0.812
2	3.47	0.812
3	3.23	0.904
4	3.39	0.889
5	4.23	0.618
6	4.63	0.641
7	4.23	0.843
8	4.59	0.691
9	3.23	0.731

Table 8.6 shows the results from the questions on resources. The questions on the aspect reveal that there are issue related to employee perceptions of the available resources to support the information security. Two thirds of the questions scored less than 3, these indicate that staff perceive that there are insufficient technicians and engineers to deal with security concerns and that this results in security issues not being able to be tackled at their root cause. The suggestion here is there is a perception that that technical staff are always 'fire fighting' current issues without resources to build a comprehensive secure system. Part of this research is to address the issues relating to network security, infrastructure and communications security which we do through gap analysis and penetration and asset management tests described earlier in this thesis. These results improve the overall security of the information networks and also free up technical resources, allowing engineers to regain the upper hand in delivering

information security assurance.

Table 8.6: Resources Analysis

Question No.	Mean	STD
1	2.59	1.014
2	3.39	0.997
3	2.91	1.095

Table 8.7 shows the results from the questions on awareness. More than half the questions had a mean score below 3 indicating significant concern needs to be raised over these areas. In general there was a lack of awareness found over the information security policy with some staff feeling that information security was not their concern. The perception being that individual departments have their own sets of practices on security and there is a lack of an overarching policy for all departments. This issue will be addressed later in chapter 8 where a compressive e-Government policy is developed. Once this implemented the management is required to deliver training programmes to communicate the policy to employees and assure it is integrated into their working practices.

Table 8.7: Awareness Analysis

Question No.	Mean	STD
1	2.90	1.032
2	3.12	0.844
3	2.89	1.378
4	3.78	1.211
5	2.96	1.27

Table 8.8 shows the results from the questions on employee behaviour. Here the results were mixed with one area scoring above 4 however two questions scored below 3 indicating a significant problem around the use of the staff use of IT equipment for non-work purposes and the sharing of passwords with other users. Both of these

require immediate attention, again this should be addressed through the recommended training programme.

Table 8.8: Behaviour Analysis

Question No.	Mean	STD
1	3.12	0.856
2	4.11	0.956
3	2.71	1.33
4	2.45	1.243
5	3.06	1.475

To assess the information security perception of the employees by each area under study, the average mean for each area was plotted against the accepted threshold of 4. Figure 8.4 shows the results and it is obvious that the organisation employees respond to an acceptable level with regards to knowledge and confidentiality. While the other factors fell short. Weaknesses in behaviour and awareness could be addressed by provisioning more training and employee education, whereas policy and strategy aspects are a managerial issue requiring the implementation of a comprehensive security policy and rolling out across all departments. A programme of continual penetration testing will identify any vulnerability within the information systems and these could be readily strengthened by applying financial resources.

The answers were also interpreted by considering the categories strongly agree and agree as positive outcomes. While unsure, disagree and strongly disagree were categorized as negative outcomes "or areas for development". The 'Uncertain' response is considered as a negative, or area that needs to be developed, because the employees e-Government are unsure about an information security procedure cannot be said to be fully aware of the information security policy. The threshold of 60% of the samples giving a positive response to a question was chosen as an acceptable level.

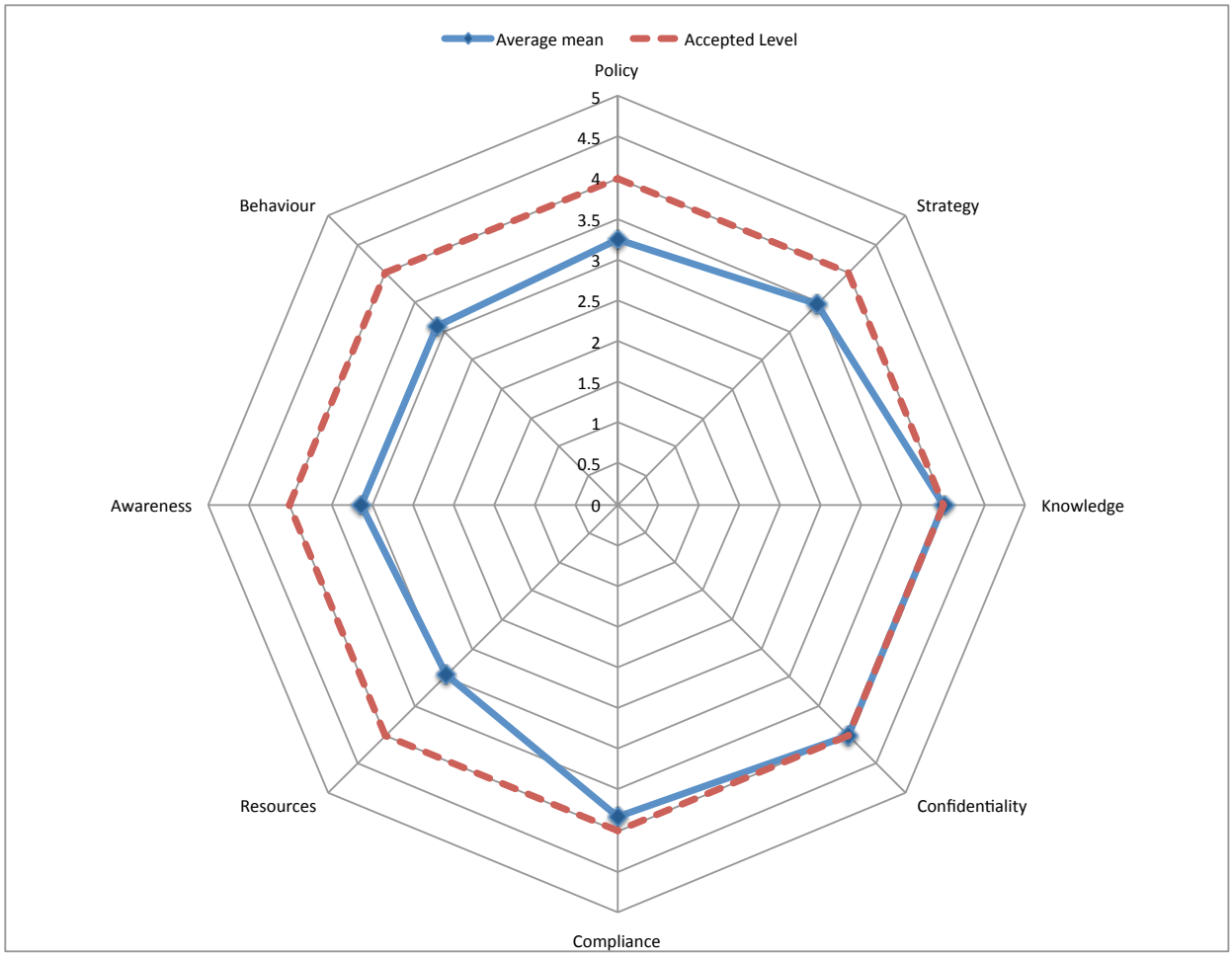

Figure 8.4: Questionnaire result vs. Agreed Acceptable Level.

Figure 8.5 shows the results from the question on policy. While there is room for improvement in all areas as none of the questions score above the acceptance threshold of 60%, there is considerable concern regarding questions 2 and 4 which relate to the quality of the Policy and system of reporting violations. Both of these concerns will be addressed in the next chapter.

Figure 8.6 shows the results from the questions on strategy. Question 7 stands apart with a widespread positive response indicating the management engage closely with the staff and take their suggestions seriously at the individual level, however the very

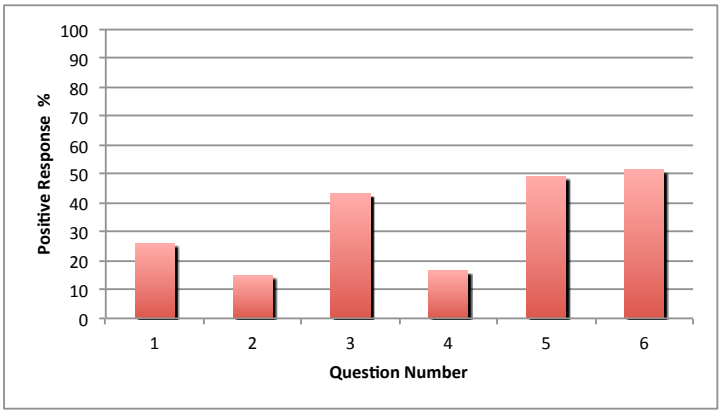

Figure 8.5: Policy Aspect Positive Response.

low positive response to question 5 indicate again that work is required to improve the security Policy, with the response to the next lowest question, question 8, indicating that employees are aware of the work management needs to do to improve it. Weakness in the other remaining areas can also be traced to weaknesses in the policy.

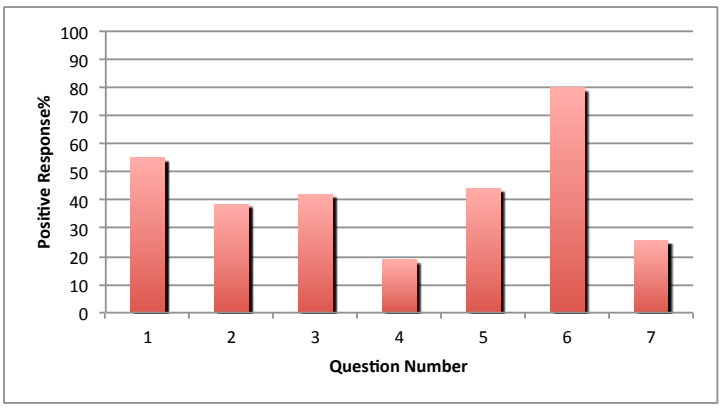

Figure 8.6: Strategy Aspect Positive Response.

Figure 8.7 shows the results from the knowledge aspect. Overall all this aspect scored exceedingly well with only one area,the lack of adequate training provision being of concern. This are should be addressed with urgency as already mentioned.

Figure 8.8 shows the results on the confidentiality aspect. Here only question 1

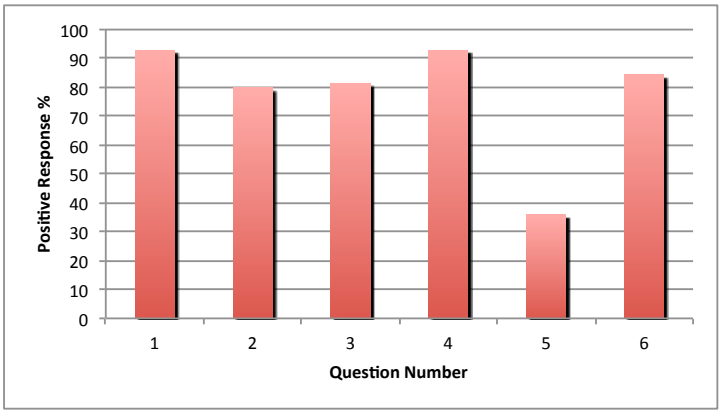

Figure 8.7: Knowledge Aspect Positive Response.

falls slightly short of our goal of 60% positive responses. This area concerns the guidance on using passwords and is dealt with through the security policy and subsequent training recommended for adoption in the next chapter.

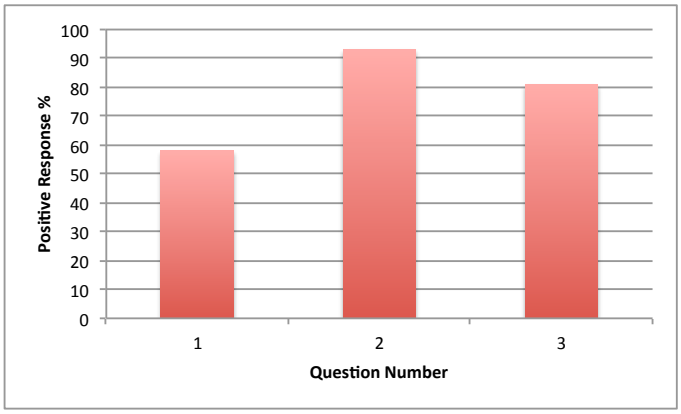

Figure 8.8: Confidentiality Aspect Positive Response.

Figure 8.9 shows the results on the compliance aspect. Here the response is split, the first 4 questions fared badly with weakness identified in how management comply with the policy and the over commitment of individual employees to complying with the policy and guidelines. Here again it is likely that the underlying cause of these issues is the lack of a single coherent policy across all departments. On the positive

side, questions 5-8 scored very well with all 90% and above positive responses. This implies the employees are broadly aware of the practices around password maintenance and incident reporting. Finally, question 9 raises a significant alarm with almost all respondents answering negatively, indicating that employee perceives no significant consequences to any departures they may make from the security guidelines. This issue is being addressed through the introduction of the policy, training and the proposed legal commitment on behalf of the employee towards maintaining the policy.

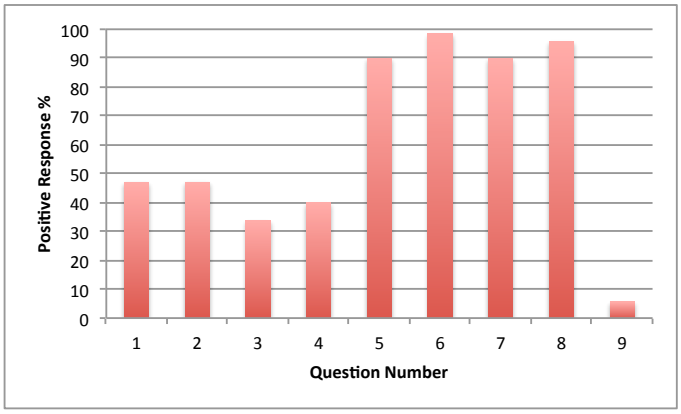

Figure 8.9: Compliance Aspect Positive Response.

Figure 8.10 shows the results on the resources aspect. Here all questions fall slightly short of our goal of 60% positive responses. Regular penetration test, with the resulting prescribed improvements being continually implemented. This will help to reduce the number of vulnerabilities within the system as well as reduce the load on the technical staff allowing them to concentrate on maintaining a high level awareness of the overall integrity of the system and be aware of any emerging vulnerabilities.

Figure 8.11 shows the results on the awareness aspect. Here 4 out of 5 questions fall short of 60%. Indicating training is required to improve the awareness of employees. Specifically awareness of the policy proposed in chapter 9 can be improved through

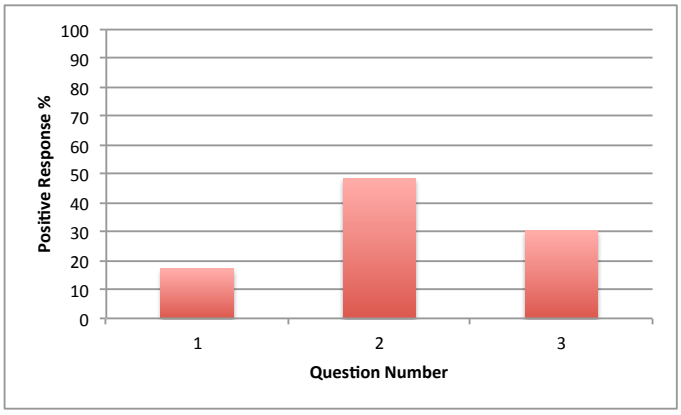

Figure 8.10: Resources Aspect Positive Response.

regular training for all employees. The high positive response to question 4 indicates that staffs already have a culture of taking responsibility for the security of devices they use.

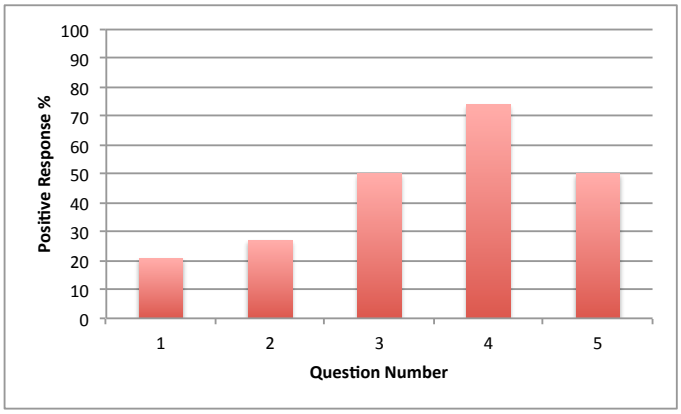

Figure 8.11: Awareness Aspect Positive Response.

Figure 8.12 shows the results on the behaviour aspect. Here questions 1 and 5 indicate the area of most concern, they indicate that some employers may not be willing to, or understand the procedure for, reporting violations by colleagues. To address this is workers must be educated as to the danger to the organisation in failing to report security violations and mechanisms must be put in place to safeguard whistle blowers

(115). In addition, there may be some weakness concerning the password provision to third parties. Question 3 all comes up slightly below the threshold indicating some staff may be using equipment inappropriately for personal use. The remedy to these issues represents the solution to improving scores in across all aspects, namely the provision of a bespoke training course for all workers regarding the policy and procedures of information security and the motivations behind them; as part of these training workers should be made aware of the ramifications and application of the organisations security policy to their department. Whilst it is important not to degrade the feeling of camaraderie between workers, failure of workers to report significant violations of the security policy can represent a serious security flaw and this should be emphasised.

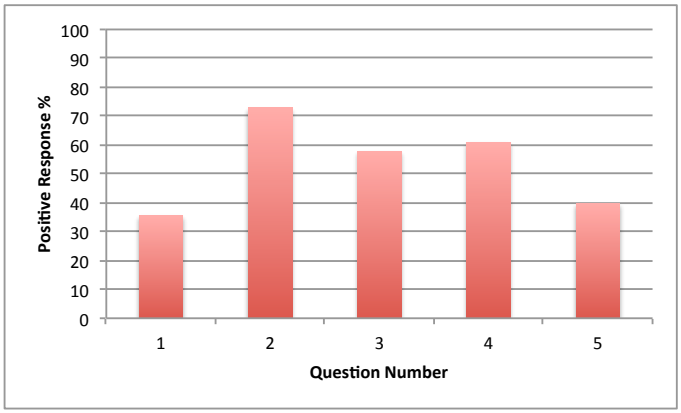

Figure 8.12: Behaviour Aspect Positive Response.

8.5 Awareness Training

Any information system is only as secure as it weakest component. All too often the weakest link is the one that is hardest to standardise, the human element. Whenever an employee departs from the security policy there is a potential vulnerability. Through the survey we have identified a number of areas where the survey indicates a weakness

in some employee's security awareness. In order to improve security culture throughout the organisation, the awareness issue goes well beyond simply informing employees of their security obligations. To overcome the inevitable change resistance or inertia, employees have to be both informed and motivated to modify their behaviours, to think security and act securely (116), (117). Conventional education on the security policy may have some benefit in improving security awareness of employees, however practical hands on applied training has a much higher chance on delivering benefits as it can help the trainee understand by providing a real life contextual situation. To ensure the maximum benefit of this type of training it should be repeated regularly, this will ensure the training has maximum impact on individuals and also that new employee will be regularly trained.

As result of our questionnaire, it was decided to develop information security awareness training course for the UAE e-Government employees. We constructed a full one day practical training course in security awareness and delivered it to 1500 employee participants over six sessions across Dubai, Abu Dhabi and Ajman and on average each session has of 250 participants. For three of the sessions we gave the participants a test to measure their security awareness prior to training. For the other three sessions we gave the participants the security awareness test after the training session. We can then compare the results to assess the impact of the training on the participant's awareness. The test was conducted asking the participants to identify security weaknesses present in a photo of an office shown in Figure 8.13.

We divide the weakness into 3 different categories:

Items left on Desk

- Day planner left on the desk.

Figure 8.13: The Clean Desk Test.

- Notebook left on the desk.
- Bank statement left on the desk.
- Check book left on the desk.
- Mail left on the desk.
- Briefcase left open near the desk.
- Cell phone left on the desk.
- Keys left on the desk.
- PDA left on the desk.
- Building access card left on the desk.

Items relating to the PC workstation

- Applications left open on the computer.
- CD left in the computer.
- Passwords on sticky note hidden under the keyboard.
- Printouts left in printer.

Other items around the office

- File cabinet drawer open.
- Key left in lock.
- Trash bin contains loose-leaf paper.
- Bookshelf contains binders with sensitive information.
- Desk positioned so its partially exposed to window or view from the hallway.
- Whiteboard with sensitive data on it visible from hallway or window.

The results show that our intervention was able to have a significant impact on employee security awareness, suggesting that a policy of continuous training is able to make improvements in an organisations information security culture, raise awareness of the organisations information security policy and best practices. Continuous training also means that new staff will be inducted into understanding the security policy at regular interval. The organisation will also be able to specifically train for any emergent weakness that may be identified. New technical and non-technical vulnerabilities, such as emergent social engineering behaviour can also be mitigated in this way.

Figure 8.14 shows the results for Items left on desk questions with the scores from the participants took the test before training shown side by side with those who took the test after the training. Clearly there is a marked improvement in the trainee's awareness gained through the training. Pre-training there are some significant areas of concern, however post training all items are identified by at least 50% of the participants. Some items are significantly more difficult for participants to correctly identify, and repeat training is recommend to ensure all participants successfully identify the majority of the weaknesses.

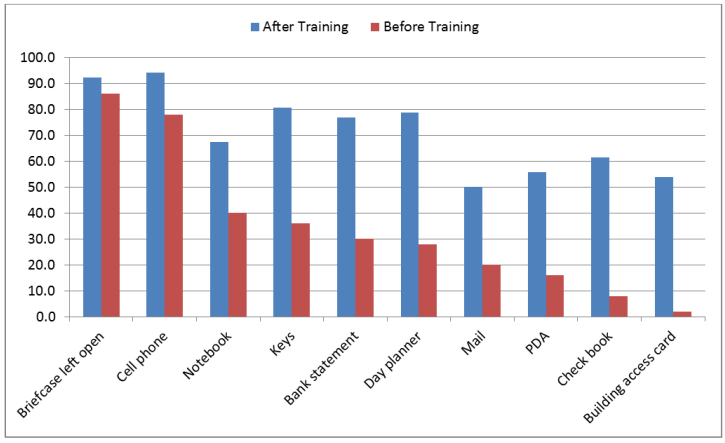

Figure 8.14: Items Left on The Desk.

These are issues relating to the PC workstation, figure 8.15 shows once again the training produces a distinct improvement. As expected, the items which scored poorest pre training demonstrated the biggest improvement through the training.

Finally, for the items located elsewhere in the office figure 8.16 show that, pre-training there are some significant areas of concern however again post training most areas score satisfactorily. One item– the position of the desk– was identified by less than 50% of the participant even after training, although it still demonstrated a marked improvement over the pre training results. This indicated the need for continual re-

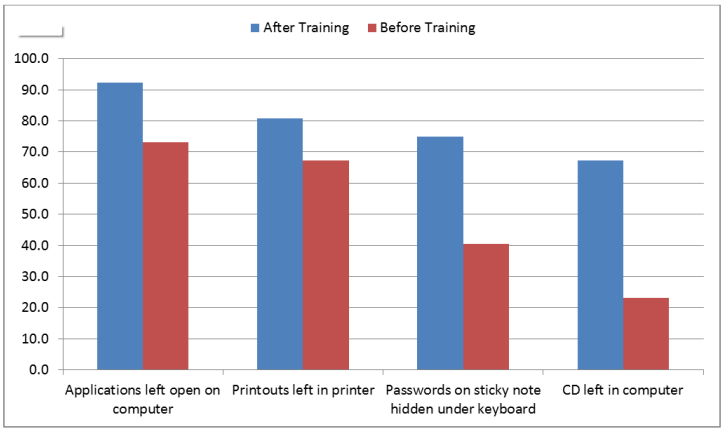

Figure 8.15: Items relating to the PC workstation.

training to be applied to all employees.

Figure 8.16: Items located elsewhere in the office.

8.6 Conclusions

All modern organisations have implemented to a degree of culture of information security; however where this culture has not become pervasive and fully embedded in the organisation's culture, there remains a threat to the organisations information security. In order to identify potential weaknesses in the practices and behaviours of workers

that may constitute such a threat, an assessment of an organisation information security culture was carried out in the form of a questionnaire. This process lead to the identification of strengths and weaknesses within the organisations security culture. Anonymous questionnaires are a key instrument for assessing the standards of information security in an organisation, being essential for evaluating the impact of any introduced measures such as training courses or new security policies. The assessment has shown that generally the UAE e-Government has an adequate culture of information security. However, there remain some areas where management could facilitate further enhancement of the culture of information security by developing a comprehensive security policy to be implemented across all departments of the organisation from these findings. A pilot study was carried out into employee practical awareness of potential information security vulnerabilities and the results have shown that there is a significant improvement in employee awareness to be gained through training. Thus it was recommended that training in security best practices be carried out within the organisation to ensure that all employees are aware of these practices within their departments. This should improve the employee's behaviour toward information security practices.

Chapter 9

Information Security Policy Development

9.1 Introduction

The aim of this chapter is to develop a comprehensive policy for the UAE e-Government, to protect the information systems and the exchange of information between different department's employees and citizens using e-Government services. In the Gap Analysis and the employee's survey, the lack of a comprehensive information security policy was identified as major concern and barrier to developing a secure information system for e-Government. Thus the final part of our work was to develop policy to ensure that the organisation uses the same standards in every security instance. This will make it easier for e-Government departments to integrate, and interact with citizens, and ensure that the UAE e-Government will always be able to protect the information assets in a manner that supports and is not in conflict with providing a high level of customer service.

Information security policies are the highest level description of how an organisation wants to protect its information assets. Policy describes security in several terms, is not itself just simple guidelines, procedures or standards. It is a statement of goals to be achieved by procedures put in place by different departments. Policy tells the employee what is being protected and what restrictions should be put in place. Management might say that every department is responsible for their own security. This is a good short term solution. But organisations should have a standard policy that is common to all their departments. If one department uses one standard and another uses a different standard, interoperability could become a signification problem and a ready source of security vulnerabilities. Although policies do not discuss how, properly defining what is being protected assures that proper control is implemented. Policies tell you what is being protected and what restrictions should be put on those controls. Implementing these guidelines should lead to a more secure system.

There are other less obvious benefits to maintaining a rigorous and comprehensive information security policy, such as protecting the organisation from litigation. In many jurisdictions, failure to provide an explicit information security policy would make dismissing an employee for incorrectly handling (even if deliberate and malicious) information would be legally untenable as the employee won't have been explicitly instructed against it.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organisation are met (113), (118).

Before a policy documents can be written, it is first of all necessary to determine the overall goal of the policy. Is the goal to protect the company and its interactions

with its customers, or will you protect the flow of data within the system? In any case, the first step is to determine what is being protected and why it is being protected.

Policies can be written to affect hardware, software, access, people, connections, networks, telecommunications, enforcement, and so on. Before beginning the writing process it's important to determine what systems and processes are important to the organisations mission. This will help determine what and how many policies are necessary. After all, the goal here is to ensure all possible areas for which a policy is required have been considered. In preparation for writing the policy document a consultation was carried out with each of the relevant departments within the UAE e-Government to determine the current working practices, we then referred to ISO 27001 in order to bring these into line with this standard.

9.2 Organisational Security and Responsibilities

To be effective, information security must be a team effort involving the participation and support of all workers in the organisations e-Government that deal with information and information systems. This policy statement clarifies the responsibilities of users as well as the steps they must take to help protect the organisation information and information systems. The responsibility of implementing and monitoring information security within the organisation is very important and requires the establishment of several committees to deal with security related activities, the committees can be formed as follow:

- The Information Security Steering Committee; members of the steering committee should include the IT director, division heads and the Information Security Consultant (if available). The responsibility of the committee is approving secu-

rity initiatives, approving proposed changes to the information security policy, standards and procedures, review security incidents and approve corrective actions. The committee will discuss information security related matters during the departmental progress meeting that should be held on a weekly basis. Any departure from the information security policy must be notified in writing and receive pre-approval from the information security manager and the appointed information security committee. Any approvals for deviation from the policy should be should be strictly limited in scope and time frame. It should be the active responsibility of the information security manager to periodically review and revise all deviations, and explicit decisions be made as to whether to extend or curtail any outstanding deviations.

- Information Security Implementation Committee; the IT management (director and division heads) holds the responsibility of designating representatives from the different divisions to form the security implementation committee. The committee holds responsibility for monitoring the information security policy implementation progress, reviewing the policy regularly and recommending changes in light of strategies and technologies changes. The committee also determine the details of security incidents related corrective actions and manages the implementation of these actions, directly supervising activities and field work related to the implementation of the policy.

- Information Security Manager; is the head of the information security division. He/she is the key person responsible for ensuring the implementation, monitoring and enforcement of the security rules that the security committees have established and approved. These rules are of different types and relates to all

areas where information is maintained and processed.

- Information Security Division; the division holds the responsibility of security day-to-day activities, it consists of three sections; the administration, control and the sites security sections. While the administration section holds the responsibility of users privileges administration on applications and databases, the control section holds the responsibility of security monitoring through daily and periodic reviews utilising manual and automated techniques. The sites security section holds the responsibility of monitoring physical and environmental security controls in computer and communication sites, and ensure these controls are sufficient and per approved standards. Information security related jobs are distinct functions that should be segregated from other IT functions to reduce the risk of negligent or deliberate systems misuse, and to ensure proper segregation of duties.

9.3 Information Transmission

The transmission of information (data) needs to be controlled and secured, data transfer can result in information leakage and disclosure. Data can be transferred physically by courier, mail, or messengers, and can logically be transferred by phone, fax, or network. There are different types of controls that can be implemented to achieve security of data.

9.3.1 Physical Controls

The following controls should be implemented on sensitive (restricted and confidential) and internal use only data physical transfer:

- A confidentiality and non-disclosure agreement must be signed with all parties (individuals and corporate) performing the job of physical data transfer.
- Sensitive information should be protected in sealed envelopes/containers with proper signatures and identification during the transfer, whether the transfer is inside or outside the organisation buildings.

9.3.2 Phone and Fax controls

The following controls should be implemented on phone and fax usage:

- Phone and fax should not be used to discuss or transfer sensitive (restricted or confidential) information.
- A separate confidentiality agreement should be signed with telephone operators highlighting possible consequences in case of system misuse.
- Fax machines should be programmed with proper answerbacks that show organisation name, correct date, and time.
- All faxes should be stamped with the following statement before being transmitted. "This Fax is confidential and may be privileged. If you have received it by mistake please notify the sender by return Fax and destroy the received paper. Any un-authorised use or dissemination of this information in e-Government or in part is strictly prohibited. The organisation shall neither be responsible or

liable for the proper and complete transmission of the information contained in this communication or for any delay in its receipt. Organisation does neither guarantee that the integrity of this communication has been maintained nor that this communication is free of interceptions or interference."

- Portables and leased computer hardware, software and accessories shall be handed over to an employee after getting his/her acknowledgement as the owner of that asset. The owner is responsible to maintain confidentiality, integrity and availability of the information stored on the leased asset.

9.3.3 Printer and Photocopier controls

During printing if a printer, copier, or fax machine jams or malfunctions when printing sensitive (restricted or confidential) information, the involved users must not leave the machine until all copies of the sensitive information are removed or are no longer legible. All paper copies of sensitive information must either be retained in the manner stipulated by the information owner, or disposed of by approved methods, e.g. by shredding. When printing sensitive information, the User must be present at the printer at the time of printing to prevent the information from being revealed to un-authorised parties, or direct the output to a printer inside an area where only authorised workers are permitted to go. With regards to photocopying documents, unless permission from the copyright owner(s) is first obtained, making multiple copies of material from publications is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

9.4 Personnel Security (HR) Policy

9.4.1 Job Definition

Specific information security responsibilities must be incorporated into all employee job descriptions if such employees have access to sensitive, valuable, or critical information. Employee responsibilities should include the following:

- Keep Logon-Ids and passwords secret.
- Keep the organisation information confidential.
- Report suspected violations of security to the information security division.
- Read, understand and implement the security policy and standards.
- Maintain good physical security by keeping doors locked, safeguarding access keys/cards, not disclosing access door lock combinations/keys, and questioning unfamiliar persons.
- Sign the organisation security statement, and abide by its conditions.

9.4.2 Third party

All contractors (temporaries, consultants, outsourcing firms, etc.) must personally sign the organisation non-disclosure agreement. The provision of a signature must take place before work begins, or if a contractor has been working without a non-disclosure agreement, a signature must be provided as a condition of continued contraction. Upon the termination or expiration of their contract, all contractors, consultants, and temporaries must hand over to their project manager all copies of the organisation information received or created during the performance of the contract.

All workers assigned security related jobs must first pass a background check. During this process the applications criminal conviction records, lawsuit records should be scrutinised as well as verification of his/her previous employment. This policy should apply to all new employees and also include re-hired and transferred employees, as well as third parties such as temporary employees, contractors, and consultants.

9.4.3 Disciplinary Action

Should a user of the organisation systems be found to have violated published security policies and procedures, the user will be subject to disciplinary action commensurate with the severity of the breach and their history with respect to security matters. Sanctions could include varying degrees of warning letters or removal of specific system(s) access. Background and reference checks should be performed on all employees e-Government perform security related functions.

Disciplinary action could include dismissal of an employee or cancellation of a contract, and may include criminal or civil legal action. The organisation IT director and concerned departments directors working in conjunction with the legal affairs division and the information security manager shall initiate implementation of sanctions and discipline actions. Organisational IT director and concerned departments directors working in conjunction with the legal affairs division and the information security manager handle disciplinary matters resulting from violations of information security requirements.

9.5 Training

All employees using the UAE e-Government systems must have sufficient initial training as well as continuing education in all critical aspects of their jobs including security. The security division staff should undergo regular information security specialised training to ensure security staff possess the knowledge required to maintain the security requirements of the organisation. The new employee must attend an information security awareness class before being granted access to the systems. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented, and had an opportunity to ask questions. To be eligible to have a login and password on any GDP system, the employee should have received security training.

9.6 Logical Security and Access Management

9.6.1 User Access Management

The organisation employee hold the responsibility of maintaining the confidentiality and integrity of the organisation and the public information and protect it from damage, alternation or loss by implementing information security processes and standards and by identifying and reporting security risks and implementing controls to mitigate these risks. Each employee should have controlled access to the information within the organisation, the access control approval process must be initiated by a worker's manager using a pre-defined form or by means of documented request that clearly specifies the name of the user, the name of the system or the information where access is requested and the details of the requested privileges. The privileges granted

remain in effect until the worker's job changes, the worker leaves the organisation or the worker's supervisor asks for a change on the granted privileges. If either of the first two events take place, the personnel department must immediately notify the the UAE e-Government in writing. All non-employees (contractors, consultants, temporaries, outsourcing firms, etc.) must also go through a similar access control request and authorisation process initiated by the project manager. The privileges of these non-employees must be immediately revoked through the UAE e-Government and the security administrators when the project is complete, or when the non-employees stop working with the organisation. The relevant project manager must review the need for the continuing privileges of non-employees once every three months. Forms used for access granting or changes should be retained for at least two years for audit purposes. All users must be positively identified prior to being able to use any multi-user computer or communication system resources. In keeping with the objective to protect the information handled by computers and communications systems, the management uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information. In keeping with these objectives, management maintains the authority to:

- Restrict or revoke any user's privileges,
- Inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and
- Take any other steps deemed necessary to manage and protect its information systems.

This authority may be exercised with or without notice to the involved users. The

organisation disclaims any responsibility for loss or damage to data or software that results from its efforts to meet these security objectives.

9.6.2 Gaining Un-Authorised Access via the Organisation Information Systems

Workers using organisation information systems are prohibited from gaining un-authorised access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. Likewise, workers are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism, which could permit un-authorised access.

9.6.3 Unique IDs/Logons

User-IDs/Logons and Passwords: To implement the need-to-know/need-to-do process, UAE e-Government insists that each worker accessing multi-user information systems have a unique user-ID and a private password. These user-IDs/Logons must then be employed to restrict system privileges based on job descriptions, project responsibilities, and other business activities. Each worker is personally responsible for the usage of his or her user-ID/Logon and password. User-IDs/Logons and related passwords must not be shared with any other individuals (users should instead utilise other mechanisms for sharing information such as electronic mail).

9.6.4 User Activity

Inappropriate Conduct: UAE e-Government management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal

and proper operation of UAE e-Government information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

Internal Reporting of Information Security Violations & Problems: UAE e-Government workers have a duty to report all information security violations / problems directly to the information security representative within their area and the information security manager, e-Government in turn should delegate responsibilities for counter action to concerned system specialists on a timely basis so that prompt remedial action may be taken.

Security Compromise Tools: Unless it is a work requirement and specifically authorised by the information security manager, UAE e-Government workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those, which defeat software copy-protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Similarly, without this type of approval, workers are prohibited from using "sniffers" or any other hardware or software that monitors the traffic on a network or the activity on a computer.

Prohibited Activities: Users must not test or attempt to compromise computer or communication system security measures, unless specifically approved in advance and in writing by the information security manager. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, or similar unauthorised attempts to compromise security measures, may be unlawful and will be considered serious violations of UAE e-Government information security policy.

Personal Use: UAE e-Government information systems (including the telephones) are intended to be used for business purposes only. Incidental personal use is permis-

sible if the use:

a) Does not consume more than a trivial amount of resources that could otherwise be used for business purposes,

b) Does not interfere with worker productivity, and

c) Does not pre-empt any business activity.

All User activity is subject to logging and subsequent analysis. Users must not perform any activity on UAE e-Government information systems that could damage the reputation of UAE e-Government. Personal Use of UAE e-Government Internet Facilities Only on Personal Time: UAE e-Government management encourages workers to explore the Internet, but if this exploration is for personal purposes, it must be done on personal, not official working time. Likewise, news feeds, discussion groups, games, and other activities which cannot definitively be linked to an individual's job duties must be performed on personal time.

9.6.5 User Accountability

Users Responsible For All Activities Involving Personal User-IDs/Logons: Users are responsible for all activity performed with their personal user-IDs/Logons. User-IDs/Logons may not be utilised by anyone but the individuals to they have been issued. Users must not allow others to perform any activity with their user-IDs/Logons. Similarly, users are forbidden from performing any activity with IDs/Logons belonging to other users.

9.6.6 User Inactivity

Notice of Last Log-In Time and Date: At log-in time, every user must be given information reflecting the last log-in time and date. This will allow un-authorised system usage to be easily detected.

Automatic Protection When Terminal Is Inactive: If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for ten (10) minutes, the system must automatically activate a screen saver that must require a password to be able to deactivate it. Re-establishment of the session must take place only after the user has provided the proper password.

Dormant User-IDs: All user-IDs must be disabled after a "Sixty (60) day" period of inactivity.

9.6.7 User Access Right Review Process

Review Process: Information owners are responsible for ensuring that the only personnel with access to their data are those that currently need it for business purposes. A review of all users with access rights for all UAE e-Government systems (including operating systems, utilities, databases and applications) should be undertaken at least once annually.

Information owners must oversee the extraction and review of user access rights to the data for which they are responsible, however the review will be initiated and performed by the information security team for application users and by the control team for operating systems, networks, utilities and databases. The information owner is responsible for revoking un-authorised or inappropriate accesses.

Information Owner Rights: To ensure compliance with UAE e-Government inter-

nal policies as well as applicable laws and regulations, and to ensure employee safety, UAE e-Government information owners reserve the right to monitor, inspect, and/or search at any time all UAE e-Government information systems under their custody.

Maintaining Evidence of Review: All details of the user access rights reviews should be documented at the time of performing the review. The details recorded should include the user accounts checked, the exceptions noted, reasons for the exceptions and follow-up actions. The documentation should be filed and kept for a period of at least two years.

Allocation of Responsibility on Termination: Whenever workers (employees, contractors, consultants, temporaries, etc) stop working for UAE e-Government, a task force should be initiated by the worker direct supervisor to ensure the proper review and handover of all assets (information, software, hardware and utility) under the custody of that worker to the concerned party within UAE e-Government. The assets new custodian should be clearly assigned to ensure the proper allocation of responsibilities for UAE e-Government assets.

9.7 Password Standards

Sharing Passwords: If users need to share computer-resident data, they should use electronic mail, shared databases, public directories on local area network servers, and other mechanisms. Although user-ID/Logons are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. One exception to this involves expired passwords which are received at the time a user-ID/Logon is issued; these passwords must be changed the first time that the authorised user accesses the system. To share a password or any other access mechanism exposes the authorised

user to responsibility for actions that the other party takes with the disclosed password. If a worker believes that someone else is using his or her user-ID/Logon and password, the worker must immediately notify the security administrator for the information system in question, and the information security manager. The following settings should be used as a minimum standard for user accounts in all of UAE e-Government IT environments:

- Passwords should be at least 6 characters for normal users and 8 characters for super (privileged) users;
- Passwords should be a combination of at least two of the following: upper and lower case letters (a-z), characters (# etc) and numbers (0-9), but should not be only characters and numbers;
- Passwords should not be allowed to be repeated within the last 6 iterations per user;
- Maximum password life should not exceed 90 days for normal users and 30 days for super users in any system, and minimum password life should not be shorter than 1 day;
- Passwords should not be similar (for example password1, password2);
- Passwords should not be dictionary words, names of pets, dates of birth, spouse name or any other word that is easy to guess;
- Accounts should not allow more than 5 continuous failed login attempts for normal users and 3 continuous failed login attempts for super users.

Non-display of Passwords: The display and printing of passwords must be masked, suppressed, or otherwise obscured so that un-authorised parties will not be able to observe or subsequently recover them. All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to un-authorised parties.

9.7.1 Administrator Responsibilities

Forced Change of All Passwords: whenever an un-authorised party has compromised a system, system owners must immediately change every password on the involved system. Even suspicion of a compromise requires that all passwords be changed immediately. Under either of these circumstances, a trusted version of the operating system and all security-related software must also be reloaded. Similarly, under either of these circumstances, all recent changes to user and system privileges must be reviewed for un-Authorised modifications.

9.7.2 Temporary Passwords

Assignment of Expired Passwords: The initial passwords issued by a security administrator must be valid only for the involved user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done.
Changing Vendor Default Passwords: All vendor-supplied default passwords must be changed before any computer or communications system is used for UAE e-Government life environment.

9.8 Operating Systems and Database Security

9.8.1 OS Security Hardening

All operating systems installations should be configured according to vendors' recommended security hardening settings. These settings should be reviewed and approved by the security manager and the system administrator prior to implementation. Hardened setup should be test in a test environment prior to live installation to ensure integration with other systems and applications.

9.8.2 Use of System Utilities

The principle of least privileges shall be applied to systems programming functions, database tools and system utilities. Programmers shall be given access privileges that are consistent to their job responsibilities. End-users must not be allowed to invoke operating system level commands. End-users must be presented with only the system capabilities and commands that they have privileges to perform.

9.8.3 User Authentication

User Authentication: All production information system user-ID/Logons must have a linked password or a stronger mechanism (such as a dynamic password token) to ensure that only the authorised user is able to utilise the user-ID/Logon. Users are responsible for all activity that takes place with their user-ID/Logon and password (or other authentication mechanism). Users must immediately change their password if they suspect that it has been discovered or used by another. Likewise, users must notify the information security representative in their divisions and the information security

manager if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised. Passwords must also be changed whenever the user-ID/Logon is assigned to another person.

Legal Notice: The following notice shall be incorporated on the login screen to all systems: "This system and the information it includes is the property of UAE e-Government and is restricted to Authorised users only. If you are not authorised to use the system and/or the information it contains, you must sign out immediately."

9.8.4 Patches Implementation

Patches Distribution: System Software companies normally provide periodic fixes to security related vulnerabilities in their products. IT and telecommunication department operations hold the responsibility of providing, testing these fixes, implementing them on live system, and updating the information security manager with the patches implementation. IT operations will utilise proper system and database scanners to ensure system and database security vulnerabilities are detected and corrected on a timely basis. Scanners will be scheduled to run periodically and on time intervals that ensure critical systems are checked and fixed properly. Reported vulnerabilities will be fixed manually for critical machines, and can be fixed automatically for other machines that are classified as non-mission-critical.

9.9 Applications Security

9.9.1 User Authentication

For all UAE e-Government application systems, user-ID/Logons must have a password to ensure that only the authorised user is able to utilise the user-ID/Logon. Users are responsible for all activity that takes place with their user-ID/Logon and password. Users must immediately change their password if they suspect that it has been discovered or used by another person. Likewise, users must notify the information security division if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

9.9.2 Use of Sensitive ID/Logons

Sensitive application ID/Logons, such as super-user and administrator accounts, should only be used on an as required basis. No users should use these ID/Logons as their normal user account. Allocation of user access levels, user access should be requested by departments' managers in writing and forwarded to the security division/administration section to grant the required access.

9.9.3 Access to Development and Production Application and Database Libraries

Access to the development environment should be restricted to only programmers and developers. Only those users e-Government require access to production system to perform their duties should be granted it. Access to the database libraries should be restricted to database administrators only.

9.9.4 Output Data Controls

Access control standards will apply to processing output results (hard and softcopies). Any un-Authorised access to processing results is considered as an incident that should be reported as per the approved incident management procedures.

9.10 Operations Management and Security

9.10.1 Microcomputers Security

Access Security: All microcomputers (workstation, desktop, laptop, pocket computers and PDA's) must be secured against un-authorised access using security products (built-in or third party) commensurate with the information accessed, stored, or processed. These security utilities include operating system access tools, and third party access control tools.

Physical Controls: All microcomputers must be secured against removal or theft commensurate with the value of the computer and the information that it holds. All loss or theft of microcomputers must be immediately reported according to the security incident management procedure.

Controlling Input/Output Drives and Ports: To protect UAE e-Government information from leakage to external parties, and to avoid introducing unnecessary or harmful software to UAE e-Government network, CD-ROMs, floppy drives, USB ports and other input/out ports on all users workstations should be disabled, unless explicit authorization is available to do otherwise. Any exception to this policy should be pre assessed and approved by the information security manager.

Unattended Management: Remote un-attended management systems are not au-

thorised in UAE e-Government networks unless explicit approval is obtained from the information security manager. Affected users should be officially informed of the availability of such systems and the possible impact on their systems and data.

All accesses to end users machines should be made in coordination with the machine custodian/owner; any access to end users machines without the prior notification of the user is considered a violation to the information security policy and will be subject to investigation, escalation and punishment.

PC Preventive Maintenance: A semi-annual preventive maintenance will be scheduled to cover all workstations, PC's, laptops and printers within UAE e-Government network. The preventive maintenance should include physical and logical health checks that ensure machines are functioning properly and are protected against threats including virus threats.

9.10.2 Virus Protection

Virus-Screening: Antivirus approved product must be installed and updated on all microcomputers (workstations, desktops and laptops), LAN servers, internet servers and mail servers connected to UAE e-Government network. In addition all gateways to the network must be protected against viruses using a proper virus-wall technology that scans all inbound traffic and stops/reports cases of suspected viruses.

Virus Signature Updates: IT operations and IT support divisions must ensure that virus signatures used by all installed instances of virus-scanning software are updated periodically, upon the release of a new update by the anti-virus software vendor. For more details on related responsibilities refer to the virus protection procedure.

Files and Media Subject to Scanning: The virus-scanning software must be used to

review all files and media introduced to UAE e-Government network. Any files that are compressed or 'zipped' must be decompressed on a stand-alone PC prior to scanning.

Prohibition on Un-Authorised Software Introduction: Users shall not download software from external systems such as the Internet, or otherwise introduce software that has not been authorised by the IT and telecommunication department, onto UAE e-Government network.

Prohibition on Virus-Scanning Deactivation: Users must not bypass or turn-off scheduled scanning processes or otherwise tamper with the installed virus-scanning software. Moreover, users must not intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.

Computer Virus Eradication: If Users suspect infection by a computer virus, they must immediately stop using the involved computer and call the help desk. Floppy disks and other magnetic storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves; qualified UAE e-Government staff will be called in to complete this task according to the approved virus protection procedure.

9.10.3 Data Backup, Restore and Retention

Back-Up Responsibility: To protect UAE e-Government's information resources from loss or damage, personal computer users are responsible for regularly backing-up the information on their personal computers, or else making sure that someone else is do-

ing this for them. For multi-user computer and communication systems, an operator is responsible for making periodic back-ups. Operations division hold the responsibility for installing back-up hardware and/or software. All back-ups containing sensitive information must be stored in an approved off-site location with proper physical access controls and/or encryption so as to ensure that the data remains confidential.

Data Restore Testing: To ensure data backup is valid and to check the reliability of backup media, periodic data restore will be performed on a testing environment only. The restore periods will depend on the data classification and should be done in coordination with the data owners for authorization and validation purposes.

9.10.4 Software Licensing

Adequate Licenses: IT and telecommunication department management must make appropriate arrangements with the involved vendors for additional licensed copies, if and when additional copies are needed for business activities. To ensure compatibility with UAE e-Government networks and computers, and to allow licenses to be centrally managed, all software must be purchased through the purchasing department in coordination with the IT and telecommunication department.

Un-Authorised Copying: Users must not copy software provided by UAE e-Government to any storage media (floppy disk, magnetic tape, CD-ROM, etc.), transfer such software to another computer, or disclose such software to outside parties, unless an advance permission is obtained from the concerned IT Division Head. Ordinary back-up copies are an authorised exception to this policy.

Installation of Authorised Software: Users must not install software on their personal computers, network servers, or other machines. Designated IT personnel are

the only party authorised to do installations in compliance with the approved change management procedure. Use of software licensed to UAE e-Government on a personal computer owned by a user is not authorised unless the system has been designated a "system which is used to process UAE e-Government information". The installation and use of games that take the form of separate software packages are prohibited on any UAE e-Government computer systems.

Review of Licenses: Appropriate inventory management system will be utilised to perform on-going monitoring on installed software to ensure licensing compliance. The security division/control team on an annual basis shall undertake a comprehensive review of licenses.

9.10.5 Information Storage and Disposal

Removable Media: Computer and network backup storage media must be stored in a separate physical location from the machine producing the backup to ensure the availability of data resources during emergency situations such as where main locations hosting primary machines are rendered inaccessible. Computer media storage procedures must assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to deterioration. For instance, operations division management must ensure copying data to different storage media if the original backup media is showing signs of undue deterioration.

Storage Restriction: UAE e-Government employees must not store private, confidential, or secret information on PC or workstation hard disks unless the information security manager has determined that adequate information security measures will be employed.

Equipment/Media Release Control: Before information systems equipment or storage media which has been used for UAE e-Government operations is provided to any third party, the equipment or media must first be physically inspected by the IT division responsible for the equipment / media to determine that all sensitive information has been removed.

Before computer magnetic storage media is sent to a vendor for trade-in, servicing, or disposal, all UAE e-Government sensitive information must be destroyed or concealed by methods that render the information non-recoverable, for example, by degaussing tapes or formatting the hard disk.

Information Destruction: Destruction of sensitive information captured on computer storage media (such as CD-ROMs, tapes, or floppy disks) must be performed in a manner that does not allow information retrieval in future. All sensitive media destruction such as main database backup should be done based on a formal approval of the IT director and under the direction of the information security manager as per an official letter listing the media name to be destroyed and the details of its contents.

9.11 Communication Security

9.11.1 Internet and Intranet Segregation

UAE e-Government internal networks shall not be connected to the Internet. Access to the Internet shall be through an independent network. PCs cannot be connected to the Internet and the internal UAE e-Government network simultaneously. PCs may not be switched between the Internet and the internal network. Ad hoc connection for any device will be controlled. Before any device gets network access, the user should be

authenticated utilizing the industry standard IEEE 802.1X. This standard applies for all connections whether they are wired or wireless.

9.11.2 Enforced Network Path

Positioning of gateways: The network path by which UAE e-Government computers communicate with less-trusted computers and networks must be controlled. The insecurities inherent in common network protocols must be, for each controlled path, mitigated by network mechanisms, which manage those risks. Accordingly, each connection to a less-trusted computer or network must be through a gateway that is compliant with the section of this policy entitled UAE e-Government Gateways.
Connections to UAE e-Government Network: UAE e-Government computers or networks may not be connected to less-trusted computers or networks without the explicit, written authorisation of the information security director. Users must not connect their own computers with UAE e-Government computers or networks without the explicit, written authorisation of the user division head and the security manager.

Internal network topography of UAE e-Government has been designed to maximize the security of UAE e-Government network, un-Authorised alterations to connections between UAE e-Government networks is prohibited, alterations should be controlled by the approved change management procedure and should be in line with the established standards under "Communication Security".

9.11.3 UAE e-Government Gateways

Gateway architecture: Gateway components, including firewalls, packet-filtering routers, and proxy servers, must operate in a restrictive manner such that if they fail, traf-

fic either fails to pass or else is diverted to a similarly-configured device. Dedicated network service servers that are intended to communicate directly with non-trusted networks, or proxy servers, shall be maintained in a dedicated subnet off the firewall (a 'Demilitarized Zone') rather than within the internal UAE e-Government network. 'Restricted' or 'Confidential' UAE e-Government information should not be stored on these servers. No gateway component shall be used for purposes other than its designated gateway role - firewalls, for instance, will not be also used as an FTP servers or file servers. Where any gateway component has an underlying operating system, that operating system will be secured, and the latest patches released by vendor applied. The availability of vendor-supplied patches and security fixes will be reviewed periodically, and applied where needed.

Each gateway component will have a different privileged password, so that a compromise of any single gateway element will not constitute a compromise of the entire gateway architecture.

9.11.4 Firewall Configuration Policy

The following guidelines apply to the configuration of the firewall rule-set and properties:

- All unnecessary network services will not be allowed into the network, nor proxied for; filters changes should be pre assessed and approved by the security division;
- No direct connections are permitted from untrusted networks to internal network hosts; rather, incoming traffic from untrusted networks must be routed to dedicated network service servers or proxy servers, or dropped;

- When developing the firewall ruleset, consideration must be given to:
  - The filtering of all levels of the TCP/IP protocol stack - UDP, TCP, ICMP, and routing protocols.
  - The filtering of traffic based on both the source and destination addresses.
  - The filtering of both incoming and outgoing traffic.
- The firewall's logging functionality should be utilised to the full extent possible, and this log should be reviewed in accordance with the security monitoring standards.
- The management of each firewall, if not performed locally on the firewall, shall be over a trusted and secured path, and authentication of the management server and administrator shall be performed on the basis of credentials other than merely the IP address of the management server.
- The firewall machines must be subject to regular monitoring and audits.
- The firewall machines should have the integrity of its files checked once a month.
- The Firewall must be available 7x24 days per week, with minimum downtimes during office hours.
- Internet access should only be available if the firewall is active. Firewall shutdown for maintenance or upgrade purposes must be planned and scheduled during weekends only.
- Logs must be automatically analysed, with critical errors generating alarms, and send automatic notifications to the administrator via email, pager, or other means.

- Logs must be archived for at least one year.
- The non-trivial log entries must be examined weekly.
- Statistics on usage must be available.
- Users should not be able to logon directly onto firewall machines.
- All login sessions to firewall machines including the administrator must use encrypted login or one-time passwords.
- Change management: Updates and configuration changes must be logged and carried out according to the approved change management procedure.
- Regular update of "Firewall Set-up and Security Policies" document must be made when configuration information changes.
- The firewall shall not be configured as a DNS server.
- The firewall shall be configured to reject any kind of probing or scanning.
- The firewall shall block all software types that are known to present security threats to the network such as Active X and Java.

9.11.5 Router Configuration Policy

The following guidelines apply to the configuration of gateway routers:

- Router access points, including the console, telnet (vty) and auxiliary ports, shall be logically secured with a password.
- Where it is supported by the router's functionality, telnet (vty) access to the router will be allowed only from certain IP addresses.

- Where it exists, the router's login timeout functionality will be enabled.
- tftp servers used to supply configuration files shall be logically secured.
- All router passwords shall be changed from their vendor-supplied default, and will be stored in the configuration files in an encrypted form.
- Privileged and non-privileged mode passwords will be different.
- Where it is supported by the router's functionality, border routers should be configured to perform packet-filtering to increase the depth of UAE e-Government's network defence.
- As for all gateway components, routers should be physically secured according to the approved physical security standards.

9.11.6 Modem Configuration and Positioning Policy

The following guidelines apply to the configuration, and positioning, of modems within UAE e-Government network. As a general rule, modems shall not be allowed within the network; exceptions to this rule include:

- Modems which are required under 3rd party support contracts
- Modems which are collected into a modem pool and are subject to the control and maintenance of the IT and telecommunication department; these modem pools shall be configured such that remote Users cannot access network resources until they are authenticated by a dedicated authenticating device, such as a RADIUS server

- Modems required by IT and telecommunication department staff to perform critical remote administration
- Modems which are otherwise deemed to be critical to the performance of UAE e-Government operational activities, and alternative means of network connectivity are not feasible
- All modems which fall within the exceptions noted above must:
  - be explicitly authorised by the information technology director or his designate and the information security manager;
  - be switched off when not in use, or when it is anticipated that remote access will not be required
  - use TCP/IP filtering, to restrict access to certain addresses
  - log all remote (dial) accesses. Logs should be reviewed on a daily basis by designated personnel, to ensure all accesses are authentic
- Remote control software, such as PC anywhere, shall not be installed on any computers, except where it is required to support modems which fall into the above exception categories

Restriction of unnecessary network roaming: Although computers on UAE e-Government networks are considered 'trusted', wherever possible, the extent to which UAE e-Government computer may access other UAE e-Government computers should be restricted to that which is necessary to perform that computer's function. As a result only required traffic between network segments will be allowed. For instance, where Authorised traffic between networks consists only of email and telnet sessions, other traffic

should be filtered by the connecting routers. VLANs Utilisation: UAE e-Government network shall utilise VLANs in a proper way. Configuring VLANs would result in breaking down broadcast domains, thus, improving performance. In addition, traffic between VLANs shall be controlled in a way that users can only access specific predefined resources.

Wireless Communication Security: All wireless access points/base stations connected to UAE e-Government Network must be registered and pre approved by the network division head. All wireless network interface cards used in UAE e-Government laptop or desktop computers must be registered as well, with details communicated to the information security division.

All wireless communications must utilise UAE e-Government approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. Wireless implementations must maintain point-to-point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e. MAC address. Wireless connections are prohibited within UAE e-Government internal network. Approved wireless connections within the Internet network are allowed, taking into consideration not storing sensitive information on devices connected to the wireless networks.

9.11.7 Browsers

Browser Configuration: The IT and telecommunication department must ensure that the browser that forms part of UAE e-Government standard:

- is updated with the latest appropriate security patches and fixes.
- is configured to use UAE e-Government proxy server.

- has the active content functionality (to support Java, ActiveX for example) disabled, unless a business need justifies otherwise.
- If a business need justifies enabling Java, the following standards should be applied:
  - Java configuration must comply with the Java sandbox security scheme;
  - Java configuration should not allow native method call;
  - Spawning should not be allowed in any way.

The web browsing software installed by the IT and telecommunication department onto the computer of those users to e-Government internet access has been granted is not to be replaced or modified. Users are not permitted to use any other web browsing software or version.

9.12 Encryption

Policy on the Use of Encryption: By the nature and medium of information transmission, information that is transmitted across unencrypted channels is exposed to the risk of interception. Accordingly, the transmission of any 'Restricted' or 'Confidential' information across untrusted network paths should only be made using encryption facilities installed and approved by the IT and telecommunication department.

Responsibility for Implementation and Maintenance of Encryption Facilities: The IT and Telecommunication Department is responsible for the selection, installation and maintenance of encrypted channels, in coordination with the Information Security Manager.

Key Management: Attacks on the encrypted information are most likely to be targeted at key management, rather than a cryptanalysis of the encryption. The following general guidelines are intended to provide assurance over the key management processes:

- Protection of the private or secret key - the security of the private key (for asymmetric encryption), or secret key (for symmetric encryption) must be at least equal to the required security of the messages sent over the encrypted channel. The private key should never be stored in plaintext, and preferably not on a networked computer. Rather, it should be stored on physically secured removable media in an encrypted form with a strong password.

- Expiration period of keys - to protect against crypto analysis, and to minimize the damage from a compromised key, keys should have a limited lifecycle. A new public-private key set should be generated at a frequency that fulfil the required confidentiality of the encrypted data.

- Measures taken following the compromise of a key - upon becoming aware of a possible compromise, the encryption facilities should be configured to no longer accept that key set, and a new key set should be generated. The method of private key storage should also be changed.

- Logging and auditing of key management activities - a hardcopy log of all key management activities should be maintained, and kept in a secure place.

- Physical keys security - physical keys should be physically secured at all times under the custody of the information security manager, and should be released only upon the receipt of an official request from the IT director or his designate.

9.13 Vulnerability Management

Policy on Scanners Usage: The vulnerability management system shall be utilised on all mission critical systems, network components and databases within UAE e-Government network. Network scanners, systems scanners and database scanners shall be scheduled to scan the different network components and to fix vulnerabilities where they are detected. All machines and systems classified as mission critical will be configured for manual fixing (manual patch update) according to the patch management standards, all other systems/machines will be fixed automatically by the vulnerability management tool.

Scanners Management: It is the responsibility of the concerned division to ensure that the vulnerabilities database is maintained up to date at all times. Security Division/Control Team holds the responsibility of checking system logs and ensuring updates are performed periodically and that scanning is carried out as per the approved schedule. All errors/irregularities shall be reported to the Information Security Manager and the concerned Division Head. Any suspected incident should be reported as per the approved incident management procedures.

9.14 Internet Usage Policy

Internet Access is Not a Fringe Benefit: Internet access will be provided only where it is necessary to perform a user's role, and once granted, should be used only for that purpose. Users should be aware that the amount of data that can be simultaneously transmitted to and from the Internet (commonly known as 'bandwidth'), and between UAE e-Government networks, is finite. Excessive use of the Internet for personal use

will prevent other Users from performing their job functions.

Information Reliability: Information held on the Internet has not been subjected to any form of quality assurance that might normally be provided by a publisher, and so should not be relied upon by Users in the absence of a confirming source. Similarly, critical correspondence should not be engaged in across the internet unless the user can confirm the identity of the correspondent through alternative methods.

Downloading Software: Users must not download software from the internet unless specifically authorised to do so by the IT and telecommunication department. Security tools will be utilised to prevent un-authorised download of files from the internet. Data files may be downloaded without explicit authorisation, but users must ensure that any downloaded files are scanned for viruses before their use. Where data files are compressed, they must be decompressed prior to scanning.

Sending Sensitive Information: Users must not send sensitive information across the Internet, or other untrusted networks, unless the connection is encrypted. Users should be aware that the appearance of a 'padlock' at the bottom of their browser is an indication of a session secured by 'SSL', but that 'SSL' is not considered adequate for any information that is deemed 'Restricted' or 'Confidential'.

Creation of Internet Services on UAE e-Government resources or regarding UAE e-Government: In the absence of written approval from the IT and telecommunication department, Users and Departments must not establish any web pages, EDI facilities, electronic bulletin boards, or other publishing mechanism which uses UAE e-Government resources, or which provides public access to information about UAE e-Government.

9.15 Electronic Mail Usage

Sharing and Forwarding: Electronic mail accounts are to be assigned to, and used by, specific individuals. They are not to be shared. If a User goes on vacation or is otherwise unable to check their mail for extended periods, mail can be forwarded to another person. Likewise, notices can be established which will automatically notify correspondents that the recipient will not be responding for a certain period of time. As for user accounts, a User's electronic mail account must be terminated upon their departure from UAE e-Government.

Naming Conventions: Users email IDs should clearly reflect the name of the mail box owner, a naming convention that contains the last name and parts of the first name is approved. Any generic names or names that might be misleading will be considered illegal. All cases of odd names will be immediately investigated and disabled.
Restriction of Use to 'Public' and 'Internal' information only: To restrict the dissemination of sensitive information, electronic mail containing 'Public' and 'Internal' information only, sent to addresses outside UAE e-Government is permitted. If an electronic mail message contains sensitive information, Users must not send the mail item outside UAE e-Government email system unless the message is encrypted using encryption facilities approved by the information security manager.

Email Broadcast: Broadcast electronic mail message facilities should not be employed unless department manager approval is first obtained, but the use of selected distribution lists is both advisable and permissible without such approval.

Message Download: Electronic mail messages sent to and from UAE e-Government email server are downloaded to the email server hard disk. Users should download their messages frequently during the day to ensure no message is stored on the mail server

hard disk for a long time.

Message Content: Users must not use profanity, obscenities, or derogatory remarks in any electronic mail messages discussing employees, contractors, or others involved with UAE e-Government activities. Similarly, users should not compose or send emails that may be reasonably perceived by the recipient as sexual, ethnic, or racial harassment. Such remarks are grounds for disciplinary action against the User. The IT and telecommunication department must ensure that the following footer is attached to every email sent from UAE e-Government network that, to the extent permissible, disclaims responsibility for the email's contents.

"This message (including any attachments) is confidential and may be privileged. If you have received it by mistake please notify the sender by return e-mail and delete this message from your system. Any un-Authorised use or dissemination of this message in e-Government or in part is strictly prohibited. Please note that e-mails are susceptible to change. UAE e-Government shall neither be responsible or liable for the proper and complete transmission of the information contained in this communication or for any delay in its receipt or damage to your system. UAE e-Government does not guarantee that the integrity of this communication has been maintained or that this communication is free of viruses, interceptions, or interference"

Message Printing: Emails containing official approvals, confirmations or any information that can be considered a reference in future must be printed and filled in a proper way.

Message Deletion: The retention of messages stored on the hard disk remains the user's responsibility depending on the message content and the possible need in future, and should be in line with UAE e-Government approved retention periods for other data sources.

9.16 Web Servers and Electronic Services Security

The following standards will apply to web servers and services, whether these are locally managed or outsourced to a third party: Content Management: Prior to being posted, all changes to the UAE e-Government internet web page must be approved by the public relations division e-Government will make sure that all posted material has a consistent and polished appearance, is aligned with operations goals, and is protected by adequate security measures. Web server home pages must store minimum information required to process Internet-based transactions. Hyperlinks, which transfer Internet users from UAE e-Government web sites to the web site of any external entity, should be pre-approved by the Information Security Manager. Active contents (including Java scripts, Active X, Visual Basic Scripts, Macromedia Shockwave files) will not be allowed in UAE e-Government web servers, unless a business need justifies the utilization of such contents and after obtaining the approval of the Information Security Manager.

Virus Protection: Up-to-date virus checking programs approved by the information security manager must be continuously enabled on all web servers, whether hosted locally or maintained through an outsourcing agreement

Transactions Authentication and Authorisation: A current digital certificate to connect internal network is required for every Internet server handling UAE e-Government transactions to which public, and others may connect. All internet based applications transactions should be made through a Demilitarized Zone and no transactions shall be made directly to UAE e-Government central databases. Web based transactions shall be secured using encryption techniques such as SSL or through the utilization of secure web applications such as HTTPS.

9.17 Outsourcing and Third Party Access

9.17.1 Outsourced Services Controls

Written approval to be provided, before third party users are permitted to gain access to UAE e-Government's internal information systems via any means (dial-up lines, the Internet, or physical access), specific written approval of the Information Security Manager must be obtained. These third parties include service providers, other governmental entities, as well as contractors and consultants working on special projects. These privileges must be enabled only for the time period required to accomplish previously defined and approved tasks as per the outsourcing/contracting agreement. Third party staff should be briefed on the elements of UAE e-Government security policy and procedure that are relevant to their task and environment.

Revocation of Third Party Access: Except where the need for third party access is persistent and regular, such as for long-term, full-time consultants, permanent system accounts used by third party staff should be disabled and password must be changed. Third party staff tend to use the same password at every installation, and to share their password with other third party staff that will make service calls to UAE e-Government. For these reasons, the risk posed by these accounts must be strictly managed. Third party staff, except those e-Government are long-term, full-time contractors, should be escorted while they are present outside of working hours or while they are in sensitive areas such as the computer rooms. Their arrival and departure should be logged in a visitor log. Where the provision of third party support or the nature of the outsourced service requires the connection of the third party network to UAE e-Government network, that third party must secure its connected system in a manner consistent with this policy as a condition of connection, in addition connec-

tions must be treated as untrusted, and should be in compliance with the standards established under "Communication Security".

9.17.2 Security Requirements in Third-party Contracts

Third party access to UAE e-Government systems requires signed contract, before any third party is given access to UAE e-Government systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager at the third party organisation. The information security manager must also approve these terms and conditions.

Release of Information to Third Parties: Where the work performed by the third party will involve the provision of access to UAE e-Government information resources other than "Public" information, or will involve the third party gaining access to UAE e-Government network configuration information, UAE e-Government non-disclosure agreement must be signed by the third party. If sensitive information is lost, is disclosed to un-Authorised parties, or is suspected of being lost or disclosed to un-authorised parties, the information owner and the information security manager must both be notified immediately.

9.17.3 Outsourced Software Development

Shareware Controls: Free software (also known as shareware) and 'demo software' is not permitted within UAE e-Government network unless specifically approved by the information security manager. The source code of software developed by a third party for the use of UAE e-Government services and operations must be owned by UAE e-Government or otherwise should be escrowed. This requirement should be clearly

reflected within the contract signed with the third party.

9.18 Security Incident Management:

This incident response policy defines what constitutes a security incident and outlines the incident response phases. This incident response policy document discusses how information is passed to the appropriate personnel, assessment of the incident, minimising damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handing various security incidents. This section explains the procedures required to build an incident response plan.

- Mandatory Reporting: All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize UAE e-Government information or UAE e-Government information systems, must be immediately reported according to the "Incident Reporting Procedure" Un-authorised disclosures of UAE e-Government information must additionally be reported to the involved information owners.

- What To Report: All workers must promptly report any loss of, or severe damage to, their hardware or software. For example, if a portable computer was stolen, this must be reported. Workers must also report all suspected compromises to UAE e-Government information resources and information systems. For instance, if a hacker is believed to have broken-into UAE e-Government systems, then this too must be reported. Likewise, if serious information security vulnerability is known to exist, this too must be reported. All instances of

suspected disclosure of sensitive (Restricted or Confidential) information must additionally be reported.

- Handling of Incident Reports: The information security division must investigate the problem with the information security representatives e-Government must deal with all likely security incident reports that they may receive. Information security manager has the responsibility to determine adequate responses and escalation procedures for all likely scenarios, including procedures to notify seniors in UAE e-Government and possibly external parties as appropriate.

- External Reporting Of Information Security Violations: In conjunction with security representatives and the Information Security Manager, management must weigh the pros and cons of external disclosure before reporting these violations. Reporting security violations, problems, or vulnerabilities to any party outside UAE e-Government without the prior written approval of the IT director is strictly prohibited.

9.19 Conclusion

A clear policy need direction and management support. It requires commitment, supporting procedures, an appropriate technical framework within which it can be implemented, a suitable degree of authority, a means by which compliance can be checked and a legally agreed response in the event of it being violated. In this vein we have created the information security policy above that could be used universally across the UAE e-Government. The policy covers all area of relevance to information security and is generic in nature so that it can be applied to the specific needs of each depart-

ment within the e-Government. Applying the policy across the e-Government will facilitate greater interoperability and exchange of information between departments without causing security weaknesses.

To ensure the policy is correctly implemented and adhered to, it was proposed that a number of committees be established to oversee the adoption process and regulate any alterations that need to be made. The requirements set in this policy should apply to all workers, e-Government have access to information and information systems no matter what their status (employee, contractor, consultant, temporary, etc.). Employees that deliberately violate this and other information security policy statements should be subject to disciplinary action in accordance with the legal affairs division policies and procedures.

Chapter 10

Conclusions and Future Work

10.1 General Overview

This thesis has made a rigorous appraisal of the security of information systems for the UAE e-Government which has led to the successful certification of the departments in this case study, under the ISO 27001 programme in February 2013. As a result of this work a number of other recommendations have been adopted and led directly to improvements in the security of e-Government systems. Carrying out of a survey of workers in four e-Government departments via a comprehensive questionnaire has offered valuable insights into employee perceptions. Areas of weakness have successfully been strengthened using a targeted training intervention. Finally the insights into worker perception combined with the ISO 27001 standard have been used to produce a comprehensive information security policy which may be applied to all departments and levels of the UAE e-Government. The policy standardises the approach to security and provides a reference point for all security interventions.

In Chapter 2 the concept of e-Government was reviewed and the growing emphasis

on achieving maximum security standards highlighted, as there is a growing threat to the e-Government from cybercrime. Several countries experiences of developing their e-Government were analysed and the lessons learned from and best practises were used to develop the UAE e-Government security strategy.

Four standards of information security are evaluated in Chapter 3. The requirements of the UAE e-Government were outlined and the standards evaluated based on these. ISO 27001 can be positioned in the middle tier in security management, representing the requirement of a good information security management. ISO 27001, including 11 domains, 34 control objectives and 133 controls, is based on past experiences of information security management. It was found that ISO 27001 has the highest quantitative value and best meets the requirement of UAE e-Government. The implementation a certification standard helped government win the trust of the service users.

Chapter 4 describe the SWOT analysis and TOWS matrix used to examine both internal and external factors for the UAE e-Government. The UAE government has initiated a plan to enhance government information security. One of the basic components of this plan is e-Transformation which aims to transform the UAE into an information society. One of the two purposes of this study are to define and prioritise the strengths, weaknesses, opportunities, and threats (SWOT) groups and their subfactors for e-Government in UAE. The other purpose of this work is to determine and to evaluate the alternative strategies for e-Government applications at the national level in country.

As the work described in Chapter 5 shows, the results of Gap Analysis can help an organisation make decisions on the allocation and prioritisation of resources. In our case study, management is the weakest domain when it comes to compliance with

ISO 27001, while maturity level analysis demonstrates a clear map in the maturity of protection controls, which clearly indicates the priorities and directions to which the UAE e-Government should pay attention and improve.

Gap Analysis is an important tool for the implementation of an ISMS. This chapter uses a case study method to show the effectiveness of Gap Analysis, by interpreting the results of the UAE e-Government Gap Analysis. In the initial stage, Gap Analysis helped the UAE to find the gap between its security levels and the ISO 27001 best practices of information security. We used compliance level, MTO Model (also compliance level) and Maturity Model in the methodology to gain different Gap Analysis results in different aspects.

Risk management was the focus of Chapter 6 which provide the foundation for information security program, requiring that entities protect information commensurate with the risk and magnitude of harm that could result from its loss, misuse, unauthorized access, or modification. Risk management is the means by which sound security decisions are made and it's supporting systems through the implementation of security controls. While all systems require security, not all systems need the same level of controls. In order to reach a satisfactory level of security, the controls have to be balanced and the interactions between the various building blocks have to be taken into consideration so e-Government can reach an optimal solution.

Penetration testing plays an important role in information security management, by identifying the weaknesses of the whole management system, from technical to organisational or personnel vulnerabilities. Chapter 7 describes the tests that were carried out to test the security of UAE e-Government systems. Almost all security management is about the access control of information. Penetration tests check the gatekeepers of the management system of an organisation, logically or physically, where they help

the organisation to have a secured zone concept. The most important target of the tests are networks, applications, physical environments and infrastructures. The goals of the tests are finding the weaknesses and vulnerabilities of systems and management, and provide objective and impartial third-party monitoring to improve security management. Following the tests, recommendation were made to improve the information security of the department being tested. The e-Government is planning to enrol this test in other departments, to ensure the security of the network.

Having examined the security of the information systems from the perspective of physical vulnerability in Chapter 8 we turned to analyse the more subtle nature of the security culture held by the organisations employees. This is aspect of security is at least as important as the security of the physical information systems (as the incorrect behaviour of employees can completely undermine these) however it is often overlooked as it is less tangible to measure. We devised a questionnaire to generate a quantitative measure of the strength of the security culture and distributed to a significant sample of the employees of the four departments used as a case study. The analysis of the responses highlighted a number of areas of weakness to address which we created a bespoke training programme. The evaluation of the training showed that it was capable of producing a marked improvement in the strength of the employees information security culture.

From the work carried out, it became increasingly clear that there was a pressing need to develop a comprehensive information security policy to be adopted universally across all departments of the UAE e-Government. Through consultation with the management and with reference to the ISO 27001 standard, such a policy was developed in Chapter 9. The policy covers all area of relevance to information security and is generic nature so that it can be applied to the specific needs of each department within

the e-Government. Applying the policy across all departments will facilitate greater interoperability and exchange of information between them without causing security weaknesses.

10.2 Conclusions

In the current era of information technology and communications, governments are investing heavily in the implementation and adoption of information technology, and its incorporation in to governmental strategies. From the security perceptive, the government has to ensure maximum security standards, as the biggest threat to e-Government is cybercrime. Currently, this is an uncontrollable activity which has affected numerous domains, but can be dealt effectively with powerful technological infrastructures. The best way to maintain the e-Government structure is to implement continuous evaluation and monitoring systems, which can effectively deal with the internal and external threats.

A key contribution of this study is the highlighting of the importance of maximising risk awareness. Qualitative findings from interviews point to the importance of both technical and human dimensions to the design of the e-Government security policy. At the centre, the model e-Government policy and procedures is subject to managerial processes that identify and manage risk and incidents across e-Government security dimensions. The framework emphasises the significance of risk awareness, integrated with training and development, that supports a reflective process of continuous improvement that is vital in the continually evolving security context.

The assessment of the security culture for e-Government departments was carried out via a comprehensive questionnaire which results in valuable insights into employee

perceptions. Areas of weakness have successfully been strengthened using a targeted training intervention. The training programme was rolled out to all departments and levels of the UAE e-Government departments.

Finally, a standardised policy approach to security provides a reference point for all security interventions. To ensure the policy is correctly implemented and adhered to, we have proposed that a number of committees be establish to oversee the adoption process and regulate any alterations that need to be made. The requirements set in this policy should apply to all workers at the UAE e-Government, all workers should have access to information systems no matter what their status (employee, contractor, consultant, temporary, etc.). Employees that deliberately violate this and other information security policy statements should be subject to disciplinary action in accordance with the legal affairs division policies and procedures. We have developed an information security policy that could be utilised throughout the UAE e-Government. The arrangement covers all areas of importance to data security and is generic in nature so it can be deployed to the particular needs of every office inside the e-Government. Applying the policy will encourage better interoperability and trading of data between divisions without incurring increased security risk.

10.3 Future Work

The thesis has offered an extensive study that shows the advantages to implementing ISMS to part of the e-Government organisation. There is however some additional work which could be done to enhance the overall security of the organisation and these are outlined below:

- The e-Government organisation should appoint an information security task group

embedded within the existing departments e-Government whose primary role will be to ensure that each department is fully certified in ISO 27001 and plays a leadership role in ensuring a strong culture of information security is nurtured within all departments and at every level of the organisation. The task group should be responsible for the deployment of the single information security policy developed in this thesis to all departments of the e-Government and ensure compliance is maintained universally.

- An incident management system should be established within each department of the e-Government. His role is to flag any security incidents as they occur and ensure information is shared with other departments and devise unified mitigation measures as appropriate.

- The methods used in this thesis such as gap analysis and risk assessment must not be considered as one off measures rather they should form part of a regular rolling security audit process. The e-Government should establish a team of internal security auditors whose role will be to visit locations within the e-Government department carrying out detailed audits (gap analysis, risk assessment) on an annual basis. This process will help mitigate vulnerabilities as well as ensure the correct processes are in place to deal with any new or emerging security issues.

- The benefits of an awareness training programme have been made clear by the study. To further maximise the benefits of this type of interventions this type of training should be further expanded to a permanent rolling intervention which immediately addresses any identified weaknesses in employee awareness and quickly corrects these. This programme would need to be delivered to all new

and relocated employees but also existing employees' awareness should be closely monitored to ensure no gaps in awareness emerge. New vulnerabilities that may arise from technology changes in particular must be keenly watched and it is the role of security officers to keep abreast of development in the security world and ensure these are continuously rolled into training programmes.

- The emerging science of behaviour change and the psychology of human behaviour should be drawn on as a means to creating subtle interventions such as nudges(119) which can have a lasting and important impact on employee culture without any overhead cost. When combined with a formal training programmes these types of intervention can be particularly effective. Future research collaboration with a project such as the "Wales Centre for Behaviour Change at Bangor University" could be considered as it could very likely yield both highly effective employee security behaviour change and also lead ground-breaking research in this field.

Appendix A

Gap Analysis Compliance Forms

Compliance Gap Analysis

	Score	Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
		80 - 100	60 - 80	40 - 60	20- 40	0 - 20
A.5. Security Policy						
A.5.1 Information Security Policy						
	A.5.1.1 Is a published policy document, approved by management, published and communicated, as appropriate to all employees and relevant external third parties?					
	A.5.1.2 Is the published policy reviewed regularly, (at planned intervels) or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness?					
A.6. Organization of Information Security						
A.6.1 Internal Organization						
	A.6.1.1 Does Management actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities?					
	A.6.1.1 (a) Is a management forum in place to ensure that there is clear direction and visible management support for security initiatives?					
	A.6.1.1 (b) Does the management forum promote security through appropriate commitment and adequate resourcing?					
	A.6.1.1 (c) Is specialist advice on information security sought from either internal or external advisors and co-ordinated throughout the organization?					
	A.6.1.2 Are information security activities coordinated by representatives from different parts of the organization with relevant roles and job functions?					
	A.6.1.3 Are information security responsibilities clearly defined?					
	A.6.1.4 Is there a management authorization process in place for new information processing facilities?					
	A.6.1.5 Are confidentiality or non disclosure agreements reflecting the organization's needs for the protection of information identified, issued and regularly reviewed?					
	A.6.1.6 Does your organization maintain appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators?					
	A.6.1.7 Are contacts with appropriate special interest groups and/or other specialist security forums and/or professional associations in place and maintained?					
	A.6.1.8 Is the organizations approach to managing information security and its implementation reviewed independently at planned intervals, or when significant changes to the security implementation occur?					
A.7. Asset Management						
A.7.1 Responsibility for assets						
	A.7.1.2 Are all information and assets associated with information processing facilities owned by a designated part of the organization?					
	A.7.1.1 Is there an inventory of all important assets associated with each information system drawn up and maintained?					
	A.7.1.3 Have the rules for the acceptable use of information and assets associated with information processing facilities been identified, documented and implemented?					
A.7.2 Classification Guidelines						
	A.7.2.1 Is Information classified in terms of its value, legal requirements, sensitivity, and criticality to the organization?					
	A.7.2.2 Are procedures in place for information labeling and handling in accordance with a classification scheme adopted by					
A.8. Human Resources Security						
A.8.1 Prior to Employment						

Compliance Gap Analysis

		Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
	Score	80 - 100	60 - 80	40 - 60	20- 40	0 - 20
	A.8.1.1 Have Security roles and responsibilities for employees, contractors and third party users been defined and documented in accordance with the organizations information security policy?					
	A.8.1.2 Have background verification checks on all candidates for employment, contractors and third party users been carried					
	A.8.1.3 Have all employees, contractors and third party users agreed and signed their terms and conditions of their employment contract, which clearly states their and the organization's responsibilities for information security?					
A.8.2 During Employment						
	A.8.2.1 Has management enforced the requirement for employees, contractors and third parties to apply security in accordance with the organization's established policies and procedures?					
	A.8.2.2 Have all employees of the organization, and, where relavant, contractors and third party users received appropriate awareness training and regular updates in organiational policies and procedues, as relevant for their job function?					
	A.8.2.3 Is there a formal disciplinary process for employees who have committed a security breach?					
A.8.3 Termination or Change of Employment						
	A.8.3.1 Are responsibilities for performing employment termination or change of employment clearly defined and assigned?					
	A.8.3.2 Is there a process in place that ensures that all employees, contractors and/or third parties return all organizaional assets in their possession upon termination of their employment, contract or agreement?					
	A.8.3.3 Is there a process that ensures the access rights of all employees, contractors and/or third party users to information or information processing facilities are removed upon termination of ther employment, contract or agreement or adjusted upon change?					
A.9. Physical and environmental security						
A.9.1 Secure Areas						
	A.9.1.1 Have security perimeters been used to protect areas that contain information and information processing facilities?					
	A.9.1.2 Are the secure areas protected by appropriate entry controls to ensure that only authorized personnel have access?					
	A.9.1.3 Have secure areas been created to protect offices, rooms and facilities with special security requirements?					
	A.9.1.4 Are physical protection controls in place to protect against damge from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters?					
	A.9.1.5 Have physical protection guidelines for working in secure areas been designed and applied?					
	A.9.1.6 Are delivery and loading areas controlled and, if possible, isolated from information processing facilities to avoid unauthorized access?					
A.9.2 Equipment Security						
	A.9.2.1 Is equipment sited or protected to reduce the risks form environmental threats and hazards, and opportunities for unauthorized access?					
	A.9.2.2 Is equipment protected from power failures and other disruptions caused by failures in supporting utilities?					
	A.9.2.3 Is power and telecommunications cabling carrying data or supporting information services protected from interception or damage?					
	A.9.2.4 Is equipment correctly maintained to enable its continued availability and integrity?					
	A.9.2.5 Has security been applied to off-site equipment taking into account the different risks of working outside the organiation's premises?					
	A.9.2.6 Are all items of equipment containing storage media checked to ensure that all sensitive data and licensed software has been removed or securely overwritten prior to disposal?					

Compliance Gap Analysis

	Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
Score	80 - 100	60 - 80	40 - 60	20- 40	0 - 20
A.9.2.7 Does the removal of equipment, information or software belonging to the organization require the authorization of management?					
A.10. Communications and Operations Management					
A.10.1 Operational procedures and responsibilities					
A.10.1.1 Are operating procedures documented, maintained and available for all users who need them?					
A.10.1.2 Are changes to information processing facilities and systems controlled?					
A.10.1.3 Are duties and areas of responsibility segregated to reduce opportunities for unauthorized or unitentional modification or misuse of organzational assets?					
A.10.1.4 Are development, test and operational facilities separated to reduce the risk of unauthorized access or changes to the operational system?					
A.10.2 Third Party Service Delivery Management					
A.10.2.1 Are security controls, service definitions and delivery levels included in the third party service delivery agreement					
A.10.2.2 Are services, reports and records provided by the third party regularly monitored and reviewed, and audited on a regular basis?					
A.10.2.3 Are changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls managed? Taking account of the criticality of business systems and processes involved in the re-assessment of risks.					
A.10.3 System Planning and Acceptance					
A.10.3.1 Are capacity demands monitored and projections of future capacity requirements made to enable adequate processing power and storage to be made available?					
A.10.3.2 Are acceptance criteria established for new information systems, upgrades and new versions and suitable tests					
A.10.4 Protection against Malicious Code					
A.10.4.1 Are detection and prevention controls to protect against malicious software and appropriate user awareness procedures implemented?					
A.10.4.2 Are controls in place to ensure that mobile code operates according to clearly defined security policy, and unauthorized code is prevented from executing?					
A.10.5 Back-up					
A.10.5.1 Are controls in place to ensure backup copies of information and software are taken and tested regularly in accordance with the organizational backup policy?					
A.10.6 Network Security Management					
A.10.6.1 Are the organization's networks adequately controlled, in order to be protected from threats, and to maintain					
A.10.6.2 Have all security features, service levels, and management requirments of all network services been identified and included in any network services agreement, whether these services are provided in-house or outsourced?					
A.10.7 Media Handling					
A.10.7.1 Are procedures in place for the management of removable media?					
A.10.7.2 Are formal procedures in place for the secure and safe disposal of media when no longer required?					
A.10.7.3 Are procedures for the handling and storage of information established to protect information from unauthorized					
A.10.7.4 Are controls in place to ensure system documentation is protected against unauthorized access?					
A.10.8 Exchange of Information					
A.10.8.1 Are formal exchange policies, procedures, and controls in place to protect the exchange of information through the use of all types of communications facilities?					

Compliance Gap Analysis

		Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
	Score	80 - 100	60 - 80	40 - 60	20- 40	0 - 20
	A.10.8.2 Are agreements established for the exchange of information and software between the organization and external parties?					
	A.10.8.3 Is media containing information protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundaries?					
	A.10.8.4 Is information involved in electronic messaging appropriately protected?					
	A.10.8.5 Are policies and procedures developed and implemented to protect information associated with interconnection of business information systems?					
A.10.9 Electronic Commerce						
	A.10.9.1 Are controls in place to ensure information involved in electronic commerce passing over public networks are adequately protected from fraudulent activity, contract dispute, and unauthored disclosure and modification?					
	A.10.9.2 Are controls in place to ensure information involved in on-line transactions are protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay?					
	A.10.9.3 Are controls in place to protect and ensure the integrity of information being made available on publicly available systems from unauthorized modification?					
A.10.10 Monitoring						
	A.10.10.1 Are audit logs recording user activities, exceptions, and information security events produced and kept for an agreed period to assist in future investigations and access control monitoring?					
	A.10.10.2 Are procedures established for the monitoring and review of information processing facilities on a regular basis?					
	A.10.10.3 Are logging facilities and log information protected against tampering and unauthorized access?					
	A.10.10.4 Are system administrator and operator activities logged?					
	A.10.10.5 Are faults logged, analyzed and appropriate actions taken?					
	A.10.10.6 Are clocks of all relevant information processing systems within the organization and/or security domain synchronized with an agreed accurate time source?					
A.11. Access Control						
A.11.1 Business requirements for Access Control						
	A.11.11.1 Has an access control policy been established, documented and reviewed based on business and security requirments for access?					
A.11.2 User Access Management						
	A.11.2.1 Is there a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services?					
	A.11.2.2 Are the allocation of Privileges restricted and controlled?					
	A.11.2.3 Is there a formal Management process that controls the allocation of Passwords?					
	A.11.2.4 Is there a formal Management process for the review of users "Access Rights" at regular intervals?					
A.11.3 User Responsibilities						
	A.11.3.1 Does the organization follow good security practices for the selection and use of Passwords?					
	A.11.3.2 Are user controls in place to ensure unattended equipment is appropriately protected?					
	A.11.3.3 Has a Clear Screen, Clear Desk policy been adopted for papers and removable storage media?					
A.11.4 Network Access Control						
	A.11.4.1 Are users only provided with access to the services that they have been specifically authorized to use?					
	A.11.4.2 Are appropriate authentication methods used to control access by remote users?					
	A.11.4.3 Have automatic equipment identification methods been considered as a means to authenticate connections from specific locations and equipment?					

Compliance Gap Analysis

		Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
	Score	80 - 100	60 - 80	40 - 60	20- 40	0 - 20
	A.11.4.4 Are physical and logical access to diagnostic and configuration ports controlled?					
	A.11.4.5 Are controls in place in networks to segregate groups of information services, users and information systems?					
	A.11.4.6 Is the connection capability of users in shared networks restricted in line with the access control policy?					
	A.11.4.7 Do shared networks have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications?					
A.11.5 Operation System Access Control						
	A.11.5.1 Is access to information services via a secure logon process?					
	A.11.5.2 Are users provided with a unique identifier (user ID) for their personal and sole use so that activities are traceable to individuals and has a suitable authentication technique been chosen to substantiate the claimed identity of a user?					
	A.11.5.3 Are password management systems in place that provide an effective, interactive facility for the provision of quality passwords?					
	A.11.5.4 Is the use of system utility programs restricted and tightly controlled?					
	A.11.5.5 Are interactive sessions shut down after a defined period of inactivity?					
	A.11.5.6 Are there restrictions on the connection times to high-risk applications to provide additional security?					
A.11.6 Information Access Restriction						
	A.11.6.1 Is access to information and application system functions by users and support personnel restricted in accordance with the access control policy?					
	A.11.6.2 Do sensitive systems have a dedicated (isolated) computing environment?					
A.11.7 Mobile Computing and Communications						
	A.11.7.1 Is there a formal policy in place and have appropriate controls been adopted to protect against the risks of working with mobile computing facilities, especially in unprotected environments?					
	A.11.7.2 Are there policies, procedures and standards in place to authorize and control teleworking activities?					
A.12. Information Systems Acquisition, Development and Maintenance						
A.12.1 Security requirmements of information systems						
	A.12.1.1 Do business requirements for new systems or enhancements to existing systems specify the requirements for security controls?					
A.12.2 Correct processing of applications						
	A.12.2.1 Is data input to application systems validated to ensure that it is correct and appropriate?					
	A.12.2.2 Are there validation checks incorporated into systems to detect corruption of the data processed?					
	A.12.2.3 Has a message authentication system been implemented where there is a security requirement to protect the integrity of the message content?					
	A.12.2.4 Is data output from application systems validated to ensure that the processing of stored information is correct and					
A.12.3 Cryptographic Controls						
	A.12.3.1 Is there a policy on the use of cryptographic controls for the protection of information developed and implemented?					
	A.12.3.2 Is a key management system used to support the use of cryptographic techniques, based on an agreed set of standards, procedures and methods?					
A.12.4 Security of System files						
	A.12.4.1 Are procedures in place to control the implementation of software on operational systems?					
	A.12.4.2 Is test data protected and controlled?					
	A.12.4.3 Is strict control maintained over access to program source libraries?					
A.12.5 Security in development and support processes						

Compliance Gap Analysis

		Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
	Score	80 - 100	60 - 80	40 - 60	20- 40	0 - 20
	A.12.5.1 Are there strict formal change control procedures for the implementation of changes?					
	A.12.5.2 Are business critical applications reviewed and tested after operating systems are changed to ensure no adverse					
	A.12.5.3 Are modifications to software packages discouraged and any essential changes strictly controlled?					
	A.12.5.4 Are controls in place to prevent the opportunity for information leakage?					
	A.12.5.5 Are controls applied to secure outsourced software development?					
A.12.6 Technical Vulnerability Management						
	A.12.6.1 Is timely information about technical vulnerabilities of systems being obtained and used? and are appropriate measures being taken to address and evaluate the associated risks?					
A.13. Information Security Incident Management						
A.13.1 Reporting Information Security events and weaknesses						
	A.13.1.1 Are Information security events reported through the appropriate management channels as quickly as possible?					
	A.13.1.2 Are all employees, contractors and third party users of information systems and services, required to note and report any observed or suspected security weaknesses in systems and services?					
A.13.2 Management of Information Security incidents and improvements						
	A.13.2.1 Are management responsibilities and procedures established to ensure a quick, effective, and orderly response to information security incidents?					
	A.13.2.2 Are mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored?					
	A.13.2.3 Is evidence collected, retained, and presented to conform to the rules for evidence laid down in the relevant					
A.14. Business Continuity Management						
A.14.1 Information security aspects of business continuity management						
	A.14.1.1 Is there a managed process in place for developing and maintaining business continuity across the organization?					
	A.14.1.2 Has a risk assessment or business impact analysis been undertaken that identifies the interruptions and probabilities of such interruptions together with their consequences for information security?					
	A.14.1.3 Are plans developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes?					
	A.14.1.4 Is a single framework of business continuity plans maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance?					
	A.14.1.5 Are business continuity plans tested regularly and maintained by regular reviews to ensure they are up to date and effective?					
A.15. Compliance						
A.15.1 Compliance with legal requirements						
	A.15.1.1 Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?					
	A.15.1.2 Are appropriate procedures implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of propriety software products?					
	A.15.1.3 Are important records of the organization protected from loss, destruction and falsification in accordance with statuatory, regulatory, contractual and business requirements?					
	A.15.1.4 Are there controls applied to protect personal information in accordance with relevant legislation, regulations and if applicable, contractual clauses?					
	A.15.1.5 Is there management authorization for the use of information processing facilities and are controls applied to prevent the misuse of such facilities for unauthorized purposes?					

Compliance Gap Analysis

		Compliant	Largely Compliant	Currently Compliant	Partly Compliant	Not compliant
	Score	80 - 100	60 - 80	40 - 60	20- 40	0 - 20
	A.15.1.6 Are controls in place to ensure compliance with national agreements, laws, regulations or other instruments to					
A.15.2 Compliance with security policies and standards, and technical compliance						
	A.15.2.1 Do managers take action to ensure that all security procedures within their area of responsibility are carried out correctly to achive complaince to security policies and standards?					
	A.15.2.2 Are information systems regularly checked for compliance with security implementation standards?					
A.15.3 Information systems audit considerations						
	A.15.3.1 Are all audits of operational systems carefully planned and agreed to minimize the risk of disruptions to business processes?					
	A.15.3.2 Is access to system audit tools protected to prevent possible misuse or compromise?					

References

[1] J. Singels, G. Ruel, and H. Van de Water, "Iso 9000 series-certification and performance," *International Journal of Quality & Reliability Management*, vol. 18, no. 1, pp. 62–75, 2001. 2

[2] M. Terziovski and D. Power, "Increasing iso 9000 certification benefits: a continuous improvement approach," *International Journal of Quality & Reliability Management*, vol. 24, no. 2, pp. 141–163, 2007. 2

[3] E. H. Freeman, "Holistic information security: Iso 27001 and due care," *Information Systems Security*, vol. 16, no. 5, pp. 291–294, 2007. 3

[4] J. S. Lim, A. Ahmad, S. Chang, and S. B. Maynard, "Embedding information security culture emerging concerns and challenges.," in *PACIS*, p. 43, 2010. 3

[5] H. Fulford and N. F. Doherty, "The application of information security policies in large uk-based organizations: an exploratory investigation," *Information Management & Computer Security*, vol. 11, no. 3, pp. 106–114, 2003. 3

[6] B. Von Solms and R. Von Solms, "The 10 deadly sins of information security management," *Computers & Security*, vol. 23, no. 5, pp. 371–376, 2004. 3

[7] E. E. Anderson and J. Choobineh, "Enterprise information security strategies," *Computers & Security*, vol. 27, no. 1, pp. 22–29, 2008. 4, 104

[8] S. Paquette, I. Fagnot, K. C. Desouza, D. Yates, and S. M. Ho, "Information assurance, intelligence and security: Opportunities and directions for future research," 2008. 4

[9] S. Alateyah, R. M. Crowder, and G. B. Wills, "An exploratory study of proposed factors to adopt e-government services," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 11, 2013. 5

[10] G. Karokola, S. Kowalski, and L. Yngström, "Evaluating a framework for securing e-government services–a case of tanzania," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pp. 1792–1801, IEEE, 2013. 5

[11] J. K. Bakari, C. N. Tarimo, L. Yngstrom, and C. Magnusson, "State of ict security management in the institutions of higher learning in developing countries: Tanzania case study," in *Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference on*, pp. 1007–1011, IEEE, 2005. 5

[12] F.-M. Hsu, T.-Y. Chen, and S. Wang, "Efficiency and satisfaction of electronic records management systems in e-government in taiwan," *The Electronic Library*, vol. 27, no. 3, pp. 461–473, 2009. 6

[13] M. Hafiz, P. Adamczyk, and R. E. Johnson, "Organizing security patterns," *IEEE software*, vol. 24, no. 4, 2007. 7, 8

[14] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & Security*, vol. 23, no. 3, pp. 191–198, 2004. 7

[15] M. Kabay, "Improving information assurance education key to improving secure (ity) management," *Journal of Network and Systems Management*, vol. 13, no. 3, pp. 247–251, 2005. 7

[16] A. Da Veiga and J. H. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security*, vol. 29, no. 2, pp. 196–207, 2010. 7

[17] C. S. Leem, S. Kim, and H. J. Lee, "Assessment methodology on maturity level of isms," in *Knowledge-Based Intelligent Information and Engineering Systems*, pp. 609–615, Springer, 2005. 8, 90

[18] J. Wade, "The weak link in it security," *Risk Management*, vol. 51, no. 7, p. 32, 2004. 8

[19] M. E. Thomson and R. von Solms, "Information security awareness: educating your users effectively," *Information management & computer security*, vol. 6, no. 4, pp. 167–173, 1998. 8

[20] M. E. Paté-Cornell and R. L. Dillon, "The respective roles of risk and decision analyses in decision support," *Decision Analysis*, vol. 3, no. 4, pp. 220–232, 2006. 9

[21] H. Weihrich, "The tows matrix?a tool for situational analysis," *Long range planning*, vol. 15, no. 2, pp. 54–66, 1982. 17, 76

[22] C. H.-B. Lynda Lee Kaid, "Encyclopedia of political communication," 2007. eBook. 17

[23] A. Kolsaker and L. Lee-Kelley, "Citizens' attitudes towards e-government and e-governance: a uk study," *International Journal of Public Sector Management*, vol. 21, no. 7, pp. 723–738, 2008. 19

[24] M. A. Alshehri and S. Drew, "E-government fundamentals," in *IADIS International Conference on ICT, Society and Human Beings 2010*, IADIS International Association for Development of the Information Society, 2010. 20

[25] T. Carrizales, "Functions of e-government: A study of municipal practices," *State & Local Government Review*, pp. 12–26, 2008. 21

[26] K. Layne and J. Lee, "Developing fully functional e-government: A four stage model," *Government information quarterly*, vol. 18, no. 2, pp. 122–136, 2001. 22

[27] U. Government, "UAE Vision 2021." `http//www.vision2021.ae` Accessed on 2/6/2013. 26

[28] A. M. Al-Khouri, "An innovative approach for e-government transformation," *arXiv preprint arXiv:1105.6358*, 2011. 27, 29

[29] D. Westland and A. M. Al-Khouri, "Supporting e-government progress in the united arab emirates," *Journal of E-Government Studies and Best Practices*, vol. 2010, pp. 1–9, 2010. 28

[30] UN, "E-government survey: E-government for the people," 2012. 30

[31] Z. Fang, "E-government in digital era: concept, practice, and development," *International journal of the Computer, the Internet and management*, vol. 10, no. 2, pp. 1–22, 2002. 31

[32] V. Ndou, "E-government for developing countries: opportunities and challenges," *The Electronic Journal of Information Systems in Developing Countries*, vol. 18, 2004. 31

[33] A. Avny, "Swot analysis of e-government," *Annals University of Bucharest, Economics and Administrative Series*, 2007. 32, 72

[34] S. Sinawong, "The influential factors and challenges in implementing e-government in cambodia," in *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on*, vol. 2, pp. 973–979, IEEE, 2008. 32

[35] H. Mohammad, T. Almarabeh, and A. A. Ali, "E-government in jordan," *European Journal of Scientific Research*, vol. 35, no. 2, pp. 188–197, 2009. 33

[36] M. A. Hjouj Btoush, *Evaluation of e-government services in Jordan: providers' and users' perceptions*. PhD thesis, Sheffield Hallam University, 2009. 33

[37] A. Rokhman, "E-government adoption in developing countries; the case of indonesia," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 2, no. 5, pp. 228–236, 2011. 34

[38] A. J. Chen, S. L. Pan, J. Zhang, W. W. Huang, and S. Zhu, "Managing e-government implementation in china: A process perspective," *Information & Management*, vol. 46, no. 4, pp. 203–212, 2009. 34

[39] A. Tat-Kei Ho, "Reinventing local governments and the e-government initiative," *Public administration review*, vol. 62, no. 4, pp. 434–444, 2002. 34

[40] C. W. Tan and S. L. Pan, "Managing e-transformation in the public sector: an e-government study of the inland revenue authority of singapore (iras)," *European Journal of Information Systems*, vol. 12, no. 4, pp. 269–281, 2003. 34

[41] C. M. Chan, R. Hackney, S. L. Pan, and T.-C. Chou, "Managing e-government system implementation: a resource enactment perspective," *European Journal of Information Systems*, vol. 20, no. 5, pp. 529–541, 2011. 34

[42] C. M. Chan, Y. Lau, and S. L. Pan, "E-government implementation: A macro analysis of singapore's e-government initiatives," *Government Information Quarterly*, vol. 25, no. 2, pp. 239–255, 2008. 34

[43] R. Heeks *et al.*, *Most eGovernment-for-development projects fail: how can risks be reduced?* Institute for Development Policy and Management, University of Manchester Manchester, 2003. 34

[44] J. B. Joshi, A. Ghafoor, W. G. Aref, and E. H. Spafford, "Security and privacy challenges of a digital government," in *Advances in Digital Government*, pp. 121–136, Springer, 2002. 39

[45] I. Al-Mayahi and P. M. Sa'ad, "Iso 27001 gap analysis-case study," in *Proceedings of the International Conference on Security and Management (SAM)*, p. 1, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012. 40

[46] "BSI-Standard 1001-1 Information Security Management Systems." `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile` Accessed on 2/6/2012, May 2010. 40

[47] M. Dey, "Information security management-a practical approach," in *AFRICON 2007*, pp. 1–6, IEEE, 2007. 40, 81

[48] W. Boehmer, "Cost-benefit trade-off analysis of an isms based on iso 27001," in *Availability, Reliability and Security, 2009. ARES'09. International Conference on*, pp. 392–399, IEEE, 2009. 42

[49] A. Calder and S. Watkins, "It governance: A manager's guide to data security and iso 27001/iso 27002," 2008. 44

[50] A. Berger, "Continuous improvement and: standardization and organizational designs," *Integrated manufacturing systems*, vol. 8, no. 2, pp. 110–117, 1997. 46

[51] J. S. Broderick, "Isms, security standards and security regulations," *information security technical report*, vol. 11, no. 1, pp. 26–31, 2006. 50

[52] R. Tregear and T. Jenkins, "Government process management: A review of key differences between the public and private sectors and their influence on the achievement of public sector process management.," *BPTrends, October 2007*, 2007. 54

[53] A. Calder and J. Van Bon, *Implementing information security based on ISO 27001/ISO 17799: a management guide*. Van Haren Publishing, 2006. 54

[54] A. Calder, *Iso27001/Iso27002 a Pocket Guide*. IT Governance Ltd, 2008. 55, 83

[55] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, "Information security fortification by ontological mapping of the iso/iec 27001 standard," in *Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on*, pp. 381–388, IEEE, 2007. 57

[56] T. Carlson, H. Tipton, and M. Krause, *Understanding Information Security Management Systems*, vol. 2. Auerbach Publications Boca Raton, FL, 2008. 57

[57] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining itil, cobit and iso/iec 27002 in order to design a comprehensive it framework in organizations," in *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, pp. 749–753, IEEE, 2008. 57, 60, 64

[58] G. Hardy, "Using it governance and cobit to deliver value with it and respond to legal, regulatory and compliance challenges," *Information Security technical report*, vol. 11, no. 1, pp. 55–61, 2006. 58

[59] "COBIT 4.1: Framework for IT Governance and Control ." `http://www.isaca.org/knowledge-center/cobit/Pages/Overview.aspx`Accessed on 3/11/2010. 58

[60] J. W. Lainhart IV, "Cobit?: A methodology for managing and controlling information and information technology risks and vulnerabilities," *Journal of Information Systems*, vol. 14, no. s-1, pp. 21–25, 2000. 60

[61] R. R. Moeller, *COSO enterprise risk management: understanding the new integrated ERM framework*. Wiley. com, 2007. 61, 62

[62] A. Cartlidge, A. Hanna, C. Rudd, I. Macfarlane, J. Windebank, and S. Rance, "An introductory overview of itil v3," *The UK Chapter of the itSMF*, 2007. 64

[63] P. Hill and K. Turbitt, "Combine itil and cobit to meet business challenges," *BMC Software*, 2006. 64

[64] M. Kneller, "Executive briefing: The benefits of itil®," *Whitepaper. Luettavissa*, 2010. 64

[65] R. G. Dyson, "Strategic development and swot analysis at the university of warwick," *European journal of operational research*, vol. 152, no. 3, pp. 631–640, 2004. 72

[66] S. L. Mansar, "e-government implementation: impact on business processes," in *Innovations in Information Technology, 2006*, pp. 1–5, IEEE, 2006. 72

[67] I. Al-Mayahi and S. P. Mansoor, "Uae e-goverment: Swot analysis and tows matrix," in *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on*, pp. 201–204, IEEE, 2012. 73

[68] T. Wiander, "Implementing the iso/iec 17799 standard in practice: experiences on audit phases," in *Proceedings of the sixth Australasian conference on Information security-Volume 81*, pp. 115–119, Australian Computer Society, Inc., 2008. 80

[69] T. Valdevit, N. Mayer, and B. Barafort, "Tailoring iso/iec 27001 for smes: A guide to implement an information security management system in small settings," in *Software Process Improvement*, pp. 201–212, Springer, 2009. 81

[70] B. Karabacak and I. Sogukpinar, "A quantitative method for iso 17799 gap analysis," *Computers & Security*, vol. 25, no. 6, pp. 413–419, 2006. 81, 165

[71] A. Calder, *Information security based on ISO 27001/ISO 17799: a management guide*. Van Haren Publishing, 2006. 83

[72] I. Al-Mayahi and S. Mansoor, "Iso 27001 gap analysis-case study," in *Proceedings of the 2012 International Conference on Security and Management (SAM'12), Las Vegas, USA*, World Congress in Computer Science, 2012. 89

[73] A. Pederiva, "The cobit® maturity model in a vendor evaluation case," *Information Systems Control Journal*, vol. 3, pp. 26–29, 2003. 90

[74] D. M. Ahern, A. A. CLOUSE, and R. A. TURNER, *CMMI distilled: a practical introduction to integrated process improvement*. Addison-Wesley Professional, 2004. 90

[75] S. Woodhouse, "An isms (im)-maturity capability model," in *Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on*, pp. 242–247, IEEE, 2008. 90

[76] R. W. Perry, "Incident management systems in disaster management," *Disaster Prevention and Management*, vol. 12, no. 5, pp. 405–412, 2003. 98

[77] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special publication*, vol. 800, no. 30, pp. 800–30, 2002. 103

[78] M. Gerber and R. von Solms, "From risk analysis to security requirements," *Computers & Security*, vol. 20, no. 7, pp. 577–584, 2001. 103

[79] S. C. Shih and H. J. Wen, "Building e-enterprise security: a business view," *Information Systems Security*, vol. 12, no. 4, pp. 41–49, 2003. 104

[80] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002. 104

[81] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information systems security policies: a contextual perspective," *Computers & Security*, vol. 24, no. 3, pp. 246–260, 2005. 104

[82] N. Sklavos and P. Souras, "Economic models & approaches in information security for computer networks.," *IJ Network Security*, vol. 2, no. 1, pp. 14–20, 2006. 104

[83] B. Blakley, E. McDermott, and D. Geer, "Information security is information risk management," in *Proceedings of the 2001 workshop on New security paradigms*, pp. 97–104, ACM, 2001. 105

[84] M. E. Whitman and H. J. Mattord, *Management of information security*. CengageBrain. com, 2010. 105

[85] C. L. Pritchard, *Risk Management: Concepts and Guidance 4th edition*. ESI international, 2010. 105

[86] C. Alberts and A. Dorofee, "Managing information security risks: The octavesm approach," *Estados Unidos. Addison Wesley*, 2002. 111

[87] I. 27001, "Matrices for Asset Valuation and Risk Analysis ." `http://www.iso27001security.com/ISO27k_Matrices_for_Asset_Valuation_and_Risk_Analysis.pdf` Accessed on 1/3/2012. 116

[88] V. Visintine, "An introduction to information risk assessment," *SANS institute*, vol. 8, 2003. 116

[89] G. McGraw, *Software security: building security in*, vol. 1. Addison-Wesley Professional, 2006. 126

[90] A. G. Bacudio, X. Yuan, B.-T. B. Chu, and M. Jones, "An overview of penetration testing," *International Journal*, vol. 3, 2011. 127

[91] V. Lui, "Penetration testing: The white hat hacker." http://www.issa.org/Library/Journals/2007/July/Lui72007 Accessed on 7/3/2013. 127

[92] J. P. McDermott, "Attack net penetration testing," in *Proceedings of the 2000 workshop on New security paradigms*, pp. 15–21, ACM, 2001. 127

[93] N. A. Naik, G. D. Kurundkar, S. D. Khamitkar, and N. V. Kalyankar, "Penetration testing: A roadmap to network security," *arXiv preprint arXiv:0912.3970*, 2009. 128

[94] B. Linux, "Penetration Testing Distribution." http://www.backtrack-linux.org/ Accessed on 2/2/2012. 136

[95] "KISMET." http://www.kismetwireless.net/ Accessed on 2/12/2012, May 2010. 136

[96] N. org, "Nmap Security Scanner." http://nmap.org/ Accessed on 5/11/2012. 136

[97] T. N. Security, "Nessus Vulnerability Scanner." http://www.tenable.com/products/nessus Accessed on 5/11/2012. 136

[98] C. Net, "Nikto2." http://www.cirt.net/Nikto2 Accessed on 11/12/2012. 136

[99] T. G. N. Project, "Netcat." http://netcat.sourceforge.net/ Accessed on 17/12/2012. 136

[100] W. Organisation, "Wireshark." http://www.wireshark.org/ Accessed on 1/12/2012. 136

[101] W3af, "Web Application Attack and Audit Framework." http://www.wireshark.org/ Accessed on 13/12/2012. 136

[102] Yersinia, "Yersinia network tool." http://www.yersinia.net/ Accessed on 16/12/2012. 136

[103] "OXID.IT." http://www.oxid.it/cain.html/ Accessed on 12/12/2012, May 2010. 136

[104] P. W. Security, "Portswigger." http://portswigger.net/index.html Accessed on 1/12/2012. 136

[105] J. S. Lim, S. Chang, S. Maynard, and A. Ahmad, "Exploring the relationship between organizational culture and information security culture," in *Australian Information Security Management Conference*, p. 12, 2009. 157

[106] K.-S. Hong, Y.-P. Chi, L. R. Chao, and J.-H. Tang, "An integrated system theory of information security management," *Information Management & Computer Security*, vol. 11, no. 5, pp. 243–248, 2003. 158

[107] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. Wiley. com, 2001. 158

[108] C. W. Axelrod, *Outsourcing information security*. Artech house, 2004. 158

[109] P. Chia, S. Maynard, and A. Ruighaver, "Understanding organizational security culture," *Proceedings of PACIS2002. Japan*, 2002. 158

[110] U. Nation, "E-government for the people," 2012. 159

[111] I. Al-Mayahi and S. P. Mansoor, "Information security culture assessment: Case study," *(ICIST 2013)IEEE Third International Conference on Information Science and Technology, Yangzhou, China*, 2013. 159

[112] H. N. Higgins, "Corporate system security: towards an integrated management approach," *Information Management & Computer Security*, vol. 7, no. 5, pp. 217–222, 1999. 161

[113] K. Höne and J. H. P. Eloff, "Information security policyŮwhat do international information security standards say?," *Computers & Security*, vol. 21, no. 5, pp. 402–409, 2002. 161, 189

[114] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," *Journal of Management Information Systems*, vol. 28, no. 2, pp. 203–236, 2011. 168

[115] J. Rothschild and T. D. Miethe, "Whistle-blower disclosures and management retaliation the battle to control information about organization corruption," *Work and occupations*, vol. 26, no. 1, pp. 107–128, 1999. 181

[116] G. Hinson, "Information security awareness," *Handbook of research on social and organizational liabilities in information security*, 2009. 182

[117] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly*, vol. 34, no. 3, pp. 523–548, 2010. 182

[118] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2010. 189

[119] P. John, G. Smith, and G. Stoker, "Nudge nudge, think think: two strategies for changing civic behaviour," *The Political Quarterly*, vol. 80, no. 3, pp. 361–370, 2009. 241