Hull University Business School

An Information Systems Security Framework For The e-Government Programme of Jordan

Nadia Khaled Ali Samara

PhD Dissertation

University of Hull

2019

Nadia Samara

BSc, MSc.

A dissertation submitted in partial fulfilment of the requirement of the University of Hull for the degree of Doctor of Philosophy

May 2019

Signature: …….

Date: …….

Abstract

Any e-government programme provides e-services as one of the most important means by which the interaction between citizens, businesses and governments takes place. This has brought great opportunities but also raises serious cybersecurity challenges. Critical information assets are facing various potential security risks and threats. Information systems security is necessary to mitigate those risks and threats that are faced by the e-government programme and to safeguard the confidentiality, integrity and availability of the available e-services. In light of the above, the aim of this study is to examine how information security is managed and approached within e-government programmes and the case study of the Ministry of ICT in Jordan informs that aim. The study deconstructs information security through the Technical/Formal/Informal (TFI) framework and enriches that framework by customising it for e-government, expanding it also to include citizens' online trust. To achieve this aim, a qualitative investigation of the Jordanian e-government programme was conducted by following the research design of a case study in the interpretivist tradition. Furthermore, a survey was used as a complementary phase to examine citizens' perspectives on e-government security. By combining, analysing and reflecting on the empirical data, a consolidated information security framework was developed for different security aspects, based on the TFI model (technical, formal and informal). The dissertation contributes to the knowledge domain at the intersection of e-government and cybersecurity both practically and theoretically, focusing on technical aspects and non-technical aspects as well. The proposed framework provides an overview of the TFI-categorised elements that can help governments reflect on and manage the security challenges of their corresponding e-government programmes.

Acknowledgements

A journey of a thousand miles begins with a single step. Pursuing a Doctorate of Philosophy degree (PhD) was always my dream and my ambition. This dream would not have been achieved without the guidance and help of many individuals around me who assisted in the preparation and completion of this study.

Firstly, my sincere thanks and deep gratitude goes to my main supervisor, Dr. Dionysios Demetis for his guidance, support, critique and encouragement that helps me to reach this stage. His wide knowledge, constructive comments and logical way of thinking have been of great value. Without his understanding, patience, and continuous support this piece of work would never have been completed.

Additionally, I would like to extend my sincere gratitude to my second supervisor Professor Yasmin Merali for her valuable advice and encouragement. Also my sincere gratitude goes to my colleagues and research office staff at HUBS for their valuable support. Furthermore, my extended appreciation goes to individuals at MoICT in Jordan for their generosity and support during the empirical work. I would also like to thank people in Jordan for their cooperation in providing valuable information in the process of data collection.

Finally, I wish to dedicate this work to my parents and my family.

— Thank You God —

Dedication

— To my Family —

Contents

List of Figures

List of Tables

List of Abbreviations

Term	Description
CIRT	Computer Incidents Response Team
G2B	Government to Business
G2C	Government to Citizens
G2G	Government to Government
GSB	Government Secure Bus
ISMS	Information Security Management System
IS	Information Systems
ISS	Information Systems Security
IT	Information Technology
ICT	Information and Communications Technology
KS	Knowledge Station
MoICT	Ministry of Information and Communications Technology
NITC	National Information Technology Centre
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SGN	Secure Government Network
SSO	Single Sign on
UN	United Nations

1.0 Introduction

1.1 Background to e-Government in Jordan

This section provides an overview of e-government and the initiatives that the government of Jordan has taken to establish a coherent programme in this regard. A timeline of the recent e-government developments in Jordan is also presented.

The world has seen a transformation through the use of Information and Communications Technologies (ICT) that has brought about a number of innovations, such as e-banking, e-business, e-learning and e-services, and so on. Such innovations were brought into both the public and private sectors and have numerous advantages. The activities of the public sector in utilising ICT in order to enhance existing procedures, improve performance, establish better connections inside civil society, have given citizens and organisations access to online government services that have improved efficiency and effectiveness, being together known as an *e-government programme* (Yang & Maxwell, 2011).

As stated on the World Bank's e-government website, 'e-government' refers to the utilisation by government organisations of advanced information technologies, such as the Internet and mobile and wide-area networks, that can change its relations with citizens, organisations, and different government institutions. These advancements can serve a mixture of diverse objectives: greater citizen empowerment through access to information, more productive government administration, improved service delivery, a single point of contact for all government entities, facilitating the sharing and exchanging of data, and increased e-business. The subsequent advantages can be less corruption, expanded transparency, greater convenience, income development, and a decrease in expenses (Shannak, 2013). In addition, service-driven organisations work through a variety of channels, including retailers, banks and post offices. Fruitful e-government programmes ought to have the capacity to draw in citizens who are already connected to the Internet, move citizens online who are not there currently, and empower changes to e-government at three levels: government-to-government (G2G), government-to-business (G2B) and government-to-citizen (G2C) (Reffat, 2003).

The e-government programme provides services to governments and different stakeholders (citizens, businesses, public employees, and other government organisations and departments) who deal with the government.

The category of government to citizens (G2C) includes the relationships between government and citizens. This involves all interactions and communications between governments and citizens using e-government services via the programme systems and websites. The relationship between government and citizens is considered to be the most important category in an e-government programme (Al-Rashidi, 2013).

The relationships between government and businesses (private sector) are included in the category of government to business (G2B). This category covers the activities and services provided by the public sector to the private sector through the Internet (Rowley, 2011).

According to (Seifert, 2003; Yong, 2005), the government to government (G2G) category can be described as the backbone of the e-government system. The relationships in this category are important to improve the effectiveness and efficiency of e-services by allowing different government organisations and departments to share information resources, databases, and exchange services. Moreover, the use of G2G to deliver the service provides the ability to speed up the communication among public organisations and government departments, save time, reduce cost, eliminate corruption and improve the performance and productivity of the government (Lee et al., 2005; Klischewski, 2011).

The government to employee (G2E) category includes the communication and interaction between the government and its employees. The services of the G2E category allows the public sector to communicate better internally by improve internal processes and minimise administration costs. A number of scholars like (Seifert & Petersen, 2002) consider government to employee (G2E) as a subsection of the government to government (G2G) category that aims to enhance daily operations and control bureaucracy within citizens transactions. In general, the focus of this dissertation is mostly on the G2G and G2C due to the research focus areas, information security and citizens' online trust, as will be clarified in the next section.

In the context of Jordan, this is a small nation in the Middle East, with a population of around 6.5 million (according to a 2013 census) and limited resources (CountryEconomy, 2014). Jordan's e-government programme was introduced in 2001. As indicated by the official Jordanian e-government website, the vision of the programme is to be:

> "An essential and active participant in the economic and social development through the use of information and communication technology to enable easy access to government information and services for all Users regardless of their geographic location or economic status or professional capacity" (Shannak, 2013 ,p .194).

The main institution that is responsible for the e-government programme is the Ministry of Information and Communications Technology (MoICT). As stated above, the programme offers significant opportunities for Jordan, being intended to help the country in its social and economic improvement. In order to achieve the vision of the e-government programme, the ministry had set up a *Strategy for Implementation and Development* by mid-2006. This strategy was created because of a gap between government plans and the actual results of executing different e-government projects. This gap forced government leaders to defer part of the implementation stages for further appraisal (MoICT, 2014).

The e-government programme in Jordan is committed to providing e-services to individuals across society, independent of area, monetary status, training, or technological infrastructure. The e-government portal was launched in 2006 by the MoICT and was intended to provide stakeholders with government information and services. The portal was designed to coordinate all government elements in a consistent way. According to the official Jordanian e-government website, the programme mission is to oversee change in government performance and to concentrate on the satisfaction of the beneficiaries, accomplishing this through different channels by providing e-services that utilise advanced technology, information management, and by hiring experienced staff to execute e-government projects and activities that will be simple to use as well as being worthy of the citizens of Jordan. Indeed, the e-government programme has contributed to creating and administering e-transformation in the Jordanian government. To accomplish its mission, the e-government programme relies on the following: (a) e-services applications; (b) technological infrastructure improvement and definition; (c) structuring

the legislative and regulatory environment; (d) redesigning successful processes; (e) change and improvement in the areas of training, education and information exchange; and (f) rebuilding government organisations and change management (E-government-Jordan, 2015).

According to a 2010 United Nations (UN) e-government survey, 'e-government development' has now replaced the term 'e-government readiness'. E-government advancement depicts how far governments have really improved in this field, rather than how prepared or capable they are, which was the way in which e-government readiness or status previously depicted national capacity (Almarabeh & Adwan, 2013). The UN Report (2010) on worldwide e-government development positioned Jordan in 51st place, with a score of 0.5278 out of 1.0000, around the globe, which represented a slight deterioration in its position from the corresponding 2008 survey, where it had been 50th (see Table 1 and Figure 1). In 2012, it dropped a further 47 positions, to 98th place. Essentially, the drop in ranking was due to the slow deployment of e-services to its citizens. The absence of funding had an additional influence on the progress of projects for providing more e-services. However, in 2014, Jordan ranked 79th in the UN report for that year, the country having risen 19 places. This change came as a result of the efforts of the MoICT through the e-government programme such that the number of e-services provided through the e-government portal had been increased. Moreover, the MoICT has been working with essential ministries that represent key sectors, such as education, health, finance, agriculture and public sector development, in order to enhance e-services quality (UN, 2014).

The UN e-government readiness record is made up of three indices (see Figures 2 and 3): an online services element index (OSI); a telecommunications infrastructure index (TII); and a human capital index (HCI). As can be seen in Figure 3, in 2014 Jordan accomplished 0.5197 in the general list for online services, which was higher than the worldwide average (that remained at 0.3919). Basically, this indicator mirrors the level of services given by the Jordanian government through its websites. Similarly, the nation accomplished 0.3104 in the telecommunications infrastructure index, which is just below the world average of 0.3650. This indicator measures the spread of fixed phone lines, personal computers, Web clients, mobile penetration, and fixed broadband. In other words, the telecommunications infrastructure record represents the level to which a nation

is ready for e-transformation. Regarding the third indicator, that of human capital, Jordan has been given a score of 0.7202, above the worldwide average of 0.6566. Human capital reflects the extent to which citizens are able to take part in the networked world, as well as the proficiency rate and enrolment in education.

In 2016, Jordan dropped 12 places in the world ranking for e-services since 2014 and since then has been ranked 91st out of 193 for e-government services, according to the UN's E-Government survey, with an e-government development index (EGDI) of 0.5123 in 2016. This covers the three sub-components: an online services index; a telecommunications infrastructure index; and a human capital index. In the same order, with scores of 0.4565, 0.3458 and 0.7344 (see Figure 4), while the worldwide averages for the sub-components were 0.4623, 0.3711 and 0.6433, respectively. Jordan's ranking for e-participation also dropped, falling to 98th place in the index, from 71st place in 2014 (UN, 2016).

In fact, there has been a delay in launching e-services in recent years. Many governments in the region at the present time talk about smart government (i.e. UAE, Bahrain, Saudi Arabia and Qatar), which is more advanced than just having e-services. Thus, Jordan needs to speed up the process of providing high-quality e-services, which have to be also coupled with enhanced awareness so that citizens and different stakeholders will start using them. To do so, e-government programme officials have to begin to identify the different barriers and factors that influence citizens' trust in e-services, such as regarding information security.

The four phases of e-transformation through an e-government programme (emerging, enhanced, transactional and connected) are progressing through the development of services delivery. The Jordanian government planned to accomplish the transactional stage by the end of the national strategy term in 2016. At present, it is in the late-enhanced stage, given that the government offers several sources of information through the National Government Portal (www.jordan.gov.jo), the National Contact Centre (NCC), the National Mobile Portal and the National SMS Gateway (E-government-Jordan, 2015).

Since 2001, the e-government programme has completed several projects. There are now around 135 e-services available for citizens and organisations on the National

Government Portal. A number of these services also offer online payment through the Jordan Payment Gateway (JoPAY). Numerous other interactional forms of administration and online information are offered on government websites, as detailed in **Annex A**. The National Mobile Gateway and SMS Gateway (94444) promote 40 government e-services that are offered by 101 government agencies. In addition, the National Call Centre (06-5008080) serves citizens and organisations in regard to more than 200 services, as well as handling citizens' complaints about public services. Moreover, a further 77 government organisations have subscribed to the National SMS Gateway push services (MOICT, 2017a).

In mid 2016, the government announced that it would launch 50 new e-services by the end of the year, bringing the total number of e-government services to 150. The new e-services are connected to the Greater Amman Municipality, the Ministry of Interior, the Social Security Corporation, the Ministry of Education and the Civil Status and Passport Department, among other public entities. The MoICT annual report for the year 2017 states that tenders were floated in 2017 to add 287 public departments' services and that work is on-going to automate 75 services. The report noted that 136 services would be automated in 2018, 131 in 2019 and 293 in 2020 (E-government-Jordan, 2017).

Regardless of the advantages and opportunities achieved by e-government, however, the programme still needs to deal with a number of difficulties. The swift maturation of ICT has offered the government different service delivery channels. Since recipients vary in their proficiency, area and the availability of these channels, they require various methods of service procurement. Ultimately, e-services-driven organisations need to change the way all recipients collaborate with the government (Al-Shboul et al., 2014). As public organisations are facing a wide range of information threats, information security is a crucial component in their information systems. Due to increasing reliance on technologies connected over systems and networks, government organisations have to manage effectively information security as one of the most critical success factors for the e-government programme. There needs to be guidelines for effective information security management practices in order to identify the essential steps to obtain the desired results. Moreover, as the number of e-government services introduced to the user increases, a higher level of e-government security will be required.

Table 1: e-Government Development Index and World Ranking for Jordan (based on numerical data from (UN, 2016))

Year	Index	Rank	Change
2003	0.429	63	-
2004	0.4347	68	-5
2005	0.4639	68	0
2008	0.5480	50	+18
2010	0.5278	51	-1
2012	0.4884	98	-47
2014	0.5167	79	+19
2016	0.5123	91	-12

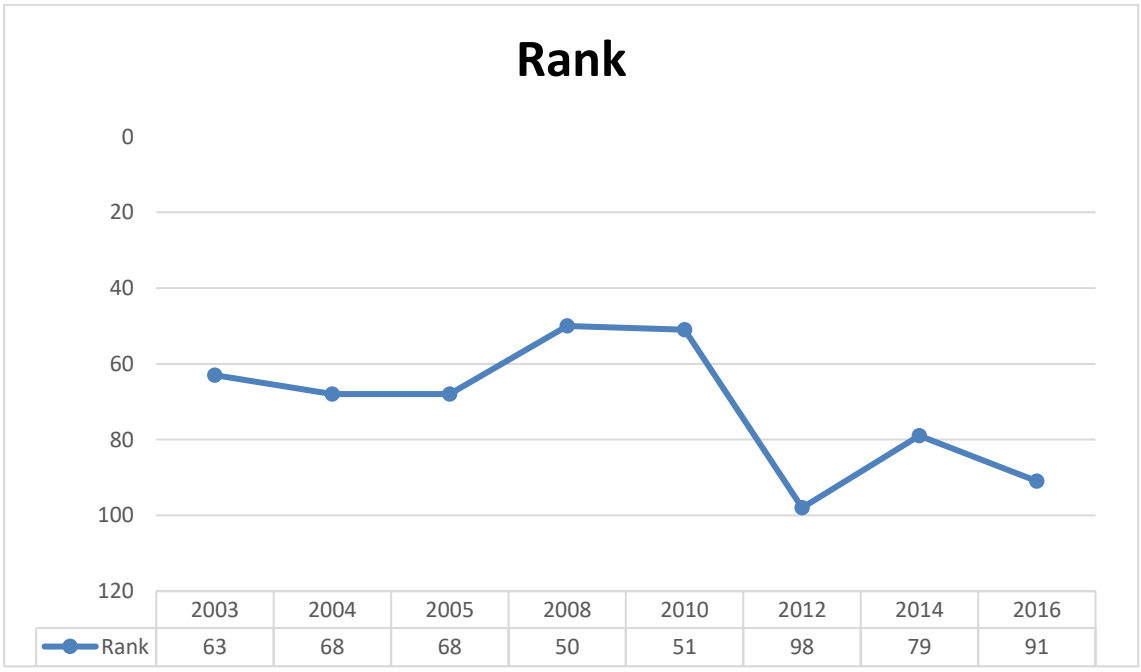
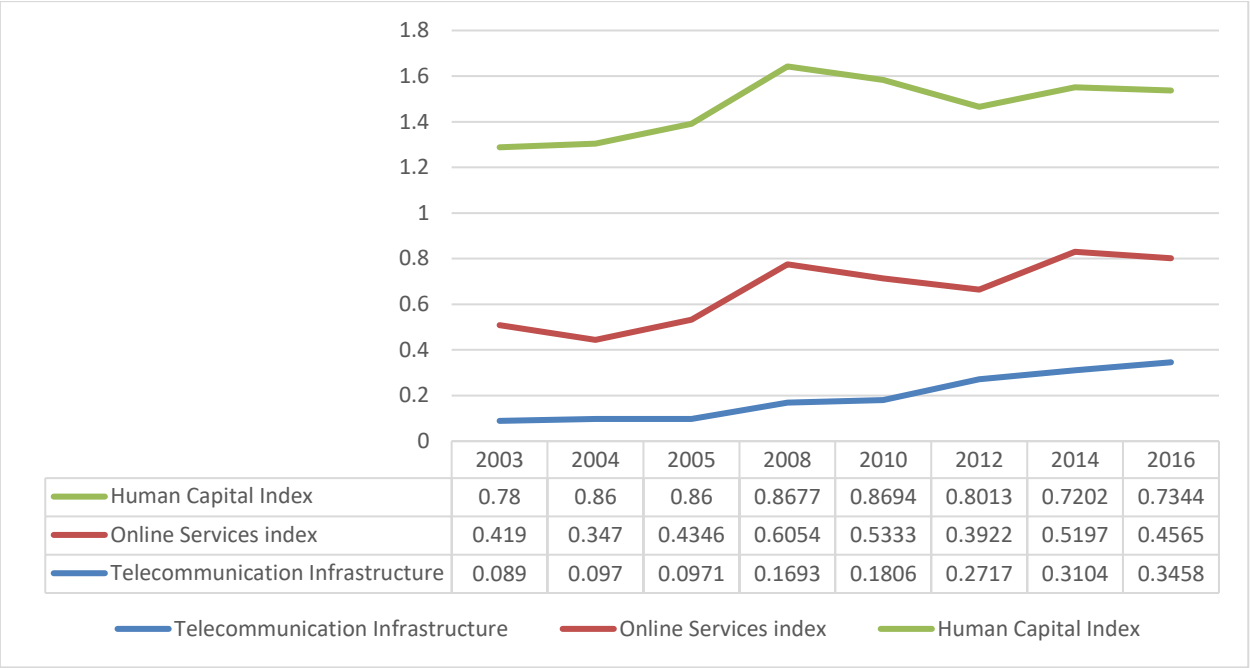


Figure 1: e-Government development world ranking for Jordan (based on numerical data from the (UN, 2016))

* The y-axis has been reversed to indicate that the 120 position is the worst possible outcome for the ranking of the e-government programme (this shows how the e-government ranking of Jordan has deteriorated in the general trend)



	2003	2004	2005	2008	2010	2012	2014	2016
Human Capital Index	0.78	0.86	0.86	0.8677	0.8694	0.8013	0.7202	0.7344
Online Services index	0.419	0.347	0.4346	0.6054	0.5333	0.3922	0.5197	0.4565
Telecommunication Infrastructure	0.089	0.097	0.0971	0.1693	0.1806	0.2717	0.3104	0.3458

Figure 2: Online services, telecommunications infrastructure and human capital indices for Jordan 2003-2016 (based on numerical data from the (UN, 2016))

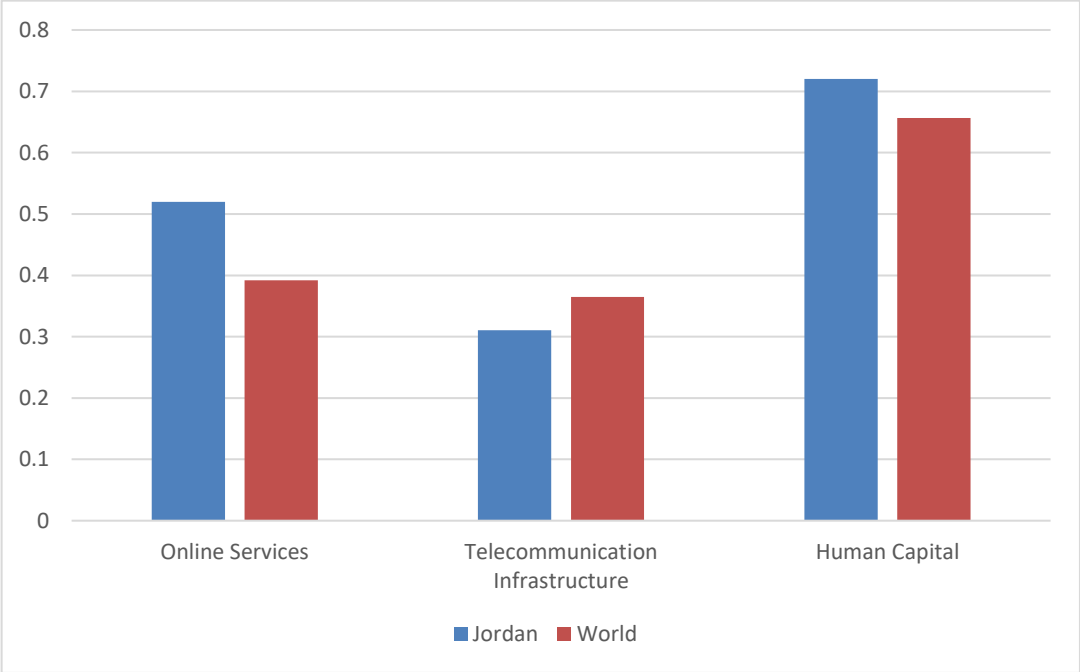


Figure 3: Online services, telecommunications infrastructure and human capital indices for Jordan with global indicators for 2014 (based on numerical data from the (UN, 2014))

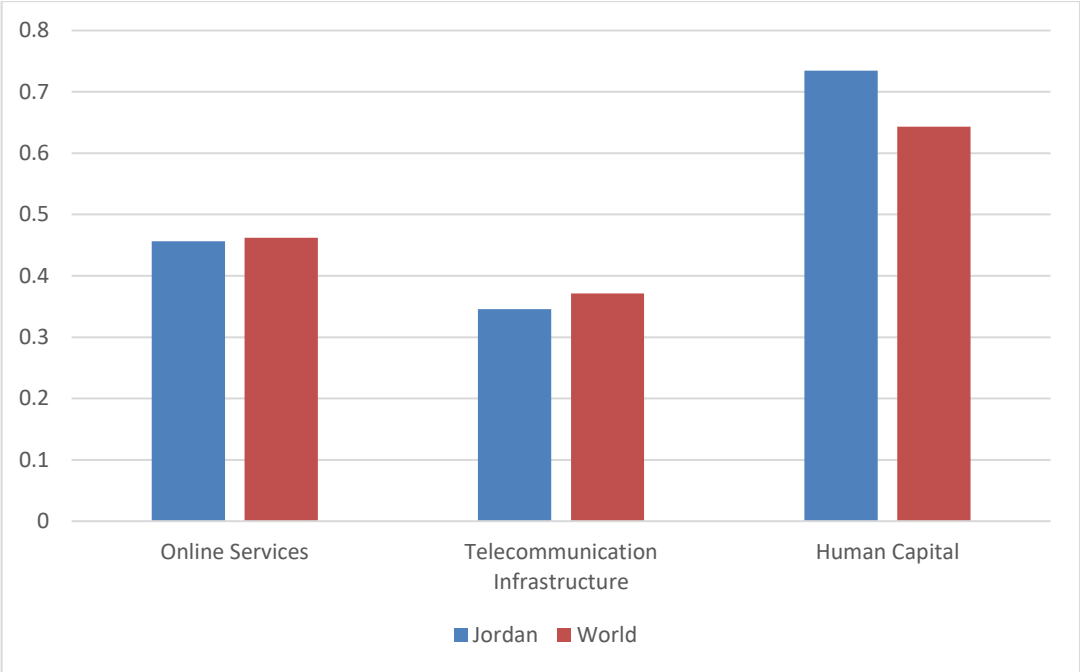
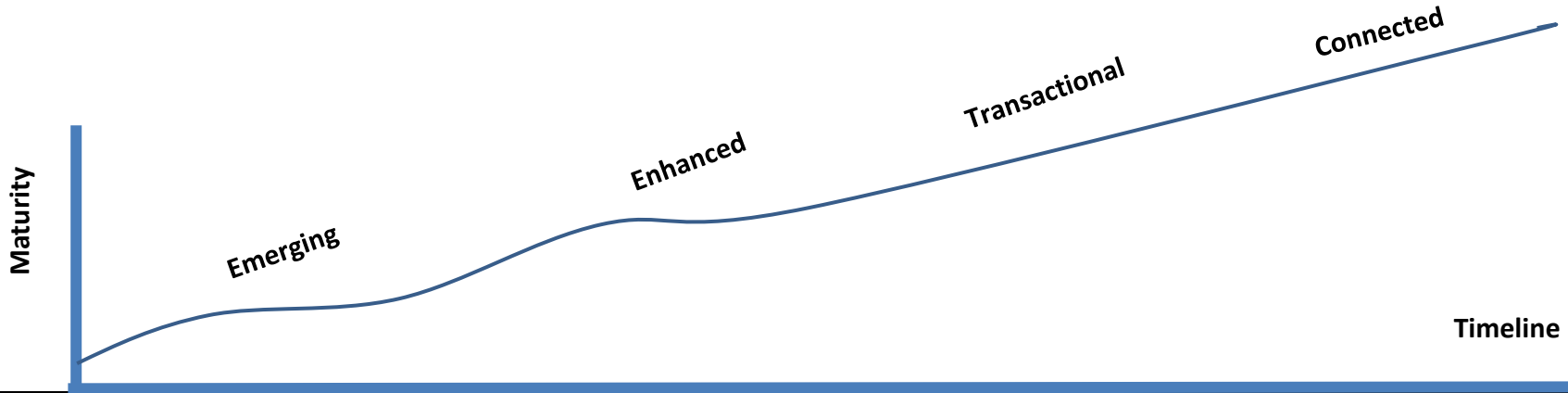


Figure 4: Online services, telecommunications infrastructure and human capital indices for Jordan with global indicators for 2016 (based on numerical data from the (UN, 2016))

Table 2: The main services provided by e-government in Jordan (based on numerical data from (Al-Jaghoub et al., 2010))

e-Government services	**%** of the population that uses this particular e-service
Information for checking traffic tickets	81.3
Information about the weather	51.1
Passport renewal	39.4
ID card renewal	28.4
Driving licence renewal	18.9
Paying bills	17.2
Information about car tax	16.8

Applying for jobs	10.1
Health card renewal	8.1
Paying tax	7.9
Tax refunds	7.3
Income tax settlement	7.1
Tax situation	6.5
Family document renewal	1.6



E-services	2003	2006	2009	2013	2016	2020
G2C & G2B	Online e-services (15)	Online e-services (30) on National Portal Official websites	Online e-services (55) on National Portal Enhanced and new official websites	Online e-services (96) Enhanced and new official websites	Online e-services (100)	
G2G & G2E			GFMIS, HRMIS, IMIS	e-Procurement		
Institutional	Launch of e-government programme initial strategy	National strategy (2006-2009) & roadmap EGSC 70 CIO Units	National strategy (2014-2016), roadmap & additional 37 CIO Units	Activate EGSC CIO Council *MADA* *Daleel* e-Gov award		
Business		Training for over 10,000 government employees	Training for over 3,000 government employees			
Legal			e-Transaction Law amendment draft	e-Participation policy		
Infrastructure	SGN 14 entities	National Portal SMS Gateway	Mobile gateway Payment gateway ESB SGN 73 entities Enhanced Portal	Transactional National Portal PKI Cloud Computing Data Model and Open Data Standards		

G2C = Government-to-customer, G2B = Government-to-business, G2G = Government-to-government, G2E = Government-to-employee, EGSC = e-Government Steering Committee, CIO = Chief Information Officer, ESB = Enterprise Service Bus, *MADA* = An Arabic word for 'extent', GFMIS = Government Financial Management Information Systems, HRMIS = Human Resource Management Information System, IMIS = Institute for the Management of Information Systems, *Daleel* = An Arabic word for 'guide', PKI = Public Key Infrastructure

Figure 5: Timeline for the Jordanian e-government programme (based on numerical data from (MoICT, 2014))

1.2 Research Focus (Information Systems Security and Online Trust)

This section discusses information systems security and online trust as key areas that influence e-government adoption. There are a number of factors affecting the adoption of the e-government programme in Jordan: social, governmental, technological, and organisational. Previous studies have shown that there is a need to focus on citizens' levels of satisfaction and their beliefs in terms of e-government, as well as their readiness to adopt it. This research focuses on information security, both technical and non-technical aspects, and how it improves citizens' online trust in using e-government services (Abu-Shanab, 2014).

To date, there has been no universally accepted definition among scholars of 'trust'. Some authors define trust as "the willingness of a party to be vulnerable to the actions of another party" (Mayer et al., 1995, p.712). Other authors essentially state the same, but use different terms: "willingness to rely on another" and "confident, positive expectations" (Rousseau et al., 1998, p.394). In particular, online trust increases the likelihood of a user being willing to expand the amount of information sharing through systems and to explore new mutually beneficial arrangements (Hart & Saunders, 1997). Moreover, the idea of trust has been clarified in a variety of situations and from different perspectives. As Warkentin et al. (2002, p.159) note, "Trust is a central defining aspect of many economic and social interactions". It is thus defined as a belief that others will act in a certain way, and a number of features should be available to the trustee, such as integrity, ability, and benevolence. *Integrity* means to what degree a trustee is honest and has ethics when transferring information without any changes or attempts at fraud. *Ability* pertains to the capability and power of a trustee to complete a process or a piece of work. *Benevolence* refers to what level a trustee is believed to do what is good and useful for beneficiaries (Mayer et al., 1995).

In the context of e-government, the government is the trustee and the citizens are the trustors. The trust of its citizens is a critical issue for a government. Hence, based on the features mentioned above, a government should adjust its way of performing tasks to align with the beliefs that citizens are anticipated to have. In other words, trust in e-government can be defined as the perception that the government will achieve an e-government programme with a high degree of privacy and security (Benbasat et al., 2010). Accordingly, this study is aimed at identifying how the government deals with personal information and evaluating its security within e-government systems in Jordan.

Extant studies have confirmed that e-government is a new way of enhancing citizens' trust and confidence in government. In practice, however, there are a number of obstacles and factors facing e-government implementation and adoption. Thus, a government needs to handle many issues in order to implement an e-government programme successfully. However, electronic interactions raise issues of security and online trust for citizens and other stakeholders using government e-services. Trust building and assurance is one of the tasks that can be performed through effective human interaction (Grimsley & Meehan, 2007).

In e-government, the relation between citizens and government is like that between a consumer and a provider of e-government services. Usually, citizens need to exchange personal information (for example, credit card details) to complete the required services and thus, the trust of citizens is critical in this kind of transaction (Al-Shboul et al., 2014). Previous studies have highlighted this as one of the main social factors and barriers that influence e-government adoption and development. In many countries, the main concern of citizens is information systems security and privacy within an e-government programme, as they fear that their information could be exploited or misused (Al-Azzam & Abu-Shanab, 2012). In practice, the security of information systems used via an e-government programme can be considered as a part of the general security of the state (i.e. homeland security). There are genuine worries about citizens' rights to privacy within a state's national security concerns. From one viewpoint, there are concerns that the government will be able to know a lot about individuals and could utilise this information improperly. There are also government concerns that free access to information could enable security attacks, causing, for example, the loss or abuse of personal data (Al-Omari, 2006).

In the context of information security, the CIA triad, standing for confidentiality, integrity and availability, is a widely used security model, which has three key principles that have to be guaranteed in any secure system. This model is applicable across all stages of security analysis, from access to users' information or profiles to the security of data across networks. In addition, any weak point or vulnerability in any one of the three principles could cause serious consequences for the security of the whole system (Cherdantseva & Hilton, 2013).

Based on Samonas and Coss (2014), for almost four decades, the terms 'confidentiality', 'integrity' and 'availability' have been widely used in the information security practice and in academic literature after Bell-La Padula and Biba presented their models, which considered

confidentiality and data integrity (Dhillon & Backhouse, 2001). Within the literature on information systems security these three key terms have shaped the theoretical understanding, as well as the practices that developed for addressing information security in organisations. Mostly, these practices focused on technical controls, which have led a number of scholars to stress the need to take different non-technical issues into consideration (Dhillon & Backhouse, 2000; Anderson, 2003; Dhillon & Torkzadeh, 2006; Kolkowska, 2009).

In an effort to address this gap, information security scholars have gradually become more interested in research that considers wider organisational and social aspects of security (Hedström et al., 2010). For instance, a significant number of studies have probed cybersecurity training, awareness, education and culture (Katsikas, 2000; Vroom & Von Solms, 2004). However, the literature is still mainly focused on security policies and standards, as well as on behaviour and compliance issues (D'Arcy & Greene, 2009).

Socio-technical research defends the view that institutions need to operate based on a harmonious structure of technical, formal and informal security components (van Deursen, 2014). As a result, the socio-technical security models are important as they highlight the key role of social and human aspects in information security management. As Harris (2010) notes, social aspects of security have become a basic part of the IS security literature. Backhouse and Dhillon (1996) emphasise that failure to achieve a balance between the three levels causes uncertainty and complexity, also eventually, leading to hazard. This is because of the strong connection and the continuous interactions between the technical, formal and informal levels. In the same research stream on socio-technical security, scholars (Dhillon & Backhouse, 2000; Dhillon & Torkzadeh, 2006) have determined the limited role of technical controls and hence, the critical need to take social and organisational aspects of security into consideration.

High levels of security will probably result in high levels of trust (Hong & Cha, 2013). However, both security and reliability will be weak, if inconsistencies between plans and actions increase, which will result in reduced trust. Accordingly, trust only occurs when a government obtains citizens' willingness to engage owing to their belief in its ability to deliver on its commitments (E-government-Jordan, 2015).

As a global network, the Internet includes commercial, educational, governmental, and other networks (Liu et al., 2007). Hence, a government should utilise its scope applications to deliver

both public services and performance improvement (Shankar et al., 2003). Since 2006, the ICT sector in Jordan has grown rapidly and many investments have been made in recent years. The Jordanian government is, via the MoICT, making great efforts to involve more people in the adoption of services provided by its e-government programme. In general, most Jordanian public sector organisations are connected to it and offer their services through the Internet. However, the use of the Internet for applying for government positions during the job application process is restricted to simple communications, e.g. e-mail. Active e-services in the public sector have not yet reached a level from which the Jordanian government can benefit. Despite the Internet being a source of risk, and real danger in some cases, most Jordanian users believe they are facing a greater loss by not being connected to it than that caused by security issues through their having access (Shaqrah, 2010). Evaluating information security within governmental systems at the public level requires critical analysis, starting with the computing infrastructure in terms of technological vulnerabilities, considering the risks regarding the nature of the organisation's business/tasks, and determining what needs to be protected.

1.3 Research Questions

Given the essential role of information security in the success of e-government programmes, this study aims to answer the following research questions.

1. What is the approach to information systems (IS) security in the Jordanian e-government programme at the technical, formal and informal levels (to be examined based on the TFI security model)?
2. Why is the government of Jordan not attempting to enhance citizens' online trust by communicating (elements of) security countermeasures in their e-government programme (technical/formal/informal)?
3. What are the citizens' perspectives and perceptions about the security of the e-government programme and how does this affect their adoption of e-services (online trust)?

1.4 Research Aims and Objectives

This section introduces the main aims and objectives of the research. For this study the approach to information systems security (ISS) within the e-government programme of Jordan

(Ministry of ICT) is explored. Then, whether citizens trust that programme is examined by probing their perceptions of information security. In order to achieve these aims, the research objectives are: to provide insights regarding the current approach to ISS; determining whether or not there is a link between ISS and online trust and how the latter can be improved; as well as analysing the real situation for the focal field through collecting data from e-government programme leaders and stakeholders.

1.5 Significance of the Study

This section explains the significance of the study. The Internet provides universal access to information, which can lead to both social and economic development at the national and international levels. It is the primary medium through which many governments seek to deliver their services and to make information accessible through their webpages. Hence, the Internet is changing the relationships between government and all other social systems from a traditional face-to-face or paper-based means of communication, to an online interactive form.

The main reasons behind the introduction of e-government programmes by both developed and developing countries can be summarised as follows: a) efficiency in delivering government services (Alomari et al., 2009); b) disseminating information (Shannak, 2013); c) ensuring more citizens participate in making political decisions (Alomari et al., 2012); d) reducing cost (Al-Shboul et al., 2014); e) increasing transparency and accountability (Abu-Shanab, 2012); and f) improving government interactions with people and business (Obeidat & Abu-Shanab, 2010).

Governments, including that of Jordan, need to identify the main factors affecting e-government success in order to specify the strategies required to implement such programmes appropriately. Jordan is one of the countries that have initiated an e-government programme to ensure the efficient delivery of services to the public and to reduce the cost of delivering such services. E-government is not only involved in improving public services, but is also part of creating "a climate in which people will feel civically more engaged" (Gunter, 2006, p.361). In general, public organisations in Jordan are faced with disparate technology platforms that are, in turn, based on different types of data and this condition creates several productivity problems. There is often no common understanding or framework for measuring performance or supporting the technologies in place for effective performance management. Moreover,

some organisations have poor IT and enterprise capabilities. These challenges are intensified, because the Jordanian public service leadership changes at a high rate (often every year) that makes it more difficult to carry out long-term endeavours (Shannak, 2013).

In terms of security, the extent to which information security and privacy need to be ensured has increased. The risks of security attacks must be reduced to a minimum and not exceed the benefits of using the new ICT and online services, if the programme is to be considered as an advancement. Accordingly, information security is an essential responsibility for any e-government programme, which has to address availability, confidentiality, integrity and accountability with regards to citizens' personal information. A high level of security will increase the level of trust and confidence among all stakeholders (whether citizens, businesses or government), being the foundation of a successful e-government programme. In order to apply and select the required and appropriate security measures, the system assets must be identified, as well as analysing the perceived threats and vulnerabilities (Lambrinoudakis et al., 2003). Accordingly, this research involves examining how information security is evaluated and approached within the e-government programme in Jordan. This is undertaken by identifying the components of the extant security threats through application of the technical, formal, informal (TFI) information security model. As mentioned before, this dissertation is not focused on the technical security aspects alone, the non-technical aspects are considered as well. Then, the findings are considered in terms of how they can be addressed so as to enhance citizens' online trust and thus, improve the take up of e-government initiatives.

1.6 Dissertation Structure

This section provides an overview of the contents of each chapter. This document consists of six chapters and is structured as follows:

This initial chapter covers the background to e-government and recent developments in the context in Jordan. It also clarifies the research focus, presents the research questions, as well as the aim, objectives and significance of the study.

Chapter II provides a literature review covering e-government research in the context of information security and then focuses this in the context of Jordan. Moreover, Chapter II describes the link between information security and citizens' online trust, in addition to the way in which this influences e-government adoption and development. The TFI (technical,

formal and informal) model is also reviewed. *Technical* concerns the hardware, software and networks; this level refers to automating parts of systems, such as the computers used in some operations and tasks. *Formal* refers to the policies, processes, procedures and all organisational-level security mechanisms. *Informal* relates to individual-level security mechanisms and includes the role of factors, such as the beliefs and attitudes of employees, culture, values and awareness.

Chapter III explains the research design and methodology. The dissertation follows a case study research design in the interpretivist tradition and uses semi-structured interviews and a complementary survey as data collection methods. The chapter provides an overview of the used methods, data collection and analysis, and how their choice was appropriate, valid and reliable.

Chapter IV illustrates the findings of the interviews and the survey, and reflects upon them in a critical manner.

Chapter V discusses the interviews and survey findings. The first part discusses the outcomes of the qualitative study conducted at MoICT to formalise the research problem, followed by a discussion of the survey conducted to clarify the link between security perceptions and online trust described in the previous chapters. This chapter also proposes a framework for the information security of e-government programmes, based on the TFI security model.

Finally, in Chapter VI, the conclusion and an overview of the research are covered. This chapter also discusses the theoretical and practical contribution to knowledge. The limitations and suggestions for further work are covered.

The next chapter is the literature review on the topics relevant to the research.

2.0 Literature Review

Part A) General Overview

2.1 Information Systems

This section discusses information systems (IS) and the reason for reviewing IS literature is that successful information systems clearly provide a powerful tool for e-government, since any implementation of an e-government programme relies on ICT.

Tapia et al. (2012, p.243) define an IS as "a combination of hardware, software and telecommunications networks that people build and use to create and process useful data to satisfy the demand for information needed by an organisation to achieve its aims". The key issue for any IS is to identify what information is actually required, which depends on who requires it and for what purpose. Hence, the development of any IS necessitates identifying potential users and their needs, as this will determine the content of that information, the form in which it is presented and the time of its presentation. Based on this argument, a successful IS is one that provides the right information at the right time and in the right form to enable users to do their jobs effectively and efficiently; this is at the core of information management.

As Tiwana and Mclean (2003) note, living in a time of great change leads to evolving needs for information, so any system used for delivering information must be flexible and easy to update and amend. This means that the emphasis shifts from supplying relevant information to eliminating that which is irrelevant; it shifts from general-purpose systems to creating information systems that are tailored to the needs of individual users. Managers and other users often do so with the data they produce and manage meeting their organisations' requirements. As a result of developments in computer technology, users can easily select the information they require, when they want it, and in the form most suited to their needs.

Whilst many previous studies have been concerned with IS in business, its importance in the public sector has also been recognised. Wiredu (2012) argues that IT development has led to pressing demands for public organisations to adopt IS innovation. However, as Yildiz (2007) finds, in public organisations this is facing significant challenges regarding IT integration, as demonstrated by the high failure rate of government IT projects around the world. These

challenges have attracted the attention of IS and e-government researchers and Wiredu (2012) emphasises that despite the latter having tried to identify and tackle these challenges, their models are still limited for the following reasons: first, the focus was on the relationship between a public organisation and the public, without paying enough attention to the internal organisational processes. Second, whilst some attention has been paid to the internal organisational processes, perspectives that are too situation-specific have been adopted, which has resulted in micro-level rather than macro-level analysis. Last, the relationship between communities and government is changing and personal technology is aiding the exercise of personal choice and control. The need to structure and organise information via systems to ensure services are available and relevant to the public has never been as important. As Cordella and Iannacci (2010) contend, well-managed information leads to more efficient performance and higher levels of citizen service owing easy access, the ability to obtain relevant information and online self-service.

2.2 e-Government

This section consists of three parts: the first provides several definitions of e-government, whilst the second outlines its benefits and the third contrasts several stage models for e-government, showing the steps of its implementation. Overall, this is intended to provide a comprehensive understanding of the concept of e-government.

2.2.1 e-Government Definitions

The first essential step in assessing an e-government programme is to understand the concept of e-government. The most common definition among researchers is that it is "the use of information technology to support government operations, engage citizens, and provide government services" (Almarabeh & Adwan, 2013, p.88). Thus, e-government not only concerns delivering government services across the Internet, for it, perhaps more importantly, relates to how government manages itself, its processes, rules, regulations and policies in order to provide service delivery and integrate processes internally.

Despite the existence of different definitions of e-government, researchers agree that the concept generally describes the use of ICT by governments to offer citizens and businesses the opportunity to engage with government by using a variety of electronic means (such as the Internet, mobiles, faxes, smart cards and self-service kiosks) (Shannak, 2013). E-government

can also be described as the use of any type of ICT to improve the services and operations provided to different stakeholders, such as citizens, businesses, and other government agencies. Majdalawi et al. (2015) define it as the utilisation of ICT in order to make government institutions and processes IT-based enablers. In a study by Shannak (2013), e-government is described as the implementation of ICT to enhance governmental transactions with all beneficiaries (citizens, businesses and within government). According to Bose (2004, p.2), it is "the application of ICTs to the innovation in, and improvement of government services". Furthermore, the UN characterises e-government as the use of ICT applications by a government to provide citizens with the information and public services they need (UN, 2014).

E-government is considered to be a new and important area of interest in the field of public sector management, which utilises ICT to improve access to government information and service delivery to citizens, businesses and government entities. Similarly, Khasawneh et al. (2011) state that e-government has captured the attention of numerous scholars. In addition, as seen in the previous section, the concept of e-government has different definitions due to the different perspectives of scholars. For instance, Al-Mashari (2007), Schware and Deane (2003) and Sprecher (2000) define it from a techno-centric perspective, as the utilisation of ICT to turn government organisations and processes into IT-based enablers. In contrast, a citizen-centric perspective is presented by Banerjee and Chau (2004) and Burn and Robins (2003), showing the role of e-government as a means of improving engagement with citizens through the latter's ability to access information and e-services. Another definition that combines these two perspectives with a communication aspect is explored by Carter and Belanger (2004), Fang (2002) and Tambouris et al. (2001), who view e-government as the implementation of ICT to enhance the overall interactions of government with all its beneficiaries and stakeholders (those within government, as well as businesses and citizens). Furthermore, in a study by Wimmer (2002), an administrative perspective is adopted by defining e-government as a framework that forms most of the public administration within the information society, while Montagna (2005) underlines the change management perspective, describing it as a striking organisational change. Traunmuller and Lenk (2002) propose a political perspective, in defining e-government as a vision for redesigning public administration.

As a result of the previous range of definitions, e-government can be viewed from multiple perspectives. Indeed, the Centre for Technology in Government (Dawes, 2002) identifies four dimensions regarding the definition: e-services, e-management, e-democracy and e-

commerce. From the above, it becomes clear that, given the variety of definitions proposed for the concept of e-government, there is still no agreement on one inclusive meaning. There are, however, some common dimensions to a number of the abovementioned definitions, despite the differences of emphasis, which will be explored in the following subsections.

2.2.2 Benefits of e-Government

Many scholars have asserted that the Internet offers significant potential and a broad range of possibilities for governments to enhance e-services (Dimitrova & Chen, 2006), to engage with beneficiaries (Dada, 2006), to promote accessibility (Hung et al., 2006), to improve accountability, to increase transparency, effectiveness and efficiency (Heeks & Bailur, 2007), to reduce service costs (Al-Jaghoub et al., 2010), to expand the accuracy and privacy of information (Wimmer & Von Bredow, 2002) as well as gaining the satisfaction and acceptance of government stakeholders (Verdegem & Verleye, 2009). Moreover, Obeidat and Abu-Shanab (2010) and Scholl (2006) argue that e-government helps in transforming business processes, enabling government organisations to reorganise and simplify their services and procedures. Scholl and Barzilai-Nahon (2007) find further benefits of e-government, such as the ability to develop information sharing, increase citizen participation and improve public sector performance. Tapia et al. (2012) contend that e-government is the most effective way of reducing weaknesses in the public sector, such as poor communication between departments, which causes the duplication of effort and inadequate responses. Moon (2002) introduces different benefits of e-government, such as its ability to change ways of working as well as achieving more cost-effective and efficient procurement.

Furthermore, Bertot et al. (2010) point out that e-government benefits can be classified according to the three main interactions that take place between government departments and citizens, government and businesses. For example, Government to Government (G2G) interactions help in improving internal communication between and within government entities, leading to greater flexibility and efficiency, thus increasing transaction speeds and information sharing. Government to Citizens (G2C) interactions enhance citizens' engagement with the government, providing the information and services required to citizens. They can also improve citizens' participation in the formulation of government policies and rules. Regarding Government to Business (G2B) interactions, the benefits include cost reduction, an increase in opportunities to carry out business with the government, and improved procurement and

transaction effectiveness, which leads to a reduction in corruption. In order to capture these potentially wide-ranging benefits, Carter and Bélanger (2005), Reynolds and Regio (2001) and Wimmer and Tambouris (2002) declare that there are three major groups of stakeholders citizens, business and government that need to be considered in order to create a fruitful e-government programme. Each category of stakeholder has certain needs from an e-government programme, as explained in more detail below.

Citizen Perspective

Citizens increasingly require convenient access to public services 24 hours a day, seven days a week, and they want to be able to access these services from anywhere (such as from home, work or anywhere else), without any device limitations on how they do this (e.g. PCs, mobile phones or other wireless devices, Web-enabled TV, etc.). In order to provide citizens with this level of service, governments need to create a one-stop national portal (a single access point). Through this, citizens can express their needs and requirements from government more effectively, because this new form of communication (using ICT) improves their participation and engagement with their government at any time and wherever they are.

Business Perspective

The opportunity for companies to conduct online transactions with government reduces costs, changes the traditional way of doing things and simplifies administrative processes, thereby making businesses more competitive. Rather than completing paper forms in a government office, it is much easier, more convenient and faster to fill in these via the Internet. Moreover, government can create a strong business environment by establishing an appropriate infrastructure to provide services for companies online. Indeed, delivering e-services through an integrated single source creates opportunities for both government and business to cooperate with each other.

Government Perspective

When the government places citizens at the centre of any service development initiative, this enables it to gain public trust and confidence, thereby possibly changing citizens' perceptions of low public service quality. Further, rebuilding a relationship with the public requires the provision of services in a different and novel way, without long waiting times and inconvenient procedures. Customer-centric organisations are able to provide easier public access to services,

increase service levels and reduce wasted employee time. Thus, they achieve greater success both within government and in serving the public.

2.2.3 e-Government Stage Models

Researchers have divided the e-government implementation process into multiple stages in order to facilitate e-government development. That is, e-government is not a one-step process or a single project. It is a major programme that consists of different stages, levels and projects (Layne & Lee, 2001). Most e-government stage models have been proposed by individual researchers, such as Bélanger and Carter (2008); Layne and Lee (2001) and Moon (2002) and a few by institutions, such as the (UN, 2014). Based on organisational, managerial and technical analysis, Layne and Lee (2001) introduced a four-stage model for e-government implementation, as follows:

- Catalogue: providing essential governmental information via websites;
- Transaction: adding some necessary online transactions for citizens to carry out;
- Vertical integration: moving towards e-transformation, which not only involves automating the available processes, but also incorporating government tasks at different levels;
- Horizontal integration: integrating multiple tasks from diverse systems.

On the other hand, Symonds (2000) presents a four-stage model of e-government consisting of one-way communication, two-way communication, exchanges, and portals. Belanger et al. (2006) adopted Symond's four-stage model, but added a fifth stage namely participation, which requires providing specific online features, such as online voting and registration. Another four-stage model, proposed by Gartner, explains e-government development in a correlated environment and has been used by the Gartner group (Baum & Di Maio, 2000), its model stages being: Web presence, interaction, transaction and transformation. In a more elaborate model, Deloitte (2000) proposes that e-government development passes through six essential stages: information publishing, official two-way transactions, multi-purpose portals, portal personalisation, the clustering of common services, and full integration and enterprise transformation. The UN (2014) suggests a five-stage model for e-government development, consisting of emerging presence, enhanced presence, interactive presence, transactional presence, and seamless or fully integrated presence.

It is clear that despite differences in the number of stages in the models reviewed above, the steps present similar ideas. For example, the researchers agree that the first stage in e-government implementation is posting government information on a website, regardless of the different labels given to this stage, such as cataloguing, Web presence, information, information publishing, or emerging presence. The abovementioned scholars also recognise that providing online transactions is an essential stage of e-government progression, even though they use various names to describe it (for example, transaction, official two-way transactions and transactional presence). In addition, integration, vertical integration, horizontal integration, transformation, full integration and enterprise transformation are all terms used by researchers to describe a basic stage of e-government development. At the same time, there are a few differences between the proposed models. For example, the UN (2014) and some scholars, such as Baum and Di Maio (2000) and Moon (2002), refer to a stage regarding stakeholders and government communication (two-way communication, interaction and interactive presence). Other scholars, such as Belanger et al. (2006), add a stage that includes citizens' participation (political participation, e-democracy and participation).

To conclude, there are differences regarding the number of stages of e-government development identified as a result of the different perspectives various scholars have, including organisational, political, cultural and technological approaches. E-government is a wide programme and it is very difficult to implement in one step, since it is aimed at achieving e-transformation in the public sector. For this reason, it is necessary to divide the implementation process into several stages.

2.3 e-Government in the Context of Jordan

This section describes the current situation of the e-government programme in the context of Jordan, where this research is conducted. It also explores the main difficulties and factors facing Jordanian e-government, introducing these through a literature search and data collected from government websites.

A number of studies have been undertaken in different countries in order to study e-government implementation and adoption, for example, Alomari et al. (2009) in Jordan and Carter and Belanger (2004) in USA. Each study was aimed at providing a clear theoretical explanation of the factors examined in its research model and to present the advantages of a successful e-

government programme. A few empirical studies have discussed the factors of e-government adoption in Jordan, such as Abu-Shanab (2012) and Shannak (2013), and some have demonstrated the merits of implementing such a programme (for example, Khasawneh et al. (2011). However, Al-Shboul et al. (2014, p.1112) assert that "these studies are conceptual, descriptive, and exploratory in nature and fail to provide relevant facts regarding the current state of e-government in Jordan". In other words, the number of studies that have discussed the adoption of e-government services in Jordan in depth is limited. However, the government of Jordan has made an initial attempt and defines e-government as "the ability to submit governmental transactions on-line and make payments electronically where they are required" (AbuShanab & Pearson, 2007, p.82). Indeed, Jordan is seeking more efficient, accountable, and transparent e-government, although inadequate human resources training and unqualified staff are a primary obstacle in developing countries, including Jordan (Mohammad et al., 2009).

In the above regard, Abu-Shanab (2014) explores the common obstacles to adopting e-government programmes in developing countries, identifying a lack of both technical support for government websites and knowledge about e-government services. According to Heeks and Bailur (2007), nearly 50 per cent of e-government programmes in developing countries have partially failed (i.e. major aims were not achieved and/or there were disappointing outcomes), 35 per cent have totally failed (the projects were either implemented, but immediately abandoned or not implemented at all) and only 15 per cent were implemented successfully. According to these researchers, the main reason behind e-government programme failure in developing countries is the gap between the design and the reality in terms of technology, information, staff training, management and other resources, such as money and time. On the other hand, recent studies have linked e-government programme success with effective IT infrastructure as well as involving different organisational types and forms of business (Alhyari et al. (2013); Tallon (2007)).

Kor et al. (2008) claim that there are difficulties in implementing an e-government programme successfully in Jordan due to the lack of transparency, accountability, and citizen participation. Moreover, their findings confirm that Jordan still needs more effort regarding ICT utilisation in delivering e-services and information. On a more optimistic note, the study indicates that Jordan has never had a lack of fundamental resources, which suggests that its e-government programme need not necessarily be condemned to failure. Despite resource availability, however, Mohammad et al. (2009) argue that e-government implementation in Jordan suffers

from internal and external barriers. The former include having a clear vision of the e-government programme, which must be translated into actions by good leadership. The latter pertain to the rapid changes in technology, people not having a PC or access to the Internet, and online service users' need for guaranteed privacy and security, so that they can feel assured that the information they provide will not be misused.

A similar range of major factors that affect e-government adoption in Jordan was identified by (Alomari et al., 2009). Their study involved exploring four different social factors: trust in government websites in terms of security and trust in government, accessibility, attitudes and beliefs, and education. Reffat (2003) also refers to the skills required for a successful e-government programme and the difficulties that need to be taken into consideration within e-government programme implementation, such as the law, public policy, e-literacy, infrastructure development, transparency, security and privacy. According to Saleh et al. (2013), Jordan has an official e-government portal, which is an entrance gate to the e-services and information provided by the government to citizens, businesses and government entities. However, since each ministry is responsible for developing and maintaining its own official website to deliver information and services, government websites work separately, with minimum system integration and communication. Moreover, most of the public e-services are still at an early stage and have not yet achieved many of the expected outcomes, due to poor IT literacy among Jordanian citizens, weak legislation and regulations, and a lack of uniform technology platforms among government entities. In addition, Al-Omari (2006) confirms that there are challenges and limitations that prevent e-government progression, such as the low level of Internet penetration, infrastructure constraints, the digital divide (the gap between the groups and regions that have ICT and those that do not or only have limited access), and privacy versus security concerns. Information security and privacy play a key role in e-government success in that they have a direct effect on citizens' trust in e-government systems and improving their intention to use e-services.

In general, Al-Shboul et al. (2014, p.1112) maintain that

> "despite increased research interest on e-government, existing research has not adequately addressed two key issues concerning the implementation and integration of e-government systems: a better understanding of the factors influencing the adoption and acceptance of e-government systems, and a better understanding of the factors that influence the effective usage of these systems."

Researchers in the e-government area have investigated the factors and barriers influencing e-government implementation and adoption (Khasawneh et al. (2011); Shannak (2013)). These can be listed under four basic headings: social factors (trust in government, attitudes and beliefs, education, accessibility and IT literacy); technological factors (computer security, privacy, ICT infrastructure and standards); political factors (legal frameworks, laws and regulations, and financial support); and organisational factors (flexible strategies, plans, management structure and the training of employees).

In fact, many studies focus on exploring implementation barriers/challenges whereas fewer studies discussed the barriers/challenges related to adoption (Rana et al., 2013). Within the group of studies which investigated the challenges and barriers of Jordanian e-government in particular (Elsheikh et al., 2008; Alomari et al., 2009; Abu-Shanab et al., 2010; Al-Shboul et al., 2014; R. Al-Soud et al., 2014), the scholars reviewed the barriers from two different points of view. First, the government organisations as services providers have explored various barriers such as: IT infrastructure; lack of security and privacy; lack of trust; lack of awareness; insufficient skilled human resources; lack of clear strategy; lack of a comprehensive policy; lack of training and knowledge transfer; poor collaboration with private sector; legal and regulatory framework; resistance to change; budgets and operating costs. Elsheikh et al., explored the technological barriers particularly system interoperability and data exchange, developing secured networks based on international standards, developing shared applications, introducing digital signatures and authentication.

Second, the barriers of non-adoption e-government servicers from citizens' perspectives referred to online culture and online trust on e-services. Jordanians prefer face-to-face services for reasons of privacy and security. In addition, inadequate the legislation and regulations governing electronic transactions (Abu-Shanab et al., 2010). Alomari et al. (2009) add more cultural factors like resistance to change and digital divide which means IT infrastructure centric in main cities, ignoring the small or remote areas.

Notably, the overlap between technological, organisational and cultural factors that affect e-government success or adoption. However, the studies placed in Jordan did not investigate the impact of government e-services quality and how secure they are on citizens' satisfaction/ trust and other stakeholders.

Whilst the importance of the studies discussed above is not denied, very few have focused on the citizens themselves and their readiness to use and adopt an e-government system (Abu-Shanab (2014); Al-Azzam and Abu-Shanab (2012); Grimsley and Meehan (2007)). Rather, e-government literature focuses more on issues, such as the stages of e-government and how they evolve with time as well as how they are influenced by the country and society (Almarabeh & Adwan, 2013). In general, studies relating to the e-government programme in Jordan present a disappointing view of project outcomes, whether in terms of cost and time management, economic returns, accessibility of e-services, or partnerships with all stakeholders (Alhyari et al., 2013). However, there is a lack of focus on the citizens' characteristics that play a key role in the adoption of an e-government programme. A few researchers (Abu-Shanab (2012); Naoum and Nadhim (2014)) discuss issues regarding lack of awareness, willingness and ability to access technological resources, but these studies have been more narrative in nature, rather than supported by empirical evidence.

Based on the literature review above, scholars have looked at many factors (social, governmental, technical and organisational), but confirm that information security is the most important one, as this affects citizens' trust and hence, has led to a low level of adoption of e-government services. Yet, despite the clear connection between *information security* and *online trust* for e-government adoption, very few scholars have explored this. Consequently, the aim of the current study is fill this gap in the literature, for this could help provide a better understanding of citizens' satisfaction and the beliefs that influence the adoption of e-government programmes.

2.4 e-Government Security

The importance of information systems in an e-government programme has been discussed above, the concept of e-government has been identified, and e-government in the context of Jordan has been clarified. The factors and barriers influencing e-government implementation and adoption were then addressed. This section concerns information security, which is the focus of this study, as being a critical issue for a successful e-government programme.

2.4.1 Background

As already mentioned, the concept of e-government has captured the attention of many scholars in both developed and developing countries. Such initiatives may be more successful in

developed countries than developing countries, such as Jordan, but most governments are still trying to deliver public services effectively and efficiently to meet stakeholders (government, citizens and business) needs. In general, one of the key challenges to the successful deployment and adoption of e-government services in most countries is information security.

Abu-Shanab and Baker (2011) point out that since using e-services requires exchanging sensitive personal data through the Internet, users will use e-government services only if they feel that they are secure and trust that their personal information is protected. A number of studies have explored different security dimensions within the e-government context, such as *secure communication* with government through a website (Hasan & Abuelrub, 2011), trust in the use of personal information by the government (Colesca, 2009), observance of information privacy (Rotchanakitumnuai, 2008), and data storage in a secure server (Henriksson et al., 2007).

In the United States, the results of a survey conducted with public sector employees, emphasise that making information public about e-government procedures regarding information security would influence citizens' attitudes toward e-government services (Holden & Ha, 2002). Moreover, research conducted in Dubai, shows that e-government users are highly concerned about privacy and security. E-government users are cautious in providing personal or financial information; they expect the government to have set high information security measures to ensure their privacy and protect sensitive data. In addition, the authors concluded that the important factors that influence e-government adoption are: perceived security, privacy and ease of use (Sarabdeen et al., 2014). Actually, the findings of many studies reconfirm that privacy and security assurance will have a positive influence on trust in e-government, such as those of Abu-Shanab (2016), Abu-Shanab and Ghaleb (2012), AbuAli and Almarabeh (2010) and Mofleh and Wanous (2008).

According to Ramtohul and Soyjaudah (2016), processing government transactions and citizens' personal information electronically makes information security a critical part of e-government systems and applications. Information security measures have to involve all aspects such as authentication, authorisation, access control, auditing of electronic transactions and logs. Otherwise, the lack of such measures will threaten confidentiality, integrity and the availability of information, thereby causing e-government programmes to become jeopardised in terms of security.

Several e-government researchers have also discussed barriers and challenges of e-government adoption and implementation (Conklin, 2007; Mofleh & Wanous, 2008; AbuAli et al., 2010; Abu-Shanab, 2016). Recent literature has addressed information security as a common key barrier to adopting e-government services, but the majority of the extant studies do not discuss *security dimensions within e-government systems* and fail to present a comprehensive framework for different security issues (Perez, 2014). Khanyako and Maiga (2013) explain that the major obstacle of e-government adoption in most countries is information security. Their study, conducted in Uganda, confirmed that inadequacy in security culture factors include IS awareness, staff training, amongst others, affect e-government adoption.

The studies show that there is an increasing need for e-government security to protect sensitive information and avoid fraud, such as mail fraud, credit card fraud, online scams, phishing, and identity theft. For example, Kim et al. (2006) assert that it is an essential responsibility of e-government to prevent different security attacks including unauthorised access to personal information or official documents, because information systems are routinely targeted by hackers. In sum, there is a need for incorporating technologies that prevent unauthorised access to online documents.

Lambrinoudakis et al. (2003, p.1873) note that:

> "Such a rapid technological evolution could not be problem free. Concerns regarding the extent to which 'information security' and 'user privacy' can be ensured are raised. However, 'growth' of computerised facilities cannot be considered 'progress' until we are sure that the drawbacks do not outweigh the benefits."

Moreover, Ihmouda et al. (2015) point out that as the number of e-government services increases, a higher level of e-government security is required. Furthermore, legislation, operations, procedures, management/administration, mechanisms, culture and ethics, all play a role in influencing information security effectiveness. A study by Joo and Hovav (2016) provides evidence that organisational and individual factors, like government preventive efforts and security awareness have a significant effect on intentions to use e-government systems. This means that the organisations have to implement preventive efforts through different information security solutions and improve employee awareness to reduce the perceived security threats. As a result, cybersecurity covers technologies, processes and controls which are developed to protect information systems and networks from cyber-attacks.

Effective cybersecurity should minimise the risk of cyber incidents and protects organisations as well as users from the unauthorised access to systems and networks.

Cyber-attacks can cause many problems that that can result in loss of assets, reputation, business, and thus, financial damage, in addition to the costs of recovery. For instance, the UK government's Cybersecurity Breaches Survey 2017 clarified that the average cost of a cybersecurity breach for large organisations is £19,600 and for small ones, it is £1,570 (IT-GOVERNANCE, 2017). In addition, the survey shows that, whilst large organisations are more susceptible to cyber threats, a large number of small and medium size organisations are still not aware that they are vulnerable in one way or another, with 45% of them mistakenly thinking they are not a real target. In fact, all types of organisations are at risk of attack. Each organisation should carry out risk assessment, because the cyber-attacks are mostly automated and usually exploit any existing vulnerabilities in a scattergun manner, rather than targeting specific organisations.

While there are many studies relating to information security for e-government, this section provides some of the findings carried out in the context of developing nations. AlGarni (2015) examined the information security policy of the Saudi e-government programme, focusing on the effectiveness, vulnerabilities and threats to the system. The findings show that the common challenges and barriers facing e-government adoption by stakeholders are coding errors, hacking and denial of service. This is in addition to lack of training for and awareness by employees dealing with e-services, which has led to a low level of trust in the e-government applications. Similarly, in a study conducted regarding the implementation benefits of Nigeria's e-government programme, as well as the risks and obstacles (Ashaye & Irani, 2014), it was that found information security, particularly the threat to citizens' personal data and confidentiality of information, was a barrier to the successful implementation of e-government. Moreover, there were many other barriers, including lack of knowledge, awareness, and weak policy implementation.

In the context of developing countries, a managerial conceptual framework has been proposed in several studies (Alfawaz et al., 2008) for e-government security management. The framework is analysing security infrastructure and managerial issues that affecting e-government programme security level. In other term, many variables influencing the effectiveness of e-government programme security such as security management system,

regulations compliance, policy and more others. The studies, based on a socio-technical approach, proposed an information maturity model for secure e-government services concerning both technical and non-technical aspects.

Tagert (2010) argues that the commonly applied cybersecurity frameworks proposed by the developed nations are not suitable for developing nations due to the differing cultural context, ICT advancement levels, experiences as well as social and economic status. Some of the security challenges facing developing nations suggested by literature are:

- Cybersecurity policy;
- Awareness and training;
- Incident handling and response capabilities;
- Technical and managerial controls to secure information;
- Social and cultural differences and context.

As a result, information systems security is a fundamental part in e-government programmes and must ensure the CIA information security triad (confidentiality, integrity, and availability). In fact, addressing information security can be accomplished by a comprehensive framework identifying security requirements for different systems that affect an e-government programme.

2.4.2 Information Security Requirements for e-Government

The key components of e-government security are based on basic information security standards. In its basis, information security consists of physical security and administrative security (Andress, 2014). Kazemi et al. (2012), (Wang, 2009), and Smith and Jamieson (2005) present a number of key success factors of information security such as: leadership, commitment to funding, organisation culture, technical and procedural aspects. That is, these factors are seen as guiding the effectiveness and efficiency of information security implementation.

Islam et al. (2011) explain through their framework how security legal requirements can be integrated into system design and follow these requirements to be addressed through systems development. The impact of national culture on e-government security effectiveness, particularly in developing countries, is demonstrated in a study by Alfawaz et al. (2008). The scholars also looked at the impact of laws and regulations on security and concluded that many

developing countries need to consider adopting adequate legislation related to information security. They went on to propose a framework for e-government security management. Their study was conducted after Seidenspinner and Theuner (2007) explored different cultural environments and found that users' culture affects their online attitudes. Further, Naik et al. (2014) point out that, nowadays, the users can easily update and access their information any time they want via the Internet. On-demand e-services have become one of the most important defining characteristics of the Internet. However, the main downside is that cybersecurity is required with *each process* within e-government systems. E-government services and processes must be secure and the users have to follow the security policies to accomplish the actions they need safely.

Additionally, e-government systems require the sharing of information between governmental organisations and with citizens and businesses. There are many challenges when integrating information systems, not least, legal and ethical issues. Hence, any government that takes cyber security seriously is required to adopt a comprehensive security framework that takes into account systems integration.

As discussed in the previous subsections, most research on information security has focused on the technical level. But as many scholars point out it is not only about technical issues. For instance, Setiadi et al. (2013) propose a balanced e-government security framework that involves both technical and managerial aspects for an e-government programme. Similarly, Naik et al. (2014) call for a comprehensive security framework that involves all aspects of e-government security (people, processes, and technology). Many studies have also contended that the importance of non-technical aspects is the same as technical aspects in relation to security management (Wimmer & Von Bredow, 2002; Dhillon & Torkzadeh, 2006; Siponen & Oinas-Kukkonen, 2007; Wangwe et al., 2012).

Conklin and White (2006) explored cyber security practices in several fields and observed some common results, such as poor awareness and a lack of understanding of cyber security issues. White (2010) asserts that e-government has significant weaknesses under abnormal circumstances (like when they face - or are exposed to - security attacks). In this regard, Wimmer and von Bredow (2001) explain that handling the security of e-government programmes in a comprehensive way is a big challenge. Several scholars have proposed general models that address distinct issues of integrated systems on different basic levels. The

Business Media Framework of Schmid (1999) and the Information Architecture of Mok (1996) provide comprehensive models to analyse where security needs to be investigated in a four-layer structure, as follows:

1. **Strategic level**

At this level, plans and administrative processes should be addressed according to the main purpose of the organisation. Developing e-government systems requires setting an overall security strategy that clarifies which security decisions should be made at the operational level (such as user authentication and identification). Moreover, a general security architecture has to be determined to outline the security management approach.

2. **Process level**

Security models have to be developed for different processes, such as administrative and/or governance ones. The general security strategies from the upper layer have to define the security concepts for different processes and transactions.

3. **Interaction level**

At this level, it is necessary to determine different system resources and train people regarding every single process. This task is important in order to handle communication and data flow during process execution.

4. **Data and information level**

This level deals with data and information access. Security mechanisms need to be addressed through systems applications to ensure user authentication and authorisation. As data access control is a core part of information security, this involves investigating and implementing security issues of data access and data protection as well.

According to Abbasovich and Fikratovich (2015), e-government systems need to take several steps in order to address information security. First, they ought to ensure the confidentiality of information and information resources. This can be enhanced through employee training and awareness to minimise the human factor in information security at the government level. Second, the control of all actions and events by the security system need to be centralised so as to have control over all the actions and events. Third, the security policy and architecture should be established to a single standard, which will address information confidentiality.

With governmental reliance on ICTs increasing, information security management has become one of the most critical success factors for public organisations and private organisations alike.

Thus, it is important to strengthen security awareness and define strong security measures in both technical and non-technical levels. Previous studies, such as those of Siponen and Oinas-Kukkonen (2007), and Dhillon and Torkzadeh (2006), have shown that security issues and e-government management are connected. These scholars have focused on the role of nontechnical issues in safeguarding personal information and security management. They concluded that, in developing countries in particular, there is a lack of organisational culture and level of awareness as to how such factors could influence attitudes towards information security and its management. Indeed, few studies in the literature have explored the social acceptance of security technologies, termed organisational security culture (May & Lane, 2006; Siponen & Oinas-Kukkonen, 2007).

Another important study (for the context of this dissertation) has been conducted by Alharbi et al. (2014), which was focused specifically on the security challenges of e-government from an end users' perspective. A survey was distributed via the Internet hosted at Plymouth University. The participants were from Saudi Arabia (73.1%), UK (11.2%) and the rest (15.7%) were from other countries. The survey involved seven statements relating to security challenges, which were ranked based on the percentage allocation of the participants. According to the findings, 85.5% of the participants agreed that there is a lack of user awareness. In addition to that, 62.4% of the participants believed that users' culture plays a key role in e-government security, and 50% of the end users were concerned about privacy when using e-government services. The authors confirmed that security plays an essential part in the adoption of e-government, and this needs to be taken into consideration within an e-government adoption model. They also revealed the importance of non-technical aspects amongst security issues. In fact, the findings show that many security challenges influence e-government adoption are related to non-technical aspects, for example, lack of user awareness and lack of trust. Hence, more focus should be given to these areas.

Creating a solid cybersecurity foundation

The most effective way to minimise and mitigate the risk of cyber-attacks is to build a solid foundation through a regular security audit, carrying out sufficient risk assessment, drawing up an incidents response plan, in addition to developing strategy and policy upon which enhance the security technology pile.

The difference between compatibility and interoperability is known as the technology gap, with attacks usually occurring owing to this gap. A solid cybersecurity foundation has to identify this gap and adopt the appropriate action to take to mitigate the risk of cyber-attacks. The problem with most of the current corporate environment regarding the security aspects is that organisations tend to focus on technology, but this alone will not protect the critical assets of an organisation. For example, in 2016, The Cybersecurity Intelligence Index, IBM showed that 60% of cyber-attacks were instigated by insiders. Greater efforts must be placed on user awareness, education and training (IT-GOVERNANCE, 2017).

Howarth (2014, p.1) states that *"Technology provides automated safeguards and processes to determine the series of actions to be taken to achieve a particular end. But even organizations with strong security practices are still vulnerable to human error. To stem errors made through social engineering, and to raise awareness of the potential caused by carelessness, technology and processes must be combined with employee education."*

Cybersecurity experts need to examine how people and technology interact to identify possible threats. Breaking down this process into steps can help fill the gap between people and technology, as well as determine vulnerabilities.

Cybersecurity Audit

The cybersecurity audit is a regular process and consultancy service aimed at offering a high-level cyber review of an organisation and its IT assets. This process identifies the vulnerabilities, threats and risks the organisation faces or may face, and more importantly, the impact and possibility of such risks across major security areas: technical, formal and informal (IT-GOVERNANCE, 2017). In fact, a cybersecurity audit is essential for all types of organisations in order to document their risks, vulnerabilities and threats and more useful for organisations that have a high volume of communications, which make them feel overwhelmed by the threats they face.

In terms of government institutions, the best way to mitigate the consequences of security breaches is an emphasis that organisations have followed government regulations, rules, initiatives and taken the necessary steps to protect citizens' personal data to the extent possible. A cybersecurity audit is a basic step to building a solid cybersecurity base for every

organisation. Furthermore, the cybersecurity audit process is a valuable precursor to compliance with the international security standards, such as ISO 27001. This can form part of organisations best practice policy of providing a regular security review report.

Cyber incident response and handling

The quicker a security breach is detected, then the faster action can be taken to reduce the spread of the attack, prevent unauthorised access and to surround or correct the threat, which will make a significant difference to the potential asset loss. Moreover, a practical incident response/ handling plan can reduce the risk of future incidents occurring, where threats can be identified at an early stage and dealt with (CISCO, 2017). Thus, organisations have to implement such a plan to defend against all types of attacks, whereas attackers try to find at least one fault to exploit the vulnerability and penetrate their networks. It is a legal requirement and part of security policy terms. According to the international information security standard ISO 27002, organisations are mandated to develop a cyber incident response plan, which should be tested at least annually (ISO, 2005). Organisations can face many challenges in responding to cybersecurity incidents, particularly advanced cyber-attacks. The top difficulties that organisations can have in handling cybersecurity incidents are:

1. Identifying a suspected cybersecurity attack;
2. Conducting a sufficient investigation and a recovery operation;
3. Collecting all available information related to the attack and analysing it;
4. Determining the actual purpose of the attack and who was responsible;
5. Identifying the compromised systems, networks and information (assets) and the information has been lead to unauthorised parties, stolen, deleted or corrupted;
6. Determining the potential impact of the cybersecurity incident.

CISCO (2017) annual cybersecurity report indicates that absence of adequate cyber-readiness and appropriate skills can significantly increase the consequences and the risk of a cyber-attack. Actually, few organisations understand their real level of readiness to respond to a cybersecurity incident, particularly serious ones and most are not well prepared in terms of people, processes and technology. Various types of organisations, particularly governmental ones, are struggling with handling cybersecurity incidents effectively and thus, these are taking place on a regular basis, thereby having a significant impact on their work (IT-GOVERNANCE, 2017).

Cybersecurity Risk Assessment

Each organisation should conduct cybersecurity risk assessment and have a qualified team in order to achieve this. The main responsibilities of this team are:

- Identifying the assets that require protection;
- Identifying relevant threats and weaknesses as well as exploitable vulnerabilities;
- Assessing the level of threat and determining the impacts of risks if attacks occur;
- Advising on a risk acceptance level and suitable control implementation.

Government organisations need to receive support, advice, and guidance developing an information security risk management strategy, thus enabling them to implement a systematic approach to risk assessment. This approach will reduce the potential risks to information assets and protect systems and networks from cyber threats (Imamverdiyev, 2013).

To summarise, future studies would need to consider these challenges and combine them within an e-government adoption model. E-government security systems have to be able to meet different requirements, such as providing multiple authentication methods, confidentiality, availability, accountability, information integrity, credential issuance and revocation, conflict resolution, platform independence, and so on.

2.4.3 Information Security Framework for e-Government

Frequent security incidences in many countries have weakened governmental abilities to control information systems. In particular, developing countries that are trying to establish successful e-government programmes have to deal with security measures very carefully. Moreover, these countries have limited ICT resources, such as infrastructure and knowledgeable and skilled IT staff. Upadhyaya et al. (2012, p.1) explain that: “Insufficient information systems security can negatively affect the public trust in organisations and willingness to use the public services, which affects the national development initiatives adversely.”

Pereira and Santos (2010) suggest conducting regular audits in order to detect and resolve any problems with existing e-government systems security. This means that government organisations need periodical evaluations to assess the effectiveness of the implemented

security controls, assess different information security systems and ensure that the security policy is properly implemented. Indeed, information system security auditing has been further supported by a number of studies, such as those of Hayes (2010), Xiang (2010), Onwubiko (2009), and Popa and Doinea (2007). These authors clarify that auditing involves a systematic and measurable assessment of an organisation's policies, procedures, standards, measures and practices for safeguarding electronic information from loss, damage, unauthorised access, and/or denial of service. Regular audit of the security function will help in identifying whether the determined security functions are working as required, which will reduce security incidents within the organisation systems (Kidd & Hiltbrand, 2007).

According to (Popa & Doinea, 2007), security auditing process involves a number of steps including: vulnerability scanning, report audit, security architecture audit, baseline auditing, internal control and workflow audit, policy audit, threat and risk assessment. A vulnerability report, threat and risk assessment report, and audit report will show the security holes by addressing the weakness points in different aspects of systems, which could be technical (HW or SW), formal (policy cases), or informal (human resources issue). A range of assessment methods for e-government security have been developed for different purposes (Al-Osaimi et al., 2008; Bakry & Muhaya, 2011; Hadi & Muhaya, 2011). Security controls based upon the most widely adopted security standards have been developed by the International Standardisation Organisation (ISO), known as ISO 27001 and ISO 27002 (Normalización, 2005). The ISO demands that legal and regulatory aspects should be taken into account when incorporating security requirements into design of systems (ISO, 2005). Luo (2010) has listed the key aspects of e-government system security evaluation, relying on a technical evaluation, as shown in Figure (6). However, conducting a technical evaluation only is not enough to analyse the security situation in a comprehensive way.

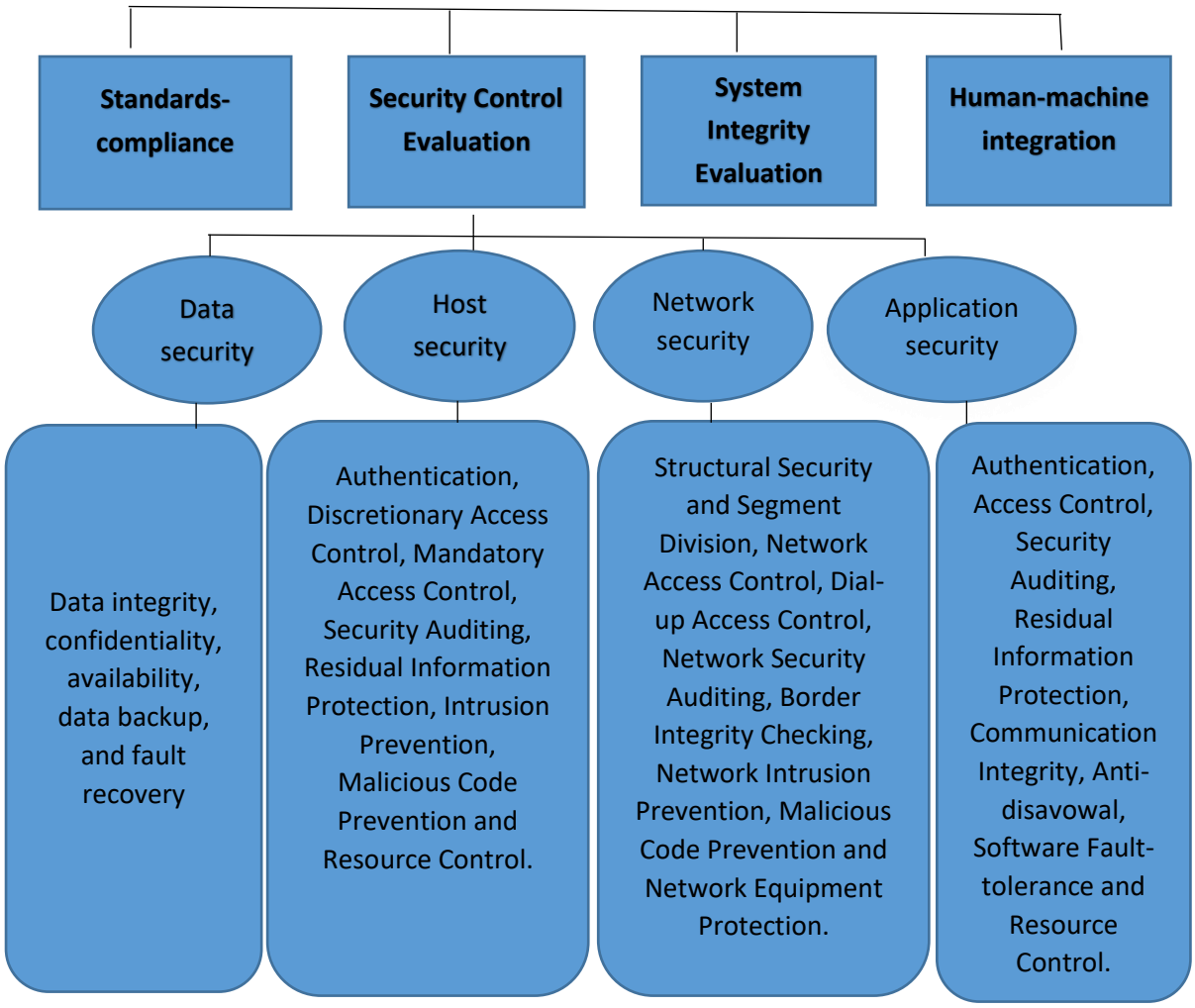


Figure 6: Information Security Evaluation of e-Government Systems (Based on (Luo, 2010))

In another important study by Naik et al. (2014), the proposed layered framework for e-government security combines security management, policies, requirements and components of e-government systems (people, processes, and technology), as shown in Figure 7. In fact, the appropriate illustration and management of security requirements and components are essential for developing secure e-government systems. Another information security framework has been presented by Wangwe et al. (2012) , called TOG (technical, operational, governance). The technical level involves hardware, software, computer applications and technology mechanisms that address the security requirements, whilst the operational level pertains to operational procedures and risk assessment. The last level, which is governance, includes laws, regulations, national and international standards. Each level has specific components that are drawn from the literature on e-government security and cover the security

requirements of e-government systems. However, the scholars of this study did not take into account a number of informal aspects, such as culture, attitudes, and the values of employees.

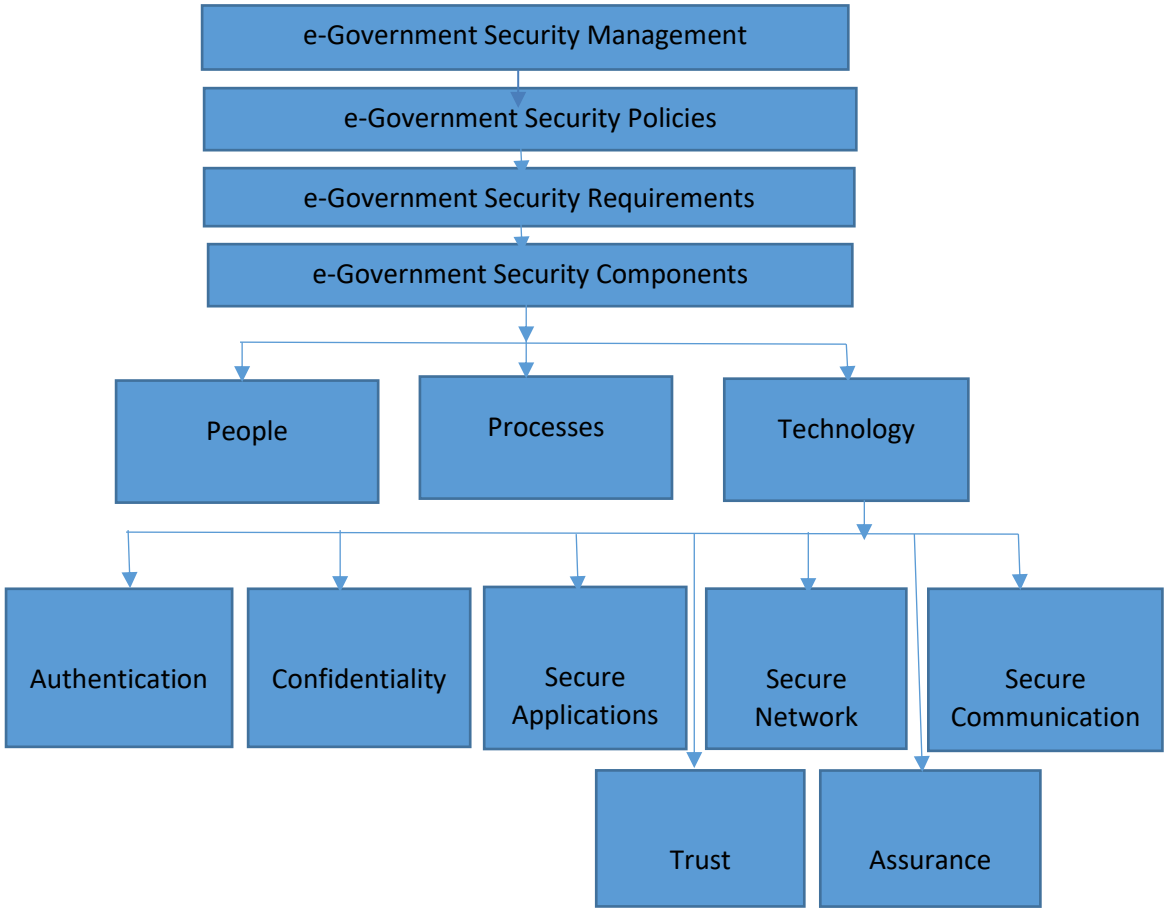


Figure 7: A Comprehensive Security Framework of e-Government Systems (Based on (Naik et al., 2014))

2.5 Trust

The topic of trust is bringing increased interest in many social and organisational studies. Its importance has been stressed in several fields, such as communication, management, e-commerce, among others. In this section, the definition of trust from different studies is presented. Next, the characteristics of both the trustor and the trustee, which affect the level of trust between them, are considered. Following that, the effects of online trust on e-government adoption are considered. Finally, the relationship of online trust and information security is clarified.

2.5.1 Definition of Trust

Previously, researchers have put forward definitions of trust, the relationship between trust and risk as well as those of trust antecedents and outcomes. Studies on trust have also explored the role of both the trustor and trustee and their characteristics (Mayer et al., 1995). However, recent research on trust has a number of definitions that reflects all these aspects mentioned above related to trust with an emphasis on vulnerability. One such definition, proposed by Mayer, Davis and Schoorman (1995) is "the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party". This definition clearly emphasises the vulnerability, which means the willingness to take a risk. Moreover, the above definition of trust can be effectively applied when using the Internet. This facet of e-services and e-commerce relies on a non-face to face interaction between the stakeholders and the service provider, which increases the user's vulnerability. Being vulnerable implies that there is something of importance that could be lost or misused, and the user is taking a risk. A number of trust definitions are listed in the table below.

Table 3: Customer Trust Definitions

Author(s)	Definitions
Moorman et al. (1993, p.82)	A willingness to rely on an exchange partner one has confidence in
Morgan and Hunt (1994, p.23)	When one party has confidence in an exchange partner's reliability and integrity
Mayer et al. (1995, p.712)	The willingness of a party to be vulnerable to the actions of another party, based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party
Rousseau et al. (1998, p.395)	A psychological state comprising the intention to accept vulnerability, based upon positive expectations of the intentions or behaviour of another
Jap et al. (1999, p.305)	The belief that the seller is motivated to act in the buyer's interests and would not act opportunistically, if given the chance to do so
Chaudhuri and Holbrook (2001, p.82)	The willingness of the average consumer to rely on the ability of the brand to perform its stated function
Dirks and Ferrin (2001, p.451)	An expectation or belief that one can rely on another person's actions and words, and/or that the person has good intentions toward oneself

Miyamoto and Rexha (2004, p.314)	One's confidence in another that the other behaves or responds in a predictable and mutually acceptable manner
Kim et al. (2009, p.40)	The belief that the promise of the other party can be relied upon and that, in unpredictable circumstances, the other will act with goodwill and benignly toward the trustor
Lee and Back (2009, p.32)	A generalised expectancy of how an exchange partner will perform in the future
Gregoire et al. (2009, p.20)	Confidence that a firm is dependable and can be relied on
Lacey and Morgan (2009, p.4)	A customer's belief that a firm is reliable, stands by its word, fulfils its promised obligations and is sincere
Chang and Wong (2010, p.263)	A belief that a firm makes an effort to fulfil commitments, is honest and does not seek to take unfair advantage of opportunities
Nguyen et al. (2013, p.99)	The level of reliability ensured by one party to another within a given exchange relationship
Sloan and Oliver (2013, p.1836)	The willingness to rely on another's actions in a situation involving the risk of opportunism

As discussed above, citizens' trust in government is developed based on expectations that are driven by some type of social context or interaction. Thomas (1998) presents three major conceptions of trust, which are: fiduciary trust, mutual trust, and social trust. Fiduciary trust relates to the relationship between citizen and the government, which is an asymmetric one. The citizens' knowledge about what the government is doing is limited and they do not know any of the details about many of the processes. This raises a communication issue between the two. The citizens trust that the government will work in their best interests by achieving the work effectively and considering ethical issues. Distributing information that increases citizens' ability to observe and understand government operations, such as details of processes, laws, regulations, and administrative policies, could enhance this type of trust. Regarding mutual trust, it is a shared respect and confidence between two parties or more, which develops after a repeated interaction between them (e.g. between an organisation and its customers). The last type, social trust, is created and shaped through many different interactions taking place in society. It is a belief that others will not, at worst, harm you, and will, at best, act in your interests. Social trust amongst citizens is essential, because it contributes to economic growth, social integration, co-operation and harmony (Cook, 2001).

Contrariwise to Thomas (1998), who categorises trust based on major conceptions, Welch et al. (2005) take a different approach and assert that there are three types of trust. They differentiate these based on reality or a practical view: characteristic-based trust, which is produced through expectations associated with personal characteristics, such as gender, age, and race; institution-based trust; and process-based trust.

Tolbert and Mossberger (2006) contend that process-based trust is driven by repeated interactions between citizens and the government through the available online resources or applications, which could lead to the former perceiving the latter as being responsive and accessible. On the other hand, institutional-based trust is established when citizens expect that their government and public sector institutions will do what is right and when institutional actions confirm transparency and responsibility. Government agencies should adopt a trust building mechanism, such as posting information on policies, laws, information security procedures and rules, which will encourage the adoption of e-services. In the same context, Bélanger and Carter (2008) confirm that institution-based trust, such as trust in the Internet, is an essential element of e-government adoption. Citizens must believe that mechanisms are in place to ensure secure and private data transmission over such an impersonal medium.

2.5.2 Online Trust

This subsection provides a review of previous studies on online trust as one of the major social factors that affect the success of an e-government programme. Online trust is also the focus of this research, so it is necessary to clarify this term and explore it in detail. Studies in the area of e-government have reported several social factors that remain important and they have also highlighted the salience of behavioural attitudes towards adopting e-government services (Mofleh & Wanous, 2008; Alomari et al., 2009). Moreover, the adoption process is described as the end phase, which is the use of technology or the intention to use (ITU) it. E-government provides e-services that touch citizens' lives and have an impact on their interaction with the government. As will be shown later, studies have, therefore, tried to identify constructs that may affect the decision to adopt this technology. Technology acceptance or adoption theories have been used to explore this issue, with a number of constructs that have a clear effect on the ITU technology being proposed. Indeed, trust is one of the constructs that significantly influence ITU e-government services. Many scholars describe it as the gateway to e-government adoption. For citizens and businesses will not use e-government services unless

they trust them (Al-Azzam & Abu-Shanab, 2012). Hence, trust is an important factor affecting the success of e-government programmes and governments need to build trust relationships with citizens before starting to interact electronically with them (Zeleti & Mustonen-Ollila, 2011). Governments should also build trust within agencies, between agencies and with businesses (AbuAli & Almarabeh, 2010).

In the e-government literature, trust is discussed as an antecedent of ITU (Obeidat & Abu-Shanab, 2010), an antecedent of perceived risk (Yaghoubi et al., 2010) and as an antecedent of the Technology Acceptance Model (TAM) (Khayun et al., 2012). As abovementioned, governments have to establish trustworthy relationships with citizens and all stakeholders before launching such electronic channels with them. Moreover, trust in e-services can be described as a process with distinct steps: first, citizens need to trust the government itself and governmental transactions generally; second, they need to trust the online step of disclosing information over e-government websites. Finally, citizens must have the ITU the services provided online. The same process of trust (in the distinct steps discussed above) can come about in the case where new technologies being adopted or implemented which influence the attitude towards e-government projects and lead to the ITU e-services.

A study by Morgeson et al. (2010) describes the relationship between trust in government and the process of e-government adoption, but fails to provide evidence to support the existence of such a relationship. According to Beldad et al. (2012), Carter and Campbell (2011), and Ozkan and Kanat (2011), trust in e-government services is a process in which citizens build their trust in governments and their transactions, only then accessing information through an e-government website and, finally, have the ITU the services provided.

Al-Azzam and Abu-Shanab (2012) propose a model with *perceived risk* in order to explain Jordanians' ITU e-government services, but fail to support this new construct. The authors suggest three constructs that influence trust in e-government (TEG) and the ITU the system: trust in government, trust in the Internet, and perceived risk. The perceived risk construct was tested against both direct variables, namely TEG and ITU, and came out with insignificant results. On the other hand, trust in government and trust in Internet essentially established TEG. In addition, TEG significantly mediated the relationship between trust in government/trust in Internet and ITU. Through path analysis, the findings support the idea that trust in government and the Internet are direct variables that influence TEG, but do not support the idea that

perceived risk has a significant direct impact on it. This is because a higher level of trust in the government reduces the perceived risk of using an e-government service. The empirical study was conducted using a questionnaire that included 17 Likert scale questions, through steps where the direct and indirect impacts of the variables were estimated. The sample was chosen randomly within Yarmouk University, and on a voluntary basis, from Jordanian citizens with regular access to the Internet (120 respondents, masters students and employees). Yaghoubi et al. (2011) identify and integrate five major antecedents of trust in e-government: perception of authentication, perception of confidentiality, perception of privacy protection, perception of non-repudiation, and perception of data integrity.

It can be seen from the above that in previous studies, the trust issue has been considered from two angles: the factors influencing trust in e-government and how it affects e-government adoption (Al-Azzam and Abu-Shanab (2012); Jiang et al. (2008); Peppa et al. (2012); Shajari and Ismail (2012)). These suggest that for Jordanian citizens' trust is highly important in succeeding e-government programme and in the context of this research it will be a focus area from an information security perspective.

As stated earlier, some studies have described trust as the gateway to technology adoption, and factors used in known models of technology acceptance, such as TAM, were considered as antecedents to trust. In this regard, Odat and Khazaaleh (2012) add that lack of security, concern about e-payments and the lack of confidentiality are all basic determinants of trust in Jordanian e-government services. Furthermore, self-efficacy and the quality of the e-government experience were proposed as predictors of trust by Horsburgh et al. (2011), while transparency and governments dealing sensitively with personal information would improve the levels of trust, according to Zaimes et al. (2012). To conclude, there are several basic factors reported in the literature that play a key role in building citizens' trust in e-government. These include citizens' trust in their government, their trust in technology and the Internet, privacy and security issues, website quality, previous experience with e-government, information system quality, familiarity with technology, and demographic factors. Based on the literature review so far, it would appear that not enough work has been undertaken on the communication of security issues and their direct impact on citizens' trust in e-government systems. A clarification of the link between online trust and information security is provided in the next subsection.

2.5.3 Linking Online Trust and Information Security

As mentioned before, the literature review on e-government presents the criteria for e-government adoption from a citizen and government views, and highlights citizens trust and information security as key factors. According to West (2004), the citizens' concern is usage, security, and trust, with the lattermost being driven by the confidentiality and privacy of information and faith in e-government services. For a government, the concern is systems management, which involves resources security management, such as IT infrastructure. An additional concern for them remains the improvement of services and information sharing among different departments and organisations.

Transparency is needed in the e-government process so that it brings trust and confidence in the available services, as well as assurances of the citizen's privacy (Marchionini et al., 2003; Lauer, 2004; Vriens & Achterbergh, 2004). However, one of the most critical points is that most of the actual security infrastructure is not being communicated or disseminated to citizens in a way that makes them informed and confident about taking the decision to use e-services. Hence, there is a considerable gap between citizens' perception of e-government security and the actual security implemented within an e-government programme. To understand the reasons for this gap it is necessary to consider the problem domain in more detail. On the internal organisational government side, actual security measures are implemented. This involves technical measures (software and hardware) and non-technical ones combining organisational regulations, rules, policies, procedures, etc. The fact that there are several government-based e-services that are not coordinated, having different procedures and operational practices, makes this more complex. Thus, consistency is needed in terms of management, more specifically, information security management. The reality that the government is not disseminating much of information about the used security approach to citizens is causing this gap. On the external and public side, the government needs to clarify the level of the security implemented within e-government systems to citizens and different stakeholders. This will ensure transparency in the e-government process, which will, in turn, brings trust and confidence in the available services. In previous studies, a link has been made between citizen trust and their perception of security, instead of their evaluation of the actual security implemented (Riedl, 2004; Akhter et al., 2005; Akhter et al., 2008). As a result, it is imperative for e-government to get its information security measures right, at the technical and

non-technical levels, and communicates those that can be made public to support the perception of citizens' of e-government security and their online trust.

In their study, Cremonini and Valeri (2003) found that citizens' concerns about security and confidence in e-services, led to a lack of trust, which was identified as a significant barrier to the adoption of e-government. Their survey findings show that 74% of EU citizens consider the awareness of security features of websites as a key factor in deciding to use e-services, such as encryption. In addition, in a comparison between U.S. and EU citizens' (Internet users), lower than 20% of EU citizens were aware of the security features of websites, such as deployment of antivirus protection, while in the US, this figure was more than 40%. The survey also revealed that the impact of this lack of awareness is even more serious, as more than 60% of citizens (respondents) had security fears, which made them unlikely to interact with e-government services, as well as there being a lack of reliable information about the security of their transactions. Regarding which, Tung and Rieck (2005) assert that the use of sophisticated website security tools and their dissemination to users, greatly enhances the confidence in e-government services.

Whilst the current research is focused on citizen perception of security, rather than trust per se, it is essential to look at trust models to clarify the role that security plays in improving citizen trust. Actually, the concept of trust is a complicated one, explored from various perspectives within different disciplines, including philosophy, sociology, management, and economics, particularly e-commerce (Lewick & Bunker, 1996; Riedl, 2004; Kim et al., 2005). These are not areas of interests for this research, so they will not be explored further, but they are mentioned here to highlight the complex nature of trust. This dissertation is focused instead, on citizens' online trust in e-government services from an information security perspective.

Furthermore, trust is hard to be observed or directly measured. Indeed, it is a dynamic concept that can be developed within a number of stages. For example, Shapiro et al. (1992) developed such a model, which was later been updated (Lewick & Bunker, 1996; Ratnasingham, 1998). This model presents a hierarchical development of trust that involves three stages: evaluation of risks and benefits; development of a trust relationship, where the trustor can predicate the trustee behaviour based on knowledge or previous experience; and identification based trust, where there is a mutual understanding of the other parties' motives and preferences.

Tassabehji et al. (2007, p.7) assert that "While the phenomenon of trust is difficult to observe in a commercial context, it is even more so in the context of government as there are more layers of complexity in the trust formation dynamics for e-government." These scholars explored citizen engagement with e-government in a security context, dealing with the different stakeholder perspectives on issues of security, trust, and authentication. Based on this, the scholars presented a case for building a trust verification agent (TVA) to bridge the gap in the interpretation of security information between e-government service providers and citizens. The TVA is a software tool that can take an organisation's security statements or audit and infer how effectively this meets the security concerns of a particular citizen. Moreover, by using rules-based expert systems techniques, the TVA is also able to describe the basis for its evaluation. The TVA provides citizens with the required information and the ability to judge the level of security provided by an e-government system. For instance, technical information of security infrastructure is complex and can be difficult for citizens to understand, but the TVA tool can translate this information to the appropriate language. This will help citizens to take decisions about whether they are able to trust the service and use it or not.

Indeed, it is required, in the context of this research, to attain a deeper understanding of the relationship that security plays in building citizens' online trust. In addition, it is required to explore how dissemination of information about an implemented security approach can affect citizens' willingness to use government e-services. Accordingly, Tassabehji et al. (2007) suggest that it is imperative to do the following; firstly, identify the basic requirements of citizens for engaging with e-government services, with a specific focus on security. This can be applied through developing a simple interface, such as a scorecard for citizens to determine what they would consider acceptable security. Secondly, an information security audit can be conducted based on an evaluation of the security infrastructure within e-government systems. Lastly, an independent trust verification agent (TVA) that is able to translate or disseminate the electronic security audit and report to the citizen regarding the level of security acceptability can be developed.

A paper by Oliveira et al. (2017) analyses how various sources of trust, i.e. consumer characteristics, firm characteristics, website infrastructure composed with a lack of integrity, privacy as well as security and likability and interactions with consumers, influence its dimensions i.e. competence, integrity, and benevolence. The researchers state that perceived risk affects purchasing behaviour, because for many people, web-browsing feels safe.

However, transacting on the Internet is a serious risk, where there is no integrity among the Internet vendors, and the web environment has no privacy or security. As a result, to what extent a user believes it is unsafe to use the web, or that negative consequences are possible, this will negatively affect customers willing to use electronic transactions. The researchers also clarify that the two ways of affecting customers' online trust are the website likability and the need for web security. From this, two different hypotheses were formulated, first, the likability of the website infrastructure positively influences the following perceptions of an Internet vendor: (a) competence; (b) integrity, and; (c) benevolence. Second, the lack of integrity, privacy and security of the website infrastructure negatively influence these perceptions. The findings of the study suggest that consumers' tendency to trust, privacy concerns, security concerns, and information quality of the website all have a strong effect on their trust in the website.

In a further analysis, several sources where trust might improve are also defined by Chen and Dhillon (2003). Based on the literature in general management and marketing, the sources of trust are categorised as the characteristics of the consumer, the firm, the website as well as the interaction between the consumer and the firm. Determining the sources and dimensions of trust (competence, integrity and benevolence), a path model for building user trust in electronic transactions is proposed. In light of the web characteristics, the researchers indicate that since it is hard to determine whether a particular website is professional enough, it could be better to focus on a number of structural assurances. Such assurances offer tangible signs intentionally used to enhance user online trust in electronic services. These signs could be a return policy, privacy and security policy, e-mail address, contact numbers and trustworthy details about the organisation that may be provided by certification or licences. Added to this, third-party assurances, such as TRUSTe for privacy assurance, and a WebTrust certificate to confirm that specific technologies to enable a secure and reliable service are being used. Moreover, legal recourse mentioning that the organisation will guarantee consumers privacy and data confidentiality. The authors concluded that by carefully addressing trust issues in the four categories mentioned above, and understanding how the different characteristics influence organisation competence, integrity and benevolence, users' online trust can be developed.

In the context of e-government, particularly in Jordan, Alomari et al. (2009) confirm that the government needs to address security in the design phase in order to enhance public trust in e-government. Majdalawi et al. (2015, p.219) state that "trust is a vitally important component

of e-government projects. Without trust, citizens who may already be cautious of using technology may avoid the use of online services that ask for detailed personal information". Therefore, these researchers suggest that the government should designate a senior official responsible for computer security; back up information regularly; train employees in computer security; continually assess systems to make sure that security precautions are being implemented; evaluate the performance of system managers in adhering to sound security practices; keep personal information collection to a minimum; and not disclose such information without expressed prior consent. Indeed, trust and security are closely connected, as information security relies on people and security extensions, such as authentication, authorisation, access control, non-repudiation, privacy and anonymity.

Part B) Theory

2.6 Theories/Frameworks used in e-Government Research

This section provides a discussion on the theories/frameworks used in e-government research, including TAM and the Diffusion of Innovations (DOI) Theory.

2.6.1 Technology Acceptance Model

Many researchers have investigated the possibility of e-government adoption by exploring the factors that influence the decision to take up a technology through classical theories of technology acceptance. The most well-known model is the Technology Acceptance Model (Davis et al. (1989), which pertains to utilising perceived usefulness (PU) and perceived ease of use (PEoU) in predicting intention to use (ITU). Management and IS researchers have deployed TAM extensively, such as Alomari et al. (2009), Dimitrova and Chen (2006) and Venkatesh and Davis (2000). Despite the similarities between TAM and the DOI model, TAM places emphasis on two basic factors: social influences and psychological predispositions. It is derived from the theory of reasoned action (TRA) by Fishbein and Ajzen (1975), which holds that intention is affected by one's behaviour towards technology and the surrounding people. Furthermore, TAM clarifies that both PU and PEoU are determinants of consumers' attitudes. Davis (1989, p.320) defines PU as "the degree to which a person believes that using a particular system would enhance his or her job performance". Davis also defines PEoU as "the degree to which a person believes that using a particular system would be free of effort". The TAM

approach is based on the relationship between the adoption of a new technology and PU and PEoU variables, which means that the higher the perceived usefulness of a new technology, the greater the possibility it will be adopted by stakeholders. The core idea is that the decision to adopt a new technology service depends on the subjective perception of the user. The other main concern of system acceptance is to provide users with a useful system that is easy to use. That is, helpful and flexible technology will encourage people to use it (Alomari et al., 2009).

2.6.2 Diffusion of Innovations Theory

DOI has evolved with studies focusing on the adoption of a wide range of innovations, such as new health practices and Internet services. According to Rogers (1995, p.12), innovation is "an idea, practice, or object that is perceived as new by an individual or other unit of adoption". In this context, e-government is considered as a technological innovation that is being adopted by many governments around the world. Previous studies relating to the adoption of IT have involved using DOI theory in order to argue that IT innovation is based on an innovation's characteristics, such as relative advantage, compatibility, complexity, trialability and observability. These studies of innovation adoption implementation found that relative advantage, complexity and compatibility were consistently significant in influencing innovation adoption (Tornatzky & Klein, 1982). In a study by Rogers (1983, p. 15), relative advantage is defined as "the degree to which an innovation is perceived as better than the idea it supersedes", while complexity is "the degree to which an innovation is perceived as difficult to understand and use". Rogers also describes compatibility as "The degree to which an innovation is perceived as being consistent with the existing values, past experience, and needs of potential adopters".

Furthermore, DOI theory introduces a comprehensive adoption model, which consists of five categories of adopters, based on how early they start to use the innovation: innovators, early adopters, early majority, late majority, and laggards (Rogers, 1995). The DOI theory has been used to identify the social factors influencing e-government adoption. In the context of Jordan, researchers have examined the applicability of relative advantage, complexity and compatibility to identify these factors. For example, (Alomari et al., 2009) explored some social factors, such as trust, beliefs, education and accessibility, which were identified through DOI theory in the context of adoption of e-government in Jordan. In short, a number of researchers have adopted DOI theory in order to study the effects of relative advantage, compatibility, ease

of use and image on citizen intention to use an e-government service and presented a high-level research model based on these constructs (Carter and Belanger (2004); Moore and Benbasat (1991)).

2.7 Theories/Frameworks used for Online Trust and Information Security

This section presents the theories/frameworks used for online trust and information security, which are the research focus: a conceptual model of trust, the TFI model for IS security, and general deterrence theory (GDT).

2.7.1 A Conceptual Model (Internet Use, e-Government Satisfaction, and Trust)

E-government is considered a new form of administration, and the degree of citizen expectations in terms of services, information access and provision, and interaction with government in general, can lead to important outcomes, such as trust (Thomas, 1998). Welch et al. (2005) propose a model that covers both perceived satisfaction with e-government and perceived satisfaction with government as contributors to citizens' trust in government. In addition, the model focuses on website usage as a key factor determining e-government perceptions. The relation between trust and satisfaction, which is recursive, also means that satisfaction leads to trust, and vice versa. The range of visits of an individual to government websites can be determined by various factors, such as general Internet use, demographic characteristics and individual needs. Moreover, overall satisfaction with government is a multidimensional construct, consisting of such values as efficiency, effectiveness, accountability and equity (Musso et al., 2000). Accordingly, the main parts of this comprehensive model are website use, e-government satisfaction and citizen trust in government.

First, citizens' use of government websites will have an impact on their expectations of how well e-government efforts fulfil their needs. Of course, general Internet use gives a comparative framework for people to assess whether government websites are utilising technology in ways that satisfy their desires regarding e-government (Hart & Teeter, 2003). Second, citizen satisfaction with e-government derives from several factors, such as information quality, service convenience, ease of access, and interactive communication. To simplify a long list of

contributing factors, Mutz and Flemming (1999) categorise them into three main groups: transactions, transparency and interactivity.

Essentially, *transactions* include the perceived convenience, quality, privacy, efficiency and security of online transactions with government. Indeed, when transactions are repeated, this may contribute to improved trust, because this does not contravene expectations of convenience, quality, privacy, efficiency and security (West, 2004). Regarding *transparency*, this refers to citizens being able to monitor the organisational performance of government entities through their websites (Reichard, 1998). For, allowing citizens to monitor organisational activities and procedures can generate greater trust. In this case, organisational processes, decisions and outputs should reasonably fit citizens' expectations, while *interactivity* is a way to describe the willingness or ability of an organisation to be responsive to citizens (Demchak et al., 2000). In terms of trust, when a government provides citizens with reliable information about its processes, decisions, activities and outcomes, this leads to two events: first, the information gap that causes distrust is narrowed; and second, as mentioned in the above section, greater transparency can enhance trust in processes and institutions in general (Thomas, 1998).

2.7.2 Technical, Formal, Informal IS Security Model

A few previous studies have shown that information security standards at the organisational and administrative levels are not clear in many organisations (Bjorck, 2005); Oscarsson (2002). For this reason, an information security model has been proposed that includes all the necessary elements. This model introduces a comprehensive view of information security and uses concepts based on semiotic theory, which views information systems security as comprising technical, formal and informal (TFI) parts. Semiotic theory is based on the observation of signs for every object, function and physical item. Moreover, the TFI model provides an understanding of the information security domain in order to create a well-founded theoretical framework.

The concept of information security is commonly used, involving data security and IT security terms (Bjorck, 2005). According to the US National Information Systems Security Glossary (US, 2006, p.I), information system security is:

> "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats."

From this definition, there are four clear characteristics of information security: availability, confidentiality, integrity and accountability. As mentioned before in the IS section, a successful IS is one that provides the right information to the right people at the right time. *Availability* concerns the ability to use resources within the desired time, whilst *confidentiality* refers to giving access rights to authorised parties only. *Integrity* is about protection against any unauthorised modifications, whereas *accountability* relates to deriving performed operations from an individual in a clear way (Dhillon & Backhouse, 1997).

The TFI model contributes to the IS security literature by clarifying the three levels it contains (Harris & Mishra, 2006). *Technical* concerns the hardware, software and networks. This level refers to automating parts of systems, such as the use of computers in some operations and tasks. *Formal* involves policies, processes, procedures and all organisational-level security mechanisms. *Informal* relates to individual-level security mechanisms, such as beliefs, the attitudes of employees, culture and values, and awareness.

From a technical perspective, IT security solutions are required to maintain confidentiality, integrity, availability and accountability. Examples of techniques for doing so include: the encryption of data, access control systems, intrusion detection systems, firewalls, authorisation and authentication mechanisms, and database security features. The technical level pertains to the selection of an appropriate technological solution based on the needs of the application used (Ahlfeldt et al., 2007). The formal level of IS security, which concerns the processes, policies, rules, and standards, is aimed at presenting an interface between the technical and informal levels. As Lee (1999) definition of an IS clarifies, most efforts in IS management are concentrated on the formal level. Regarding which, when reviewing the security literature, it shows that information system research is moving towards social and organisational perspectives, and not simply a narrow technical viewpoint (Dhillon & Backhouse, 2001). In order to address security at this level, there are such methods available as evaluation, checklists and risk analysis.

In brief, information security plays a key role across different domains, examples of which include: integrity of transactions in business, confidentiality of patients' information in healthcare and safeguarding citizens' personal information in e-government. The development of and progress in ICT has required researchers to develop complete information security models, which include all security measures, at the technical and administrative (formal and informal) levels that can be adopted by organisations (Harris & Mishra, 2006).

Thus, in the context of e-government, governments need to address IS security in order to enhance citizens' trust in e-government, which should lead to a stronger intention to use e-government services online. In addition, citizens' personal information is highly sensitive and it is the government's responsibility to protect it. Accordingly, governments should adopt a comprehensive IS security model or framework, in order to cover all potential threats at all levels and to be able to deal with them. In fact, few studies have used the TFI model, particularly in the context of e-government, although applying this model can help scholars develop an understanding of cybersecurity which goes beyond the technical level and addresses risks from an organisational and behavioural perspective (Ahlfeldt et al. (2007); Wimmer and Von Bredow (2002)). Also, the TFI model describes what information security involves in a 'holistic' way. The three levels of the TFI model (technical, formal and informal) are integrated to cover all elements of information security within the domain of e-government.

2.7.3 General Deterrence Theory (GDT)

General deterrence theory has been used in the area of information systems. Straub and Welke (1998) state that GDT introduces a theoretical base for the use of certain procedural and technical measures in order to limit unauthorised behaviours of information misuse in organisations through determining severe punishments and warning users regarding these penalties. According to Straub and Nance (1990), information misuse precautions in most organisations are derived from technical and socio-organisational measures. Furthermore, security mechanisms can be divided into four phases: information security policies, security awareness programmes, security monitoring, and preventative security software.

First, a security policy includes a statement of the policy, the authorised access and usage of equipment, system management, procedures and penalties for policy violations. The main goal of such a policy is to prevent information misuse by identifying unacceptable behaviours,

thereby assuring users of the threat of being punished (Lee & Lee, 2002). Second, many security incidents have occurred because of employees' lack of awareness of IT security procedures (Hansche, 2001). The importance of security awareness training lies in enhancing employees' attitudes relating to information security policy and to convince the staff that the organisation is serious about securing its information systems. Third, monitoring actions are active security efforts, such as observing employee activities with information systems. For monitoring purposes, information systems usually apply intrusion detection software to monitor a system or network, which records employee computing activities and policy violations and then, produces reports for management consideration. In addition, the physical audit of staff computers is undertaken to detect any installation of unlicensed software (Panko & Beh, 2002). This will make employees aware of the possibility of being punished, as the organisation is able to detect any unauthorised behaviour. Last, preventative security software is essential in order to prevent information misuse, for example, by stopping outgoing email messages that include inappropriate content, and protecting information systems against unauthorised access. Hence, users will be aware of the preventative controls and deterred from carrying out any serious levels of computer abuse (Irakleous et al., 2002).

In terms of e-government, government agencies not only have to establish clear and strict information security policies, but also need to inform employees about acceptable and unacceptable behaviours as well as stipulating what punishment may be given against the latter. Information security awareness is one of the important measures that limits information misuse within an organisation. Regarding monitoring, this makes employees aware of the possibility of serious punishment and security mechanisms then become more useful. Finally, preventative software is an urgent measure for an e-government system to implement due to the significant benefits it will provide, such as blocking undesired messages and enabling user authentication.

2.8 Justification of the Theoretical Framework Used in this Research

This section explores the importance of the theoretical framework used, which is followed by its evaluation as well as how it fits with the overall aims and objectives of the research. In order to introduce security solutions for e-government, some researchers have, as referred to above, proposed a TFI framework with a basic focus on the processes to be considered (Ahlfeldt et al. (2007); Wimmer and Von Bredow (2002)). For example, Ahlfeldt, Spagnoletti, and Sindre have used the TFI model in order to: a) evaluate the security and privacy of patient information

in healthcare, and b) examine how the users of the system are influenced by the security requirements as well as how they influence information security. Similarly, Wimmer and Von Bredow discuss security approaches to e-government programmes based on a comprehensive approach that considers security beyond the technical aspects (social, cultural, legal, and political). They then applied these security solutions to different scopes of e-government, in particular, in e-administration. As Wimmer and Von Bredow (2002, p.10) assert, "further research in this field in e-government investigating the application of existing security solutions for all domains of e-government is necessary". Additionally, research using the TFI model can help explore the gap between strictly defined security countermeasures and the investigation of more informal aspects, like security awareness.

In general, this multidimensional model presents an overall security threat analysis from different points of view, both technical and non-technical, and includes formal and informal aspects. Technical security threats in e-government can be classified into three basic groups: interceptions that attack confidentiality through unauthorised access; modifications that attack integrity by unauthorised changes; and interruptions that attack availability, because of damage to functionality (Lee & Lee, 2002). In other words, technical threats involve inter-communication, intra-communication and system threats.

Security threats also need to be analysed from a non-technical (formal and informal) viewpoint (Wimmer & Von Bredow, 2002). This analysis should involve strategic and operational security considerations for processes and transactions. In e-government, most information is security-sensitive, and the consequences of misuses of stored information relating to citizens, such as the committing of a crime or credit card misuse when paying online, are very serious. Citizens need to have security solutions in order to trust government websites and e-services, otherwise they will feel vulnerable when using e-government systems. At the same time, citizens have to recognise that there is always uncertainty with regards to information security.

In addition, security threats have to be considered for the different domains of e-government, such as e-administration, e-assistance, e-democracy and many others (Lenk, 1998). In each of the three levels of electronic processing (information, communication and transaction), certain security requirements have to be determined. The portal that provides the information has different security requirements from e-government systems and is responsible for providing protection for transactions involving highly sensitive information.

For the above reasons, using a comprehensive security theoretical framework, such as the TFI model, will enable deconstruction of the IS security in the e-government of Jordan. This research is aimed at examining how information security is evaluated and approached within the e-government programme of Jordan as well as determining whether or not this influences citizens' online trust. This requires the provision of an overview of the current status of e-government and analysis of the three levels of information security within the e-government programme: technical, formal and informal (see Figure 8). In this model, other elements relating to organisational and human aspects are taken into consideration in addition to the technical aspects, which thus expands the scope of analysis from a technical security perspective. The model aims to present information security measures by combining the three levels. Therefore, this framework can be used to examine and analyse where the problems and needs exist in the domain of information security (Ahlfeldt et al., 2007). The potential in theoretical contribution within the TFI model could be in the administrative part in particular (e.g. security awareness at informal level, external communication at formal level).

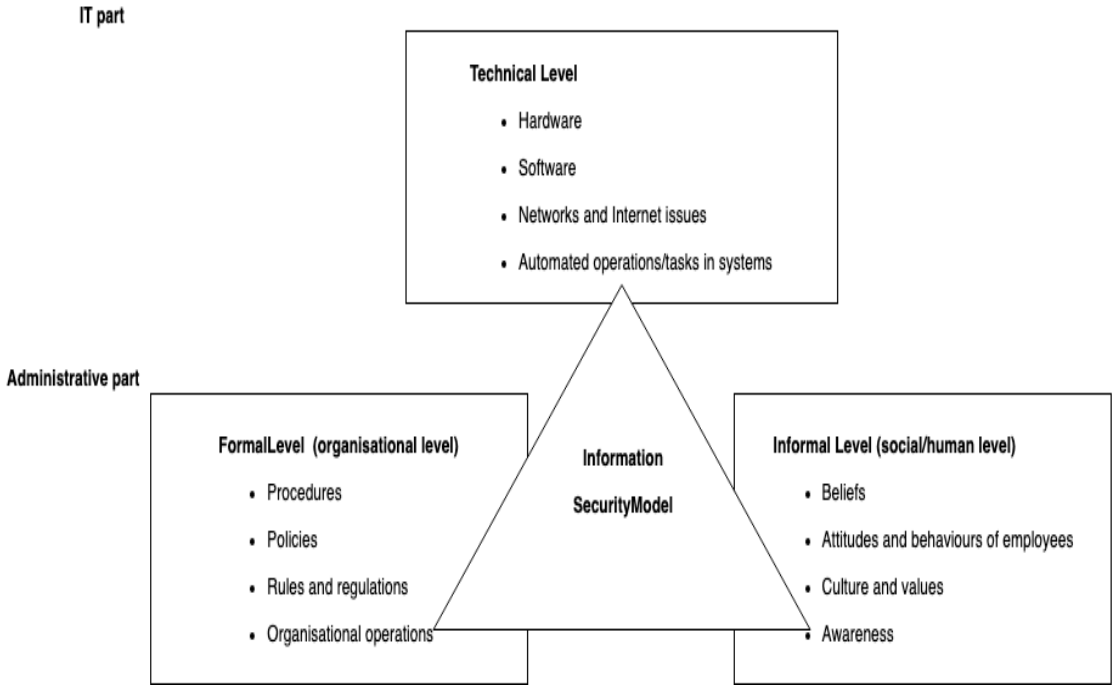


Figure 8: TFI information security model (based on (Ahlfeldt et al., 2007))

In order to re-evaluate the CIA triad, socio-technical security studies have adopted the TFI model on several occasions to interrogate its contribution (Dhillon, 1995; Halperin, 2006; Åhlfeldt et al., 2007; Canhoto & Backhouse, 2007; Dhillon, 2007; Eibl & Schubert, 2008;

Spagnoletti & Resca, 2008; Backhouse & Halperin, 2009). Halperin (2006) paper discusses the increasing issues of identity, highlighting the main developments that lead to the emergence of identity as a new field of research. The author explores what the research community has achieved so far and what is the needed future work. The state-of-the-art in identity research is analysed using the TFI model, which describes information systems through technical, formal and informal layers. This analysis shows that studies mostly focus only on one layer of the model at a time, ignoring the importance of the others. There has been practically no comprehensive study in the identity area, which has led to only a partial understanding and conceptualisation of the identity domain.

For the first phase of the analysis, the researcher considered the different perspectives according to which the theme of identity has been addressed, while the second phase in the analysis involved measuring each sampled study against the TFI model to find which levels were discussed in each case. In the conclusion of this study, a cross-disciplinary research is called for in order to achieve a comprehensive understanding of identity in the information security society.

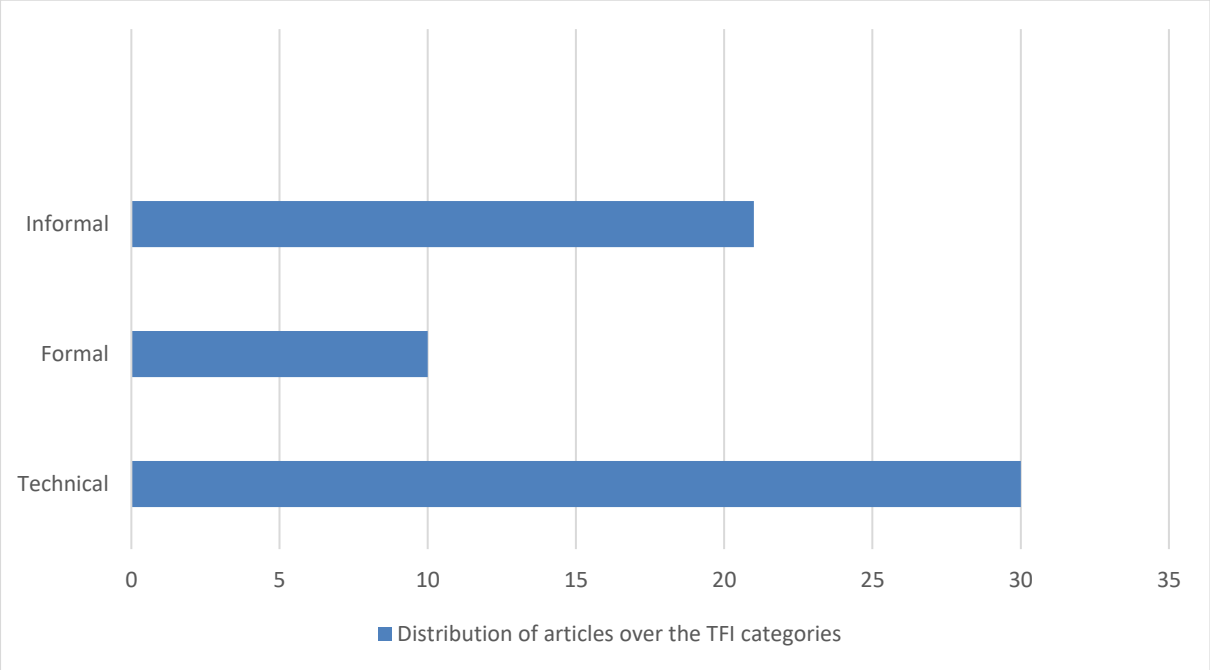


Figure 9: Distribution of articles over the TFI categories (Based on (Naik et al., 2014))

A study by Ahlfeldt et al. (2007), extended the InfoSec model in terms of its administrative part using the elements of the TFI-model. The concern of the administrative part is information security management, involving both formal and informal levels. As mentioned before, the

formal level has many elements, such as policies, processes, procedures and rules aimed at defining an interface between the technological subsystems, while the informal level concerns human aspects. First, the authors proposed a comprehensive view of information security based on a Swedish model. Then, they extended this model, adopting a holistic view of an information system as combining the technical, formal and informal (TFI) levels and proposed the InfoSec model. The paper was aimed at providing a clear understanding of the information security in order to present a solid theoretical framework. To this end, the authors applied this Information Security (InfoSec) model to three different case studies in the healthcare domain.

The first case study was conducted in the home healthcare of two municipalities. The focus was on patient information privacy and involved conducting interviews with the healthcare staff working in home healthcare, in addition to observing how they managed personal data in their work. The second case study also included interviews and observations with healthcare staff at a hospital in the western region of Sweden. The researchers examined how users of electronic health records are influenced by information security requirements, and how their practices affected information systems security. The third case study was a part of the VITA Nova Hemma research project, which had the purpose of examining the link between various processes that connects different healthcare parts. This was achieved through the participation of different healthcare providers. Interviews were held with administrators for the respective healthcare systems. The administrative part in the extended InfoSec model has been divided into formal and informal parts. The formal part also has been divided into two sections, namely external and internal. The case studies results indicated that in the internal formal part, there is a need for information strategies and information security policies strongly related to context or the type of domains, such as healthcare. Regarding the informal part, they found that there is also a need for measures to support the organisation in implementing information security awareness.

Backhouse and Halperin (2009) noted that as most European countries develop electronic identity cards for identity management, the European Union (EU) concerning about its interoperability agenda in both eHealth and e-government. Research on interoperability regarding the identity management system was performed as part of the EU federal identity information system (FIDIS) project and this study presented some of this work. It provides a clear understanding of the concept of interoperability at the beginning, and how it is being applied in the area of identity management. The conceptual understanding goes beyond the

technical elements of interoperability to three combined aspects of identity management (IDMS): technical, formal and informal. The TFI model was proposed and clarified as a useful guide for directing research efforts to the different elements of interoperability and the relation between them. The aim of the study was to find a solid base for future work on interoperable IDMS. The study presents the perspective of the most important stakeholders on the focal area. Firstly, it reports the views of specialists from the public and private sectors across Europe countries. Then, EU citizens' perceptions and attitudes with regard to interoperable IDMS are discussed. The findings showed the major challenges and implications related to shared personal data in providing e-services. Moreover, the results indicate that the ultimate success depends on satisfactorily addressing all elements of each level of the TFI framework.

In a study by Eibl and Schubert (2008), information security is discussed as a major quality factor for information systems and essential for websites that offer services like e-learning. The researchers present design criteria for e-learning systems according to three aspects, these being: disciplines of educational science, software engineering and information security. Furthermore, they discuss how the complexity in the system increases with each criterion applied in implementing such an e-learning system, this definitely leads to further demands for information security analysis to meet recent emerging security issues. The scholars stress how it is important to take security aspects into consideration to protect the learning process and learners' personal data. They consider e-learning systems to be secure, if they ensure availability, integrity and confidentiality for authorised users, emphasising on the need to sufficient access control mechanisms in order to do so. This paper shows that security aspects must be managed from a technical point of view, to build a convenient infrastructure with sufficient control and detection mechanisms, as well as from an organisational point of view in order to set an effective information security related policy, procedures and operations. Besides that, granting users' privileges should be based on planned activities of different roles in the system.

Halperin and Backhouse (2007), in their study, confirmed that the three layers of the TFI model have an interdependent relationship and a common basis. The technical controls require formal aspects, which in turn, need to consider informal issues. For instance, information security auditing relating to security incidents handling as well as human resources management is strongly connected with training and awareness courses. As a result, this model will be a useful tool, especially in bringing into consideration the informal issues into account and can be

extended to cover all areas relating to information security issues. Stamper et al. (2000, p.19) explain this mutual interrelation of abstracted layers, by stating that:

> *"Informal norms are fundamental, because formal norms can only operate by virtue of the informal norms needed to interpret them, while technical norms can play no role…unless embedded within a system of formal norms."*

In brief, the informal is considered as the outer shell containing the formal, which, in turn, contains the technical. In order to examine the insider, the technical layer, it is first strongly required to consider the outer layers, the formal and informal.

The research methodology is explained and justified in the next chapter.

3.0 Methodology

3.1 Introduction

This chapter presents the research methodology, which is aimed at evaluating information security within the e-government programme in the context of Jordan and then, relating this to the issue of citizens' online trust. This is achieved using qualitative methods and conducting semi-structured interviews for information security evaluation purposes. In addition, a complementary survey is conducted in order to collect data about citizens' trust in and beliefs about e-government systems. In this chapter, the research methods used are discussed, the data analysis methods clarified, the research ethics issues taken into account are explained and the limitations of the research methods are addressed.

As stated previously, for this research, a mixed methods design is deployed that commences with the interpretivist case study research design of the MoICT; this is followed by a survey that is distributed to citizens, the design of which is informed by the issues raised in the case study. Qualitative research is not only used to gain an understanding of opinions, behaviours and values regarding a certain issue, but also to provide insights into a research subject which will help analyse the situation, events and actions concerned. Qualitative data collection methods include individual interviews, observations and focus groups (Taylor & Bogdan, 1998). Quantitative research is aimed at measuring the research subject using numerical or statistical data, being also used to measure opinions, attitudes, behaviours, and other defined variables in order to gain results from a large sample. A common quantitative data collection method is a survey, such as an online or paper questionnaire (Neuman, 2005). This dissertation uses a survey in a complementary way and in order to elicit the views and perceptions of citizens on elements that relate to the security of e-services. The overwhelming majority of the data for the customisation of a TFI-oriented framework for e-government have come from the case study of the Ministry of ICT. The survey helps to create a connection to citizens' perceptions on the security of e-government services.

3.2 Philosophical Paradigms

In this section, a comprehensive description of research paradigms is presented, clarifying the difference between various philosophical approaches.

The two basic philosophical concepts are ontology and epistemology. According to Carson et al. (2001, p. 4), "Ontology is reality, epistemology is the relationship between that reality and the researcher". Within this, there are two main research paradigms: positivism and interpretivism. Ontology relates to 'what is reality' and 'what is the nature of that reality'. Blaikie (1993) defines ontology as the science of being and concerning the nature of reality. Put briefly, ontology refers to addressing the essential question of whether a research subject needs to be perceived as objective or subjective.

Epistemology is the philosophy of knowledge that explains how a researcher can know the reality of a particular topic (Trochim, 1998). It requires a determination of the relationship between the knower and what is known as well as how to gain knowledge. Epistemology is closely connected with ontology and methodology, as ontology concerns the philosophy of reality and epistemology clarifies how researchers come to know that reality. Methodology refers to identifying the particular tools/techniques used to seek out the knowledge.

In the context of positivism, a positivist ontology holds that there is a single external objective reality to any research phenomenon or situation, regardless of the researcher's beliefs or thoughts (Carson et al., 2001). For this reason, positivist epistemology is based on the notion that researchers are independent of science. Researchers also attempt to identify clear research topics and analyse phenomena by presenting appropriate hypotheses and using a suitable research methodology. In addition, researchers try to distinguish between reason and feelings, thereby keeping a distance between themselves and the object of the study. In other words, they know the difference between science and personal experience; fact and value judgement. In sum, quantitative researchers tend to adopt a positivist approach, measuring research phenomena using statistical and mathematical techniques (Coll and Chapman (2000); Cousins (2002)).

On the other hand, interpretivism in relation to ontology and epistemology involves adopting the stance that holds that there are multiple realities. Briefly, interpretivism allows researchers to consider different realities and perspectives, the contexts of the given phenomena, and to focus on the understanding and interpretation of data. Interpretivists adopt more personal and flexible research frameworks in contrast to the positivist approach. The researchers' personal experiences are interdependent, which means that they tend to interact with the subjects of study to collect data, such as when conducting interviews (Black, 2006).

According to Olson (1995), understanding the differences in epistemology between quantitative and qualitative research methods starts mainly as a philosophical practice. Objective information describes reality and the natural structure or manner of reality, while subjective information is defined as the ideas assigned to reality by people. Generally, objective information refers to external reality and subjective information to internal reality (Eisenhardt & Graebner, 2007). Campbell (1997, p.122) asserts that qualitative research depends on the idea that "reality is socially constructed and that variables are complex, interwoven, and difficult to measure", which requires the researcher to engage personally in the research and to seek key points of view. The purpose of qualitative methods is to figure out the meanings of the phenomenon under study, rather than measuring it, and the data collected from the participants within the study are subjective, expressed in their own words. Moreover, qualitative research provides a large amount of data, because of its exploratory nature (Creswell, 2009). Furthermore, the research process is not sequenced, but rather, it is iterative, with the data collection processes and analyses being undertaken at the same time. Thus, the qualitative researcher needs to consider effort and time, because that person has to be involved in the research process with the participants before, during and after the data collection (Harrison, 2013).

In quantitative research, any hypothesis should be proved or disproved by employing mathematical and statistical tools. A study group can be selected in the process that plays the role of a control group. The collected data are numerical and the researcher needs to measure the variables one by one. Quantitative methods are structured, such as the use of different types of surveys: for example, paper and online surveys (Crotty, 1998).

For this research, an interpretivist approach is adopted with a case-study research design involving interviews at the MoICT as the primary data collection method in order to gain an in-depth understanding of the concept of information security within the e-government programme in Jordan. In addition to this, the connection between citizens' online trust and information security is explored through a complementary survey.

3.3 Research Design and Data Collection Strategy

This section describes the research design and what methods were used for the data collection and analysis.

According to Hakim (2000, p.3), "research design is the point where questions raised in theoretical or policy debates are converted into feasible research projects and research programmes that provide answers to these questions". It involves the methodology and procedures used to conduct a piece of research. Researchers can adopt theories that try to explain certain phenomena, then design research in order to test these theories using qualitative or quantitative methods. The design of a piece of research covers the study type, research questions, theories used, hypotheses, variables, data collection methods and/or data analysis plan. In general, research designs are classified into quantitative, qualitative, and mixed methods. Other forms can also be used, such as correlational (observational studies), descriptive (case studies and surveys), experimental (using random assignment) or semi-experimental (field experiments).

In relation to this research, the research questions have to meet the main aims and objectives of the study. Accordingly, appropriate questions have been identified in order to be researched and addressed. As mentioned in Chapter 1, the research questions are as follows:

- What is the approach to information systems (IS) security in the Jordanian e-government programme at the technical, formal and informal levels (to be examined based on the TFI security model)?
- Why is the government of Jordan not attempting to enhance citizens' online trust by communicating (elements of) security countermeasures in their e-government programme (technical/formal/informal)?
- What are the citizens' perspectives and perceptions about the security of the e-government programme and how does this affect their adoption of e-services (online trust)?

The above questions guided the research in terms of enabling the researcher to focus on what to study and how to conduct the research. As mentioned above, this research is aimed at exploring the information security approach within the Jordanian e-government programme. Through a complementary survey, there is also examination as to whether citizens' online trust in the e-government programme in Jordan is influenced by perceptions of its level of information security or by other factors. Thus, the MoICT is the research case study, as it is responsible for the e-government programme in Jordan, in general and the Department of e-Government, in particular. In addition, secondary data has been utilised to support the research,

and synthesised in a literature review focusing on e-government security in the context of Jordan.

3.3.1 Data Collection Methods

For this research, three methods of data collection were used. First, the data collection relied on resources within the MoICT, including official documents and government publications. In addition, data were gathered from secondary sources, such as books, newspapers, periodicals, journals and articles. These assisted in the application of the information security TFI model, as well as in analysing and discussing the case study.

Second, semi-structured interviews were conducted with officials at the MoICT, who have experience in the e-government programme and are *experts in the area of information system security*. That is, those administrators and staff of the e-government programme within the ministry who are responsible for information systems security, networks and the management of information technology were the targets of the study. The interviews were conducted to determine the current situation of the e-government programme from an information security perspective. The interviews allowed participants to expand and focus on the topics they considered important. The semi-structured interviews consisted of open-ended questions about e-government activities regarding information system security and related issues.

Third, based on the collected qualitative data, a survey was designed and implemented in government institutions. This method allowed the researcher to evaluate the perspective of citizens' trust, beliefs and satisfaction. Thus, it was targeted at citizens who were waiting to be served in number of government service-based organisations.

3.3.1.1 Interviews

In this research, data collection relied mainly on interviews as the key method, because this was deemed the most appropriate way of gathering information about the security approach to e-government programmes. During the first month of six months of data collection, the researcher identified the issues relating to the TFI model different levels that would be included in the interview schedule. Furthermore, the researcher used this pre-interview period to determine which staff would be most appropriate for requesting an interview when considering the different levels of this model. That is, the interview questions were focused on e-

government activities regarding information system security at different levels based on the categorisation in the TFI Model (see Table 4). Department managers, information security experts and system administrators were asked to provide an overview of the cybersecurity functions at the Ministry (see Table 5). In addition, there were general security-related questions targeted at employees in terms of whether they had received IS security training, and were aware of security policies and procedures, etc. In total, 30 semi-structured interviews were conducted. In terms of data recording, in the case of the Ministry, tape-recording was not allowed as confidential and sensitive material was discussed. Thus, the researcher recorded the data by a note-taking approach during the interviews and refined those afterwards in order to produce an extensive record.

The interview data were categorised based on the TFI model, as explained in detail below.

(T) Technical Level

The researcher collected data about the hardware, software, networks/Internet issues, and automated operations/tasks in systems. For example, the ministry is using PKI, IPS, a firewall, and other software to address IS security. They also have a secure government network (SGN) and secure government bus (SGB). Moreover, the researcher asked about projects that were in progress, such as private cloud and a cybersecurity army project. She also enquired whether the administrators referred to ISO 27001/ 27002 to define security controls and requirements or not.

(F) Formal Level

(Organisational level, internal/external)

The researcher collected data around organisational procedures, policies, laws and regulations regarding information security. In respect of which, the Ministry conducts information security audits, but not regularly, and there was a lack of cooperation and trust among government departments. The latest technologies were not being used within the systems and networks. The Ministry also needs to update the national security policy and strategy regularly. Additionally, it is responsible for auditing information security compliance and commitment by other government institutions.

(I) Informal Level

(Human level, employees /citizens)

The researcher collected data regarding employees' cybersecurity awareness, beliefs, attitudes, culture and values. For example, the employees have terms and conditions regards IS security in the employment contract, whilst the NITC arranges security training and awareness courses for government employees. The participants were asked what steps had been taken to facilitate citizens using e-services securely and enhancing their cybersecurity awareness. Questions regarding the role of citizens' perceptions about cybersecurity and the role of security in using e-services were put as well.

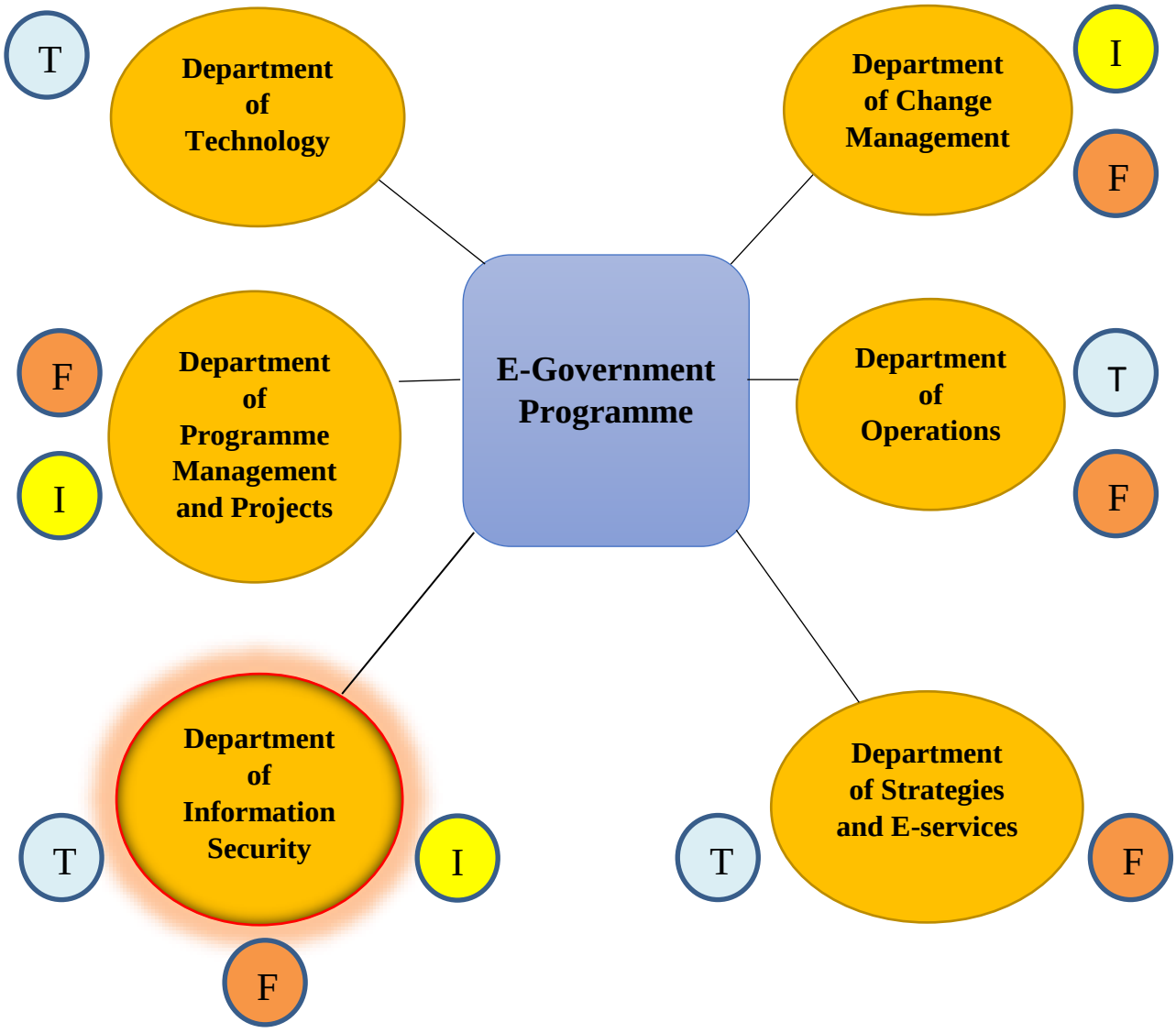


Figure 10: Interviews plan

Table 4: Interview questioning strategy based on departments (T: technical level, F: formal level, I: informal level)

Technical	1. What are the technical challenges that you face in the IS Security department? What are the latest challenges? How you are managing them? 2. How about technical interoperability of systems and updates? 3. How about the mechanisms to protect information systems from security incidents or attacks? How effective they are? 4. Have you experienced cyber security attacks? 5. In case of the occurrence of any security incident what are the incident handling and reaction procedures? 6. Have the government organisations that provide e-services identified the risks, vulnerabilities and threats from different parties? Do they implement security controls accordingly? 7. What about the mechanism of user authentication within e-government systems/websites (for e-government department staff who have access and for citizens/users using e-services)? The mechanism of access control? ***The researcher explored occasions where the way citizens were using, commenting on and giving feedback on the e-government services has influenced the TECHNICAL dimension of security.*** - Has the government changed anything in technical security because of citizen use, comments, feedback, etc.? Do they even have a mechanism for getting feedback from citizens and if so, how is that used to improve security and perceptions about security? - Does the government have a process of communicating certain technical advances in security so that they can enhance citizen trust? Does it have an information campaign on security? By what standards/mechanisms does it decide what is safe to disclose from a security perspective?
Formal	1. What is the management system of information security? 2. What is the general policy of information security (security guidelines and requirements)? 3. How are the duties and responsibilities separated or distributed to ensure that administrators control all systems and prevent any attempt at unauthorised access? 4. Are you using ISO certification? Why/Why not? 5. What have been your positive experiences, problems, concerns and challenges and how have these affected the management of the e-government security? 6. Are you conducting a regular information security audit? The process of auditing includes what (ex; monitoring, capturing, storing, analysing, and reporting information related to a security event)? 7. What about the general security environment (organisational security policies, procedures, laws, regulations to protect data and confidentiality of information)? ***The researcher explored where the way citizens were using, commenting on and giving feedback on the e-government services had influenced the FORMAL dimension of security.*** - Has the government changed anything in policies, procedures, etc., because of citizen use, comments, feedback, etc.? Does it even have a mechanism for getting feedback from citizens to input into the formal management of IS

	Security, and if so, how is that used to improve security and perceptions about it?
Informal	1. Regarding information security, are there any conditions mentioned in employees' contracts? 2. What are the human challenges that you face in information system security? 3. How do you mitigate for the human security challenges or human factors in information security? 4. What has been the impact of Jordanian culture on cyber awareness? Are employees applying good security practices (ex; logging off computer whenever leaving a computer system, setting strong passwords, reporting security incidents to the appropriate department, checking that antivirus software is enabled and updated, backing up files and data, among others)? 5. What about training courses? What do these courses include? ***The researcher explored where the way citizens were using, commenting on and giving feedback on the e-government services has influenced the INFORMAL dimension of security.*** - Has the government changed anything in the context of cyber awareness? Do they have a mechanism for getting feedback from citizens to input into the informal management of IS Security, and how is that used to improve security and perceptions about it?
General questions with the managers * What are your department tasks and responsibilities? * What has been the impact of Jordanian culture on cyber awareness? * Is the e-government programme responsible for all the services, i.e. are they centralised? * What do you think of cyberwarfare, cyber-attacks between countries, what would you do in such a scenario?	

There is an interrelationship between all three levels as well as between citizens and government organisations. Moreover, the aim was to elicit whether citizens were cyber-aware and had confidence in the security of the e-government programme. The interviewing approach that was followed is described next.

First, the interviewing started with officers of the six departments in the following order: information security, technology, project/programme management, change management, strategies/e-services and operations. The questions interview related to the role of the interviewee and the specific department they were working for (as shown in Figure 10). Second, there was interviewing of employees from all these departments. To do so, the secretary for the e-government programme set a schedule for the researcher based on the availability and roles of the employees in terms of the research goals. Third, interviews were held at MoICT with the general manager of the e-government programme and then the general secretary to discuss the main findings from all the previous interviews. Fourth, additional

interviews were conducted in the National Information Technology Centre (NITC), as they host the database, SGN, and the power is divided with the Ministry. NITC plays a key role and is considered as being the operator of the e-government programme. The interviews at NITC started with the information security officer, then, with the manager of awareness and development, and finally, the manager of the knowledge stations project and two employees on it were interviewed.

Table 5: List of Interviewees (in the same order that the interviews were conducted)

Interviewee post title/role	Expertise of the interviewee regarding the e-government programme	Duration of interview
Head of information security department	4 years	2 interviews 1 hour each
Head of technology department	4 years	1 hour
Head of operations department	6 years	1 hour
Head of change management department	3 years	1 hour
Head of strategies and e-transformation department	5 years	1 hour
Head of programme management and projects department	4 years	1 hour
Employee in security department	3 years	1.30 hours
Employee in security department	2 years	2 interviews 1 hour each
Employee in technology department	3 years	1 hour
Employee in technology department	4 years	1.5 hours
Enterprise architect (application development and big data)	3 years	1 hour
Employee-transformation department	2 years	1 hour
Employee in management and projects department	3 years	1 hour
Quality manager/ department of technology	4 years	2 interviews 1 hour each
Complaints call centre manager/ department of operations Previous manager for e-services projects	5 years	1.5 hours
E-transformation director or manager/ department of business (projects) and department of strategy	6 years	1 hour

(initiatives e-services) / and department of change management.		
Employee in change management department	**2 years**	**1 hour**
Manager of security and technology projects	**7 years**	**1 hour**
Systems engineer in technology department	**2 years**	**1 hour**
Manager of awareness and development at NITC	**3 years**	**1.5 hour**
Information security officer at NITC	**5 years**	**2 interviews 1 hour each**
Manager of knowledge stations programme at NITC	**4 years**	**1.5 hours**
Manager of knowledge station of al-Jubayha branch	**3 years**	**1 hour**
Manager of knowledge station of Abu-nseer branch	**2 years**	**1 hour**
General secretary of MOICT	**5 years**	**1 hour**
IT manager, GENERAL SUPERVISOR	**4 years**	**1 hour**

3.3.1.2 Secondary data collection

In addition, 70 government documents from the e-government programme were studied (ex, national cybersecurity policy, national cybersecurity strategy, annual reports of the MoICT, RFP form, etc.). The researcher examined all documents and reported them within the findings chapter. Information security policies were clarified, each one in the related theme, check meaning covering access control policy, password policy, user privilege policy, incident response policy, intrusion detection policy, file backup policy, systems update policy, asset control policy, anti-virus policy and Internet connection policy.

4.3.1.3 Survey

For the second phase, a survey for citizens was designed and developed based on the collected qualitative data from phase one and also issues highlighted in related studies on developing countries (Bannister & Connolly, 2014). The survey questions were devised to collect data about citizens' perceptions and online trust regarding e-government services from an information security perspective.

The link between the interview findings and the survey is fully clarified in the next chapter (findings chapter)**.** In general, the survey addressed the main information security related topics that were explored in the interviews. For instance, the researcher asked the citizens about government systems functionality, government websites design, the citizens' complaints centre, cybersecurity awareness and online culture. Moreover, a number of questions in the survey asked the them how cyber-secure they felt about sharing their data online for e-government services and how trustworthy they perceived government systems and websites to be. In general, the survey included direct questions regarding citizens' online trust and cybersecurity perceptions of e-government services (see **Annex E**: Survey of citizens). The dissemination of the online survey was completed in two different ways: first, by the researcher in the field, whereby random Jordanian citizens were chosen in various government departments (three service-based departments; Traffic & Licensing, Civil Services and Tax) waiting to be served in person.

The researcher achieved this by using an iPad connected to the Internet. In the first place, she gave the participants a brief overview of the study and confirmed to them that it was fully anonymised. This encouraged them to give consent and participate in the survey. Second, the citizens (respondents) were contacted electronically. That is, the researcher sent the link of the survey to personal friends and connections via email and mobile applications. Of the 200 respondents contacted via email, 101 responses were received, in addition to 102 responses by the researcher in the field. Overall, 203 respondents fully completed the survey, which indicates that the response rate electronically was 50.5% (101/200), and the completion rate of these responses was 66.9% (203/303).

As mentioned above, information about the purpose of the interviews and survey, approval to participate and a clause regarding the confidentiality and privacy of the responses were included with both methods. All the research ethics rules were complied with and all the appropriate formal forms were signed. The first step was to get approval from the MoICT in order to conduct the interviews with the staff on the e-government programme. In addition, it was ensured that no interviewees' names or any information about them would lead to them being identified. In addition, on the front of the survey explaining its purpose there was the reassurance that there was no way of tracing people's names through their responses.

3.3.2 Data Analysis

As aforementioned, the themes were drawn from the TFI model and the data related to these was first collected through the interviewing process, with the NVivo application being used for subsequent coding. This process also helped in identifying issues that needed further inquiry during follow up interviews, which, as can be seen from Table 5, occurred for four members of the information security department.

The researcher then imported all interview transcripts and appropriate documents into the NVivo application to start the coding so as to identify the main themes and sub-themes (see Table 7). As abovementioned, the categories covered all the answers to interviews questions for the technical, formal and informal levels. In addition, the data from the survey collected and analysed using the BOS online survey tool were put into the application. The data gathering and analysis procedure is shown in table 6 below.

Table 6: Data collection and analysis

Case study design	Primary data	Secondary data	Coding/Analysis

MoICT (Department of e-Government)	• Policy on IS security
	• Interviews
	  ○ Senior managers
	  ○ Staff
	  ○ Administrators
		• Books
		• Journals
		• Official documents and government publications
		• Official government websites
			NVivo (coding all themes and categories based on the collected data)

	Develop a small survey (on online trust and information security) based on the collected qualitative data (from a purposive sample of citizens at a number of government entities).	• Books • Journals • Official documents and government publications • Official government websites	The survey data are collected and analysed using the BOS online survey tool

Table 7: NVivo Coding

Parent Node	**Child Node**
Technical Level	Access Control
	Secure Government Network
	Technical Assessment
	Information Security Management
Formal Level	Business and Management
	Policies and Procedures
	Communications
	Governance and Risk Management
	Laws and Regulations
	Information Assets Management & Classifications
Informal Level	Training and Awareness
	Employee Vetting
	Security Culture
	Citizens' Security Awareness
	Citizens' (online)Trust
	Citizens' (online) Culture
Additional Nodes (Supplementary coding)	
NITC	Database and Network Control/ host
Knowledge Stations	Training Courses and Computer Services for Citizens

3.3.3 Validity and reliability of the methods of data collection and analysis

Various data collection methods, such as interviews and surveys, can be integrated in order to collect richer data, more ideas and present opportunities for participants to clarify their experiences and views. This is consistent with how this study has been conducted. After finishing the interviews, the survey took a place, which was aimed at seeing things from the other side, that of the citizen. As a result, the researcher had a comprehensive picture about the related issues from both the government and citizens' points of view together. According to Gregor (2002), inductive research works moving from specific observations towards generalisations and theories. This is also called the "bottom up" approach as it begins with specific observations and measures to detect patterns and formulate some empirical hypotheses that the researcher can explore, and finally, end up developing some general findings or theories. In contrast, deductive research works from the more general to the more specific and this is informally called a "top-down" approach. Researchers might begin with thinking up a theory about a specific topic and then narrow that down into more specific hypotheses in order to test it.

These two methods of research have a very different point of view when a researcher is conducting the research. Inductive reasoning, by its nature, is more open-ended and exploratory, especially at the beginning. Deductive reasoning is narrower in nature and is concerned with testing or confirming hypotheses.

In relation to this research, it is inductive research starting with clarifying or highlighting the strong connection between cybersecurity and online trust. Based on the literature review on information security, in e-government, in particular, cybersecurity could influence citizens' online trust and that leads to the need for a comprehensive cybersecurity approach, which has communicable security elements with citizens.

From the analysis of both methods and the empirical data clarified in Table 6, the researcher adopted a multi-dimensional information security model, which is the TFI model. Mind-mapping was chosen as an appropriate technique to visualise the TFI model, which is depicted above in Figure 8 (Mazza, 2009). The cloud-based software (Coggle) was used, which allowed the user to explore changes, modifications, additions and go back in time for the development of the mind-map using a timeline feature. As a result, there is an ability for an interactive

expansion of the TFI model. Visual data coding offers a flexible tool for a visual depiction of model clarification, this is as text-based data coding methods provide a standard clarification, even when using an advanced software application, such as NVivo (Spence, 2007).

In other words, visual coding was interactive and enhanced flexibility to organise the categories and subcategories (themes and subthemes) of model levels. The visualisation technique helps scholars doing their researches as it allows them to explore the underlying data easily through drawing physical representations of all of the factors involved as noted by Isenberg et al. (2011). The mind map also helps linking interviews results with survey results through putting the related subjects together (see **Annex G**: Mind Map).

3.4 Research Ethics

This section provides a discussion of the research ethics. There are general ethics for all types of research, as well as more specific guidelines, depending on the field. For example, for social research, such as management research, there are a number of ethical principles for researchers to follow, such as no harm must come to participants, there must be informed consent, anonymity, dignity, privacy, confidentiality, affiliation, honesty and transparency, and there must be no deception, misrepresentation or reciprocity (Miller et al., 2012).

In terms of e-government, it is a national issue and sensitive when it comes to information system security within an e-government programme. Hence, it is important to make the purpose of the interview clear; the interviewer should be concerned with research ethics and honest in clarifying the reasons for the interviews. In addition, explaining the nature of the study to the interviewees, as Manheim et al. (1991, p.156) suggest, "establishes credibility and improves the chances that respondents will agree to the interview".

3.5 Challenges to the Data Collection Process (Research Limitations)

The issues that needed to be addressed before the interviews took place included having to gain legal permission to access the ministry concerned, and to gain access to confidential information, and sometimes encountering employees who were not willing to answer questions. However, the researcher got the ministry approval to conduct the interviews eventually, but this caused a delay to the start of the data collection process. Regarding the few

employees who were not happy to be interviewed, this did mean that some valuable data held by individuals being omitted from the analysis.

The researcher also faced number of obstacles doing the survey in the field. For instance, the chosen government departments have different procedures and are managed or controlled by the military. As a result, formal permission was required to do the survey in each one of them separately. In addition to that, people have different reactions and responses. For example, some people did not want to talk at all, because they were very upset about the current situation of e-government services in general, and had had a bad experience with them or they had never used the e-services and had nothing to say. Moreover, the mentality of Jordanian people to accept a female researcher was another challenge. In general, as a researcher, I could not take any effective action to deal with those issues/limitations mentioned above.

Despite the unclear relationship between nonresponse and bias, it is still important to clarify the impact of nonresponse bias as affecting the accuracy of results derived from a survey and thus the ability of researchers to draw inferences and make a generalisation from the sample. As well as at the interview level, because of the negative effect that nonresponse can have on findings quality.

However, in this study the researcher is not missing data on any aspect that is strongly connected with cybersecurity and online trust, the researcher does not expect that the missing data affected the research findings, validity and quality, in a meaningful way. In their study, Boudreau et al. (2001) believe that IS researchers can put some efforts on improving or assuring the validity of the findings by reducing nonresponse bias. At the same time, there is no evidence that efforts to enhance response rates within the context of a survey will lead to minimising nonresponse bias on survey estimates (Curtin et al., 2000; Groves et al., 2006; Singer, 2006).

The research findings are presented and critically reflected upon in the next chapter.

4.0 Research Findings

4.1 Introduction

Jordan is one of those developing countries that have started implementing e-government initiatives after it had been proven to be useful in providing efficient and quality public services to citizens and organisations. As the Ministry of Information and Communications Technology (MOICT) indicates, the Jordanian e-government programme vision is "An essential and active participant in the economic and social development through the use of information and communication technology to enable easy access to government information and services for all users regardless of their geographic location or economic status or professional capacity" (MOICT, 2017b). The main goals underlying the vision are: ICT as a key enabler for sustainable economic growth, improving service delivery to individuals and businesses as well as raising the productivity and efficiency of the public sector.

However, obstacles and challenges invariably exist in e-government implementation. A number of studies on e-government have pointed out that cybersecurity remains one of the key concerns for many government organisations (Conklin, 2007; Mofleh & Wanous, 2008; AbuAli et al., 2010; Abu-Shanab, 2016). Cybersecurity is essential for e-government implementation and this involves hardware and software as well as networks and information systems, that are probably insecure by design and hence, come with their own vulnerabilities. Therefore, ensuring confidentiality, integrity and availability of information (the classic CIA model of security) is essential for successful e-government adoption. Moreover, the protection of e-government systems and networks from cyber-attacks has become especially crucial for government organisations in Jordan, as they have had to face several cybersecurity incidents originating from malware, hacking, denial of service and phishing (to name but a few).

According to Interviewee 1, “(Our) Government organisations faced several cybersecurity attacks, most of which related to viruses, either because of employees’ faults or system vulnerabilities. Information systems security is still not a priority for top management and needs to be considered more seriously by the government.”

Furthermore, cybersecurity is important as it plays a key role in building citizens online trust in the e-services provided by the e-government programme. This study involves examining the

information security approach within the Jordanian e-government programme, according to three aspects: the technical, the formal and the informal (using the TFI model). Then, there is investigation into whether these aspects of information security affect citizens' online trust in e-government services.

The chapter is divided into two main sections reflecting the two phases of research. First, the findings of the qualitative interview study are presented and critically reflected upon. This presentation is organised into subsections based on the NVivo themes and subthemes that emerged from the thematic analysis, as explained in chapter three. Second, how the interview study informed the design of the subsequent survey is explained in detail. Third, the results of the survey are presented.

4.2 Findings of the interview study

Thirty interviews were conducted with e-government staff and managers working for the e-government programme in various roles and departments. Their department, interviewee number, gender and length of service on the e-government programme are shown below in Table 8.

Table 8: Interviewee department, interviewee number, gender and length of service

Department	Interviewee number	Gender	Length of service on the e-government programme
Information Security Department	1	M	4 years
Technology Department	2	M	4 years
Operations Department	3	F	6 years
Change Management Department	4	F	3 years
Strategies and E-services Department	5	F	5 years
Programme Management and Projects department	6	M	4 years
Information Security Department	7	M	3 years
Information Security Department	8	F	2 years

Technology Department	9	M	3 years
Technology Department	10	M	4 years
Technology Department	11	M	3 years
Strategies and E-services Department	12	M	2 years
Programme Management and Projects Department	13	M	3 years
Technology Department	14	F	4 years
Operations Department	15	M	5 years
Programme Management and Projects department	16	F	6 years
Change Management Department	17	F	2 years
Information Security Department	18	M	7 years
Technology Department	19	M	2 years
Information Security Department at NITC	20	F	3 years
Information Security Department at NITC	21	M	5 years
Knowledge Stations Department at NITC	22	M	4 years
Knowledge Stations Department at NITC	23	M	3 years
Knowledge Stations Department at NITC	24	F	2 years
Secretary Department of MoICT	25	M	5 years
Information Technology Directorate	26	M	4 years

The interviews were conducted at MoICT in the e-government unit between March and July 2017 and varied in length from one to two hours. For this study, a number of government organisations (like MoICT) and government departments (like NITC) took a part in the interviews, as shown in the following table.

Table 9: Governmental organisations and departments involved in the interviews

Institutional stakeholder	Brief Description & Responsibility
Ministry of ICT	Is the government organisation responsible for developing policy and strategy in the areas of information technology, telecommunications and post in Jordan. The MoICT's key mission is to achieve the national goals and objectives within ICT. Basically, it is tasked with developing, and supporting ICT initiatives at a national level, such as the E-government Programme.
E-government Programme	Hosted by the Ministry of ICT, this is the department that is responsible for managing all e-government related initiatives and providing e-services on behalf of the public sector regarding all three areas (G2G, G2C, and G2B).
NITC (National Information Technology Centre)	The 'operations room' of the e-government programme, responsible for the technical domain of the Secure Government Network (SGN). NITC is responsible for utilising the national IT resources of the public sector in general, and offers many IT services to different organisations, including governmental ones and the private sector.
Knowledge Stations Programme	Is an initiative to ensure that every Jordanian has access to Information and Communications Technology, being significantly targeted at local communities and remote areas that would not be able to experience ICT easily, in order to prepare them for e-government initiatives. The National Information Technology Centre (NITC) has been mandated with the execution of the project.

Analysis of the interview data identified three main overarching themes technical, formal and informal, which reflects the design of the interview schedule. These main themes are then divided into subthemes.

4.2.1 Technical level findings

The first part of the interview schedule comprised questions relating to technical matters. The questions were about access control, the secure government network, technical assessment, and information security management.

4.2.1.1 Access control

Access control is a basic aspect of computer system security to ensure the authentication and authorisation of the users. The interviewees were asked to describe the mechanism of user authentication within e-government systems/websites, both for e-government departmental staff and for end users of the various services. Two interviewees (7, 8), employees within the information security department, noted that the e-government programme uses the role-based access control mechanism (RBAC) within the computer systems and networks. Interviewee 8 stated,

> "System administrators make roles according to the requirements of departmental tasks and give rights to these roles. Then, roles are assigned to the users. These not only determine users' resource access authority, but also determine its limitation."

Interviewee 10 highlighted that implementing RBAC as a mechanism for access control effectively reduces the complexity of managing the authority of users within e-government systems and makes it safer as well as more rational to use government information. This indicated that the access for all e-government systems and network is perceived to be under control and is being managed in an appropriate way. As the interviewee mentioned,

> "Only the authorised users can access particular information resources via networks and systems. Access control is the most essential security mechanism in the ministry and in the e-government programme, in particular. It is a basic measure to protect the resources of the information systems." (Interviewee 10)

A further important topic related to access control is employees' access rights to citizens' personal data and sensitive information, in general. Interviewee 2 stressed that employees are not given unnecessary system privileges or data access rights as this could lead to misuse or unauthorised action, the impact of which could be very serious. Instead, staff had "a reasonable level of system privileges and access rights required for their role. In addition, the granting of a highly elevated system access rights is carefully managed and controlled by systems administrators" (2). Interviewee 6 explained in response to the question on user access rights that there are three types of administrators within the e-government programme: administrators for software, administrators for information systems, and super administrators for access rights. The same interviewee added that government organisations need to determine what level of access employees need in terms the information, resources and databases in order to complete their tasks successfully.

In fact, the findings relating to access control theme show that they had discovered no violations up to that time. Access control is being managed through distributing the control tasks amongst several systems administrators. Administrators place users into roles, who get only the rights and permissions assigned to these. In the event of changing the role of an employee, the rights and permissions of the new role are assigned and previous access is entirely revoked. The process of access management involves username and password control in addition to the creation of groups of users with the same roles or defined access privileges.

However, regarding the Jordanian e-government programme, access management of e-government systems is not being reviewed regularly meaning that the entitlements for access have probably become outdated, with people having access who should no longer have permission. That is the access management is inadequate for revoking rights when the status of an employee changes due to transfer or termination, etc. In general, the administrators possess four basic functions, namely, identity verification, authentication, authorisation, and accountability, which work together to grant access to resources. In addition to rights, responsibilities were also discussed separately (mainly relating to password changing and authorised access). Interviewee 7 asserted that all users in government departments should adhere to the user password policy, which describes what all personnel in government departments should follow in terms of user identification and passwords.

> Compliance with the user password policy is very critical and a core issue to protect the public information and image of government organisations. Accordingly, cases of non-compliance are recorded in line with the discipline process. The purpose of this user password policy is to ensure that no unauthorised access to computers, networks, applications, or government-specific information occurs and to ensure that all user processes can be tracked and identified. (7)

According to interviewee 1, users should choose passwords according to the ISO 27001 criteria and immediately change them when prompted by the system. The password management system used by the IT department on the e-government programme requires a password change every 60 days. The system also maintains two previous passwords. Two reminders are sent to users to change their password, and if they do not, they cannot access the system. Interviewee 21 referred to the policy of acceptable use in the government departments and the expected utilisation of all information resources. This policy is aimed at facilitating understanding and awareness among users as well as ensuring compliance with security policies. The interviewee went on to explain,

> Greater commitment to the Acceptable Use Policy has been granted to protect the information and public image of IT management in government departments, but compliance needs to be recorded and handled in line with the discipline process. All users should be responsible for their use of information and the means of processing it. (21)

The administrators of the e-government systems are of the opinion that, once the Acceptable Use Policy is put in place, all government employees will fully comply and use the government network resources and computer systems only for work purposes, but this is not correct. This means that there remains the need for a continuous monitoring and enforcement mechanism, with clear consequences for violation, to be introduced into the usage policy. Regarding the Jordanian e-government programme, implementing an acceptable use policy without these two elements leaves government systems and network resources open to the on-going risk of unwelcome scenarios and legal responsibility issues.

Furthermore, the access management role, which is also known as identity management or rights management, is about making sure that the users in government organisations are able to use the systems that help them do their job, whilst only having as much access as they really need. This process works on the information security principle

of “least privilege” or “least authority”. In Jordanian e-government, it remains important for employees to follow this process to maintain a secure environment that not only avoids unauthorised access, but also prevents data breaches that can influence citizens’ trust in e-services. It is very important to set up an access control policy in order to improve the security of e-government systems and protect government information resources. At present, the role-based access control is an effective mechanism for controlling system information resources.

4.2.1.2 Secure government network

The Secure Government Network (SGN) is important for providing a communications network specifically for electronic government transactions. Since 2001, the e-government programme has completed the first phase of the SGN, which delivers connectivity, Internet and e-mail services to 18 government entities. In 2006, the programme has produced a National E-government Strategy and Roadmap (2006-2009) and since then, the four phases of the SGN that connect a total of 84 out of the targeted 120 government entities have been completed. Phase 4 of SGN involved connecting 10 more government entities from 2014 to 2016.

The e-government operations centre of the government of Jordan is hosted at the National Information Technology Centre (NITC). The purpose of this operations centre is to operate the SGN, the e-government portal and other shared services. It is connected to the NITC operations centre, with both being located in the same premises. The SGN is a large initiative linking all government entities into a secure governmental network as part of a recently developed connectivity strategy. Currently, the following services are provided through it: file sharing/exchange between government entities, e-mail services (electronic services that include email messaging solutions, the calendar, personal communications tools, etc.), inter-governmental data communications through the Government Services Bus (GSB) and government private cloud solutions.

Network security is at the core of (technical) cybersecurity. Accordingly, the researcher asked interviewees how secure they thought the government network (.gov.jo) is from security incidents and attacks; the effectiveness of countermeasures taken was also discussed. Interviewee 26 clarified that The SGN links government organisations to the e-government systems through the National Information Technology Centre (NITC) which is hosting the gate of the national electronic services and is also the host site for the e-government programme. Interviewee 1 further explained,

> The SGN facilitates the e-government programme to become a key connection point among government organisations in a secure and cost-effective manner. The National Information Technology Centre (NITC) is the operator of the Ministry of ICT and hosts the database and secure government network, which is an internal network for governmental organisations (operational network).

In this regard, interviewee 9 added that the communications of government organisations should be characterised by a high level of efficiency and reliability to provide very fast data transfers and should provide security in the data transfer process through the use of the latest techniques (web https, Secure FTP (either by FTPS or SFTP), Advanced Encryption Standard (AES) and Secure Sockets Layer [SSL]) so as to be able to connect through the SGN. However, and perhaps more interestingly, interviewee 7 mentioned that a number of ministries and government institutions are not hosted by MOICT. This indicates that there is a fragmentation of services as different ministries host their websites and applications in different ways and through different providers. This means also that they manage their systems and network security separately, which has led to various coordination problems. This was corroborated by interviewee 2, who said that a number of government organisations independently manage their servers, websites and information systems. These organisations (Ministry of Foreign Affairs, Traffic and Licences Department, Amman Municipality, Lands Department) have faced many more cyber-attacks than those hosted by the MoICT. In Jordan, the MoICT is responsible for e-government, with NITC as the operations centre, providing a number of cybersecurity services for the different government organisations. The services being offered by NITC include a cybersecurity audit service and a cybersecurity incident reporting service as well as incident management. The NITC also helps raise awareness in the field of information security and provides a digital certification service for government websites.

As the primary arm for utilising the national IT resources of the public sector and establishing and managing an integrated National Information System (NIS) at the national level, the NITC links together the various information systems and networks in the public sector, coordinating their efforts for secure data/information exchange and transfer. As a result, those government organisations that are not hosted by the NITC find themselves at increasing risk and in an unsecure environment. The lack of integration between computer systems, absence of a fully shared database and sufficient security requirements, increases the chances for cyber-attacks to occur like, DDS, malware, and etc. National networks and communication infrastructures

must be more secure, reliable and available. They must maintain the trust of government, private sector and individuals, and should be resilient to malicious attacks, arbitrary disruption and/or deception. In this context, interviewee 6 spoke of the role of the E-government Department,

> The E-government Department should be, by law, responsible for all agencies of government. For example, the Ministry of Foreign Affairs, Department of Car Traffic and License registered a domain on their own and hosted their own websites, which put them in an unsecure environment, where a number of cybersecurity incidents occurred. The MOICT centralises the e-services and automates the public services. The Secure Government Network is a general network, but there is a lack of trust between governmental institutions. The number of organisations linked to SGN reached 110 by 2017 meaning 30 are still not included. (6).

Based on the contribution of Interviewee 6, fragmentation of delivery of public services due to mismanagement, lack of cooperation and coordination, as well as lack of trust among government organisations, has led to poor cybersecurity and an increase in the number of cyber-attacks. This interviewee explained a number of ministries were failing to manage cybersecurity, because they did not accept a consistent approach across all government departments. Thus, good communication between different government agencies is a pre-requisite to minimise information security issues. Also, e-government programme managers must be kept aware of which providers are delivering which e-services, so they can appropriately advise the systems administrators on how to address cybersecurity.

Additionally, e-government managers must be able to keep track of how secure are data transfers via the SGN. In order to do so, all government organisations websites should be, by law, hosted by NITC. It is crucial to build in a way for securing all e-services by government organisations sharing their data and information via the SGN so they can continue to perform their jobs effectively. The existence of many shared services *between* government organisations, increases the need for a more consistent approach. For example, e-payment service for all government organisations are connected to different banks, as well as registration, authentication and authorisation services.

The current situation is such that each governmental organisation has developed its own information systems, and some have many information systems for different services. In most

cases the information systems are monolithic groups. No general structure exists that supports communication between front-office and back-office applications in a single organisation. Functionality, like authentication and authorisation, is exist in each of these information systems, but is not reused within one organisation, only between organisations.

Regarding data exchange via SGN, the interviewees were first asked about the Government Service Bus (GSB). This is a middle platform for sharing data on government transactions across departments, which offers frequent services, such as identity management and core data exchange, through the e-government national portal or through the SGN. As interviewee 10 suggested,

> The e-government programme should apply the technical solution and use latest integration software to enable the provision of e-services from different governmental agencies. Agencies, then, will be able to use a shared infrastructure for integration, sharing of data and the use of centralised common services through the GSB. (10)

When discussing high level security applications and technologies used to secure the SGN, such as Public Key Infrastructure (PKI), firewalls, digital signature, and advanced encryption techniques, three interviewees (2, 9, 10), each employed in the technology department, noted that isolating internal users is achieved using a firewall and other security applications. Moreover, PKI has an important role as a security solution used to cover everything for user authentication that consists of software, hardware, standards and policies to manage the creation, administration as well as distribution of keys and digital certificates. Interviewee 1 stated that without PKI, sensitive information could still be encrypted to ensure confidentiality and exchanged as well, but identity assurance of the other party (authentication) was missing. Any form of sensitive data exchanged via the Internet among government organisations or the e-government programme relies on PKI for security. Interviewee 26 also discussed the role of PKI,

> PKI was a very important step in programme development as it consists of a set of enabling technologies and supporting people and processes that will allow the government to perform certain functions and services securely. PKI is part of the Identity Management System, being a strong authentication preferred way to manage keys and authentication certificates to securely exchange data within the SGN. In addition to that, there is an intrusion prevention system (IPS) and firewall for network security as threat prevention technology that

> monitors network traffic flows to detect and prevent vulnerability exploitation.

Interviewee 2 clarified that the firewall logs need to be reviewed and monitored on a regular basis in order to ensure that the firewalls are operating in a secure manner and that the logs are free of any kind of unauthorised activity. This interviewee added,

> … different systems providing firewall functionality have to be managed according to the information security policy and associated rules. These devices need to be upgraded or replaced with another device to fulfil the requirements of information security policy within the e-government programme.

Two further technologies that were mentioned by interviewees were Intrusion Detection Systems (IDSs), which are either network or host based and the Intruder Prevention System (IPS). The latter has been deployed within e-government systems since 2012. According to interviewee 19, the system will ultimately be installed on all relevant network parts in order to send automated notifications to the system administrator when suspicious activity occurs, so that preventative or corrective action can be taken.

Within the e-government programme, the PKI delivers a way to prove online identity and provide security mechanisms for information exchange over networks. As it is critical when conducting online transactions to prove that data have not been tampered with, it is important for government organisations to take measures that will help protect their PKI. The MoICT deploys a PKI to support critical management processes and functions, such as strong authentication of users among government agencies to protect access to sensitive data. Thus, security of the systems and processes that compose a PKI is an important consideration in the design and deployment stage. It is important to treat PKI systems as critical and to deploy strong technical controls to help protect them from unauthorised access.

Furthermore, on-going monitoring of the infrastructure and supporting processes is required as a key component of any PKI security plan. The governmental organisations need to collect the right information, review the processes in place and have appropriate alert mechanisms so that if an issue occurs, it can be properly investigated. Unfortunately, there is no standard formula for what to do when a PKI is compromised or presumed so. Depending on the type and severity of the compromise, there are several response options, with each having its own positive and

negative attributes. If a PKI is properly implemented, it becomes a foundational component for building effective security controls for information systems. It can play a critical role in the protection of sensitive data and is an enabling technology that helps promote the security of e-services. Of course, while no IT infrastructure is immune from attack, implementing appropriate policies, procedures, and technical controls can limit the extent of a compromise and help keep critical systems, such as a PKI, protected. The next section discusses the technical assessment of the IT infrastructure of the e-government programme in more detail.

4.2.1.3 Findings from the technical domain of the e-government programme assessment

The technical assessment focuses on ICT infrastructure and technology aspects, being an essential part or subtheme of the technical level. First, the interviewees were asked about the process of systems maintenance and development. Those from the information security and technology departments, mentioned the object-oriented standards several times, which they are using within the e-government programme systems. The object-oriented approach is considered to be the best practice for software development and functions.

According to interviewee 9, the technology department is responsible, in part, for systems maintenance and development. However, at each government organisation, there is a different IT unit and they are tasked with carrying out any maintenance when required. This means that there are no regular procedures or a sustainable plan for systems maintenance and development. Of the eight interviewees working in the technology department at the e-government programme, six made reference to the need for security controls and requirements being introduced at an early stage of system development, as this is considered more effective and cheaper than applying those controls retrospectively. Typical of the contributions, interviewee 4 stated,

> The security team should meet with the systems management and development team to ensure that all security requirements are covered, conduct risk assessment process and identify the vulnerabilities at a very early stage as well as supporting the development of new services and infrastructure. The security analysis of new systems should take into account any risks to assets that may be introduced by the new system as well as risks associated with the integration of the systems with the existing infrastructure and services. (4)

The findings elicited the need for greater action to protect citizens and a fundamental shift in how cyber risks are managed.

There was widespread agreement among employees that the process of updating systems and applications was very slow, with the NVivo-based analysis showing that 20 interviewees made some mention of it. Other related comments pertained to the lack of a regular schedule for system updates, indicating that the latest and most effective technologies are still not in use at all levels of the ICT infrastructure. For example, the ID smart card is not being used yet by citizens as the national the infrastructure is not completely in place. An Automated Fingerprint Identification System (AFIS) is necessary for this project to ensure that the principle of a single person being identified is addressed.

The government of Jordan has prepared 25 centres to issue smart ID cards and complete the secure ID solution in the Kingdom. The citizen's details are both laser-engraved in the card and stored in the microprocessor to enable officials to verify the identity of the holder. The new electronic identity card will add security features and offers the Jordanian government the ability to add new applications after issuance for developing new secure e-government services. Early in 2018, the Civil Status and Passports Department (CSPD) declared that only 3 million citizens have obtained the new national ID card so far, which will offer quality and consistency of the information gathered with few errors. Basically, there is a critical need to simplify the processes and reduce the number of means of identification, thereby increasing Internet security. When this system of e-ID is rolled out, it could help streamline a set of processes that require multiple ID into one general procedure.

The ID cards project could offer some basic interest for public and business benefits. On the other hand, it identifies a number of other areas of concern with the government’s plans. For example, evidence from other countries identity cards projects shows that the systems perform in a better way when established for clear and focused purposes. A shared platform is an essential requirement, not only general connections through the technical infrastructure. The smart ID cards can address only a small amount of the estimated cost of possible identity fraud attacks. In terms of technology, no step has been taken at any government organisation or department and no scheme on this project have considered technological and operational obstacles that are likely to be raised in a large-scale national system. The use of biometrics raises particular concerns because this technology has never been used in Jordan at the national

level. Furthermore, the current status of related laws and regulations is unorganised and may have some conflict. The requirements for various civil services should be determined or specified. From a cybersecurity perspective, as the national information technology centre is creating a national portal which is a very large database for citizens registration in one place that could be a serious risk in case of any security attack or breaches like unauthorised access. Online culture plays a key role in the success of smart ID cards project as well. The identity system should be accepted by citizens and not raises security concerns. It is very critical to realise the public value from the successful use of ID cards by citizens in a wide range of services. To ensure compliance with the use of the ID cards, this means that even small departments are likely need to have smartcard readers and other requirements which will add to the administrative load and fees (LSEIdentityProject, 2007).

In the context of interoperability of systems within the e-government programme, there are many systems working together. Everyone has a specific task and is different with distinct characteristics. For example, transaction processing systems, management information systems, expert systems and neural networks. Interviewees were asked how they perceived the level of interoperability of systems and updates. Interviewee 2 gave the most thorough overview of interoperability issues - organisational, technological and conceptual. Regarding which, this interviewee pointed to technological barriers, such as the incompatibility of information technologies or organisational barriers, relating to authority, tasks allocation and organisational structure. Whereas conceptual barriers basically involve semantic differences of information to be exchanged, these barriers together can impact negatively on the system's operation or even stop it from functioning. The interviewee commented,

> E-government can have many advantages from applying enterprise architecture as it is capable of interacting among government organisations. Enterprise architecture helps the government to manage and process information in an effective manner, as a key asset. At present, the e-government programme needs to provide an environment to keep distributed information together and a shared information station for all organisations and to avoid duplication. (2)

As previously explained, e-government in Jordan involves four types of interactions between government and stakeholders, which are: Government-to-Citizen (G2C), Government-to-Business (G2B), Government-to-Government (G2G) and Government-to-Employee (G2E). To deliver e-services to citizens, business and to the government itself, the government needs to

focus on improvements in various areas, such as IT infrastructure, common services and one stop service delivery to enhance to it in an effective and secure way. IS interoperability of e-government programme provides benefits when interaction between entities through technical, semantic, and organisational interoperability is implemented with standard KPIs focused on one-service delivery.

Strategies and work processes need to be in line, whilst at the same time common standards and knowledge should be shared for effective e-government interoperability. All governmental entities should determine their current and expected levels of e-government interoperability and clarify their objectives and initiatives for reaching the required status. In order to gain the advantages of e-government services, IS interoperability must be developed systematically. To accomplish the aim of IS interoperability of e-government in Jordan, it is necessary to work more on performance indicators, such as the availability of service, flexibility and decreasing response times. This will improve ICT quality, thereby ensuring the effectiveness and security of the services of the e-government programme. One of the most important elements of the technical assessment concerns information security management, the findings regarding which are presented next.

4.2.1.4 Information security management

As controls need to be available within applications and business processes to ensure that the information contained within the systems is accurate, up to date and available in the correct format, the researcher was interested in finding out about the mechanisms/ applications in place to protect information systems from security incidents or attacks as well as how effective they are perceived to be.

Interviewee 11 highlighted the need for government organisations to ensure the software of e-services consistently exhibits its required desirable properties, especially when it comes under attack. This should minimise the numerous flaws in software that are often located and exploited by attackers to compromise the software's security.

> It's really important that a certification and accreditation programme is introduced covering all of the most crucial software in use across government departments and agencies, especially where critical national infrastructure is involved. All governmental organisations

must closely adhere to rules, standard and best practice frameworks. (11)

Information security requires a governance structure that guarantees a coherent direction, with the ability to drive the implementation of the security policy within the organisation and to ensure constant monitoring and improvement of the overall security system. Hence, the interviewees were also asked to describe the information security management system and from their own perspectives, suggest whether it could be improved. The interviewees working in the E-government Department were generally very consistent in arguing for a better information security management system for government organisations. Security information management (SIM) is the practice of collecting, monitoring and analysing security-related data from computer logs, while the security information management system (SIMS) automates that practice. According to interviewee 3, security information management is sometimes called security event management (SEM) or security information and event management (SIEM), which involves three main steps: collecting data from the device, analysis and finding any suspect (intrusion detection system) activity.

One prominent point, which both technology and information security interviewees (8, 10, 11, 19) raised, is that although SIM products can automate many tasks around security information gathering and processing, but they cannot operate effectively without significant effort and investment. However, they noted that in this context, Jordan is a poor country with limited resources; the budget of the MOICT, and the e-government programme, in particular, cannot afford all the required technologies and updated ICTs. Moreover, as interviewee 7 stated, security information and event management (SIEM) products are only as good as the policies and processes they support. In addition, this depends on the analyst resources the organisation can provide, and this was reported as missing to some degree, in particular, in the context of the storage of the most sensitive data (e.g. e-ID, health records, social security number or status). Choosing a suitable system regarding the management of citizen sensitive information can deliver important improvements in information security. For instance, when the citizens are not forced to provide the same part of information multiple times since the data are shared and reused among different administrations. This allows for a decrease in the administrative burden for this particular citizen.

As interviewee 19 argued,

> Systems developed locally really shouldn't be used for our most sensitive or critical data and we really need to ensure that storage associated with these locally developed systems is linked to centrally control backed up systems so that they can be recovered in the event of outages or other problems (19).

In fact, the perception from interviewees of the information security and technology departments seemed to be that most of these steps are not yet applied, thus being mostly absent from the e-government programme. Management of large amounts of sensitive and critical data is associated with multiple risks. For example, the possession of information of this scale (i.e. for the entire population that uses e-services) makes it possible for unauthorised public staff to verify critical information, like checking the name associated to a plate number and using this to track the address of one individual. This explains why a centralised information management model raises cybersecurity concerns. To manage this large number of information systems of government organisations, refined and comprehensive (combining people, process, and technology) security strategies and solutions are required, thereby enhancing cybersecurity in e-government infrastructure. On the other hand, decentralisation offers the possibility to make this cross-checking more challenging for unauthorised users (provided that some precautions are taken), thus raising different concerns.

Information systems are targets for cyber-attacks for different reasons. Based on the 2017 annual report of the ministry of ICT (MOICT) cyber-attacks increase the possibility of data revelation, data manipulation, data loss, and systems devastation. Hence, the researcher was interested in the perceptions held by interviewees concerning the way security incidents are currently being dealt with. They were asked first whether they had experienced a security incident, and if so, how it was handled. Unsurprisingly, the interviewees most familiar with cyber-attacks and related security incidents came from the information security department. Five such interviewees (1, 7, 8, 21 and 26) contributed their experiences and opinions. It was clarified that it was the security officer's role to respond when an incident was reported to the e-government programme by one of the government organisations. Furthermore, the absence of automated incident response processes was mentioned (7), together with the lack of a systematic incident reporting process (8). It was also pointed out that there was no official incidents response team (21). The findings show that there is a need to create a Computer Emergency Response Team to handle coordinated analysis, dissemination of cyber threat warning information and to respond to cyber incidents.

The Jordanian e-government programme is not developing and deploying the appropriate capabilities to respond to cyber-attacks. It needs to have well-defined and tested incident management processes, capabilities and mitigation activities. This is in order to minimise and contain the impacts of cyber security incidents. Speaking of cyber-attacks, in general, interviewee 1 explained,

> Cyber-attacks occur due to the low level of concern about cybersecurity. In other words, most government agencies still do not take cybersecurity or information security generally as a high priority issue. The incident response and the way they handle (the incidents), depends on the attack type, but mainly the steps are: formatting, server updating, back up, recovering or prevention procedures. (1)

Interviewee 21 stated that around 70% of attacks are internal. It is of course a shocking finding that 70% of incidents come from individual mistakes by government employees across all the different government entities. Internal threats to government organisations are as a result of employee action or failure of an organisational process. Non-malicious insider threats are an expected consequence of lack of security training and awareness. These threats mainly involve the unauthorised or accidental modification of software. For instance, corruption of data caused by a coding error, operator or user error.

In contrast, external threats occur from outside the government organisations, caused by other individuals or organisations that do not have authorised access to the government computer systems or network. Such incidents occur through connected networks (wired and wireless), physical intrusion, or a partner network. While in most countries, the Foreign Intelligence Services (FIS) are considered to be the greatest threat to all government information assets through direct external attacks on the information systems, this shows that the most likely threat to government organisations in Jordan is Hacktivists that use technical tools and illegal means to get unauthorised access to information systems or networks for various reasons, such as political, social, ideological, or religious purposes.

The human factor is the biggest cybersecurity vulnerability, where information security breaches can be the result of a single employee carelessness or the absence of cybersecurity awareness and this will be clarified in the following part below.

Four types of security attacks were mentioned by the interviewees. The first type was a rootkit virus, which was described to the researcher as one that allows an attacker to maintain control of a computer, while remaining undetected. Once in place, the attacker can run executable files on the host computer and alter its configuration (1). Interviewee 19 described the rootkit as a hacker tool that can evade even regular virus scanning, as it appears as part of the operating system. To protect against this kind of virus, the system and especially the operating system and applications must be kept patched for known vulnerabilities; so updatability is key. Interviewee 1 mentioned that following one rootkit attack, the entire server had to be replaced as reformatting it would not have been sufficient. He also said that the cause of the problem had been a member of staff accessing a non-secure website.

From the interviews, it became evident that detection solutions are still inefficient and tools of evidence-collection are inadequate. Detecting and mitigating rootkit threats depends on how technologically advanced they. That is, it is very difficult to detect a well-made rootkit, so it is essential to assess the damage and mitigate the threat elsewhere in the network once this type of attack has occurred. The best way to deal with this attack is to use more than one detection solution and conduct reengineer and collect details about captured malware. The Jordanian e-government programme should be able to assess systems remotely, capture programs and applications to handle such attacks. Despite this, rootkit detection is still a human problem, so the real challenge is the scaling of these attacks and how to make government employees more qualified and aware.

A second type of common cyber-attack sustained in the MoICT was Denial of Service (DoS), with interviewees stating that it had occurred at various government agencies with very high frequency. According to interviewee 2, this type of attack is aimed at preventing authorised users from accessing and reaching the e-government service that was affected. This could occur by targeting computers and networks of the websites and may allow the attacker to prevent the user from accessing email, online accounts and other services that depend on the affected computer.

A related (third) type of attack mentioned is the Distributed Denial of Service (DDoS). Interviewee 21 stated that at the NITC, DDoS attacks had occurred several times. He explained that in this type of attack, a computer is taken over by an attacker (it becomes a zombie). The

hacker sends many requests from all the zombies, which causes overload, thus bringing the system down.

There are three main categories targeted in these attacks: networks, systems, and applications. Networks and systems can be considered as one group, because the former form the latter and the targeted information is mostly embedded within one or the other. These DoS attacks typically attempt to consume all the available capacity on network links, thus leading to the network hardware or software failing due to overload. In contrast, applications are handled differently, whereby one or more are kept busy dealing with junk requests, and so, in the end it becomes unable to treat legitimate requests for service. For instance, when trying to access an online application, the DoS or DDoS attack may have already filled the browser application, making it useless and unable to connect to the Internet. These DoS attacks typically attempt to consume the computer resources of the service by exercising compute-expensive functionality, or by generating many more application sessions than the service has been designed to cope with.

In fact, it is difficult to pre-determine DoS attacks and there are not many effective ways to prevent them. Given its regular suffering from such attacks, this indicates that Jordanian government needs to take into consideration the following points, which could help in reducing. First, the installation of an antivirus program and firewalls in the SGN network to restrict the usage load to authenticated users only. Second, the network administrator needs to take a look at network configurations and harden the firewall policies so as to block out unauthenticated users from utilising the server's resources. Lastly, third party services can offer guidance and protection against DoS attacks, which, whilst being costly, can be very effective.

A fourth type of attack mentioned was the Tesla virus. Interviewee 1 recounted how the Consumer Foundation had been attacked with this virus, again as a result of a user downloading a file from a non-secure website. As is typical with this kind of ransomware, the hacker had sent a message requesting money in return for a decryption code. The interviewee stated that in this case he had confined the attack inside the internal information system, formatted the systems and used the backup (which is hosted by the NITC).

There are number of Ransomware Detection Techniques that should be followed by government organisations in Jordan, such as creating hidden folders for sensitive files that

employees should not access, known as a Honeypot. It provides simple detection, for if anyone accesses those files this will be considered as a threat and an alert raised. In case the hackers that write the ransomware did not encrypt the hidden folders, this detection method will be useless. Another simple detection method is using filenames. Many times ransom notes with specific file names will be saved to the folder during an attack and encrypted with a specific file extension (like Resume.docx.encrypted). It is essential to monitor systems and networks to detect such cases, but this will not catch new forms of ransomware that could occur later on.

To summarise, the main points concerning cybersecurity: there is no comprehensive incident handling team in each government organisation. The Information Security Department in the e-government programme at the MOICT is responsible for incident handling. The interviewees (1, 7, 8, and 21) indicated that government organisations ask them for help as they do not have the resources and processes to respond to cybersecurity incidents. When asked about the security incidents they had suffered during the past few years and the most prevalent security risks to their organisations, these interviewees considered hacking attempts, malware and user Internet downloading to be the most prevalent. Unfortunately, for most Jordanian government departments security comes third or fourth place after applications, websites, and production or administrative issues.

The Jordanian government needs a more advanced and secure e-government network to protect data from increasing cybersecurity threats and risks, like the examples mentioned above by the interviewees. Security threats involve unauthorised access to resources, data intercepts and modifications. While security risks could be a virus, and/or a leak of key information, which regularly occur in networks most of time. This makes the controlling of information leakage a very critical aspect in the government's network design. Furthermore, a security breach may be aimed at restricting the availability of information to the citizen or to other stakeholders (business), and this is where many e-government projects in developing countries, like Jordan, fail.

As a result, finding the security vulnerabilities in the SGN layers and all information resources, technical or non-technical, is more important as a first step than providing security in the e-government programme. Moreover, the Jordanian e-government programme needs a standard mechanism for detecting vulnerabilities, which in some cases are known, whilst in others they are not.

4.2.2 Formal level findings

This section presents the findings relating to the formal level, which include the perceptions of the relationships with third parties, the way tasks are allocated, policy-issues, the perceived levels of cooperation and the efficacy of security management. While these findings raised issues and areas for improvement, the section also highlights perceptions on a range of positive initiatives and on-going projects.

4.2.2.1 Business and management

Interviewees were asked to describe the way roles were organised and the relationships with third party providers. Interviewee 5 clarified that the government of Jordan organises its National Information Assurance & Cyber Security Strategy (NIACSS) across nine major national interdependent priorities, each requiring collaboration across government, and with international partners, the private sector, and/or the citizenry. These nine aspects identified are the: 1) Risk Management Programme; 2) National Computer Emergency Response Team (JOCERT) 3); Security Awareness and Capacity Building Programme; 4) National Information Security Standards and Policies; 5) Legal and Regulatory Regime; 6) National Encryption System; 7) International Information Security Cooperation Programme; 8) Securing National Information Systems/Networks; and 9) the Critical National Infrastructure Protection (CNIP) Programme.

Interviewee 3 talked in general terms about the role of the Ministry of ICT, stating,

> … the Ministry of ICT is taking more of a consultancy role. The ministry makes a request for proposal (RFP) and starts looking for a bidder (IT company) to develop websites or systems and guides the ministries. The RFP includes a component for each department (security, quality, management, business, technology etc.) and covers all standards. (3)

Also, on the subject of third party bidders, interviewee 12 highlighted three criteria which any systems design bidder must meet: Firstly, they are following the ISO 27001 standard, otherwise they're excluded, whilst secondly, they must assign a security specialist to conduct security testing. Thirdly, their bid must be accompanied by a two-year maintenance and development agreement. The emphasis on security in the RFP process is clarified in the information security component, which is very critical and the winning bidder is required to perform a number of

activities to ensure system security. First, there must be the development of a detailed security policy and related procedures involving handling the proposed solution and security controls, like the backup policy and procedures, auditing policy, etc., in compliance with the ISO 27001 standard. Second, it has to assess, implement, test and deploy information security controls and measures. Third, it must prepare and test the business continuity plan, disaster recovery plan and the incident handling policy before launching an e-service in cooperation with the operational team at e-government programme. Fourth, it has to design and build secure connections and communication channels, which will ensure that applications used by a portal website are protected against related threats. Both the e-government team and the winning bidder, should agree with an independent and qualified third party to test the security solution against known vulnerabilities. At the end, it is important that the final solution includes comprehensive audit and log management as well as reporting tools for all transactions, with the system access controls protecting the different types of resources.

The same interviewee (12) explained the responsibilities of the Project Management Office (PMO). These include determining whether the service in question should be automated, having regard for the importance, priority and potential benefits this would bring. However, they have decided not to automate number of services and make them part of the e-government programme by law owing to security concerns, such as renewing passports and national cards. They are also tasked with reengineering the business process, including simplification of procedures and then returning the outcome to the originating department. To check the customer journey and ease of use, the PMO involves the change management unit for an evaluation. Finally, before the new service goes live, it is the PMO's task to liaise with the Central Bank to have the new service connected to the e-payment channel. However, as mentioned by interviewee 12, "We mainly need to work on e-services development or reengineering, because of technical errors or faults and also, cybersecurity training and awareness. The e-government services centre (national portal) still covers only 5% of government institutions."

The Jordanian e-government programme needs to achieve the objectives mentioned in the MoICT annual report of 2017. For instance, this includes reengineering 201 government services, upgrading the SGN and national portal, connecting more government organisations.

Interviewee 13 mentioned that the programme management and project unit has to compare the system architecture document with the RFP to make sure they match. That is, the operational activities, the design, the development, and testing have to be carried out before being accepted. Additionally, various problems need to be tackled, like in some cases the government organisation not having sufficient technical infrastructure to be able to automate its related service. For example, the Department of Residence and Borders is not ready to automate the service of renewing the visas of non-Jordanians as business, medical, or education ones. Also, the Ministry of Energy has yet to be connected with other stakeholders regarding the provision of shared services, because it does do not have the required infrastructure and information systems to do this.

Interviewee 14 noted that the current e-services are not at the required level of quality. The decision makers priority is to launch a large number of e-services and then, only after that, care about quality and information security. As in the case of the e-service for issuing a non-criminal certificate, the quality manager reported that several problems were weakening the quality of the service provided and its security. However, the top management decided to launch this service because it was committed to doing so. Later on, due to the large number of faults and errors in several e-services systems and networks, the Minister of ICT has asked for a re-evaluation of all e-services; a process that came to be known as the 'Task Force'.

4.2.2.2 Task allocation and cooperation

E-government programme tasks were allocated to the various departments and units, which also explained how cooperation among them should take place. The interviewees were asked how the duties and responsibilities are separated or distributed to ensure that administrators control all systems and prevent any attempts at unauthorised access (internally and externally).

Interviewee 1 said that, in general, the information security manager had overall responsibility for all day-to-day operational aspects of information security. Further delegation of responsibility for specific security issues could be carried out within government organisations as required. Information systems security is also a basic responsibility of all employees or staff of e-government programme, which should be regularly communicated and reinforced through on-going security awareness and training courses.

Interviewee 16 explained the procedures for automating an e-service step by step,

> The management unit will start by scoping and determining which services have to be automated depending on their importance, need and benefits. A reengineering process is adopted to study the service step-by-step before it is automated. Then comes the business requirement gathering phase, meeting all related governmental organisations and putting forward the future picture of this service electronically. The technology department's job comes after that to check the technical capability and design the technical architecture. In the last phase, a request for the proposal is created and includes all the components, one for each department (e-service implementation, project manager, security, quality, infrastructure, training and operations support). Each department checks its component in the RFP document to see if it matches with their checklist and after that comes the testing phase before the final acceptance. (16)

From what is mentioned above by the interviewee, it becomes clearer that when automating a new service, cybersecurity is considered as an after-thought, with security requirements not being properly focused upon until at a relatively late phase. In addition, the appropriate government organisations should be engaged when defining security requirements. Without sufficient cooperation between stakeholders, gaining insights into potential vulnerabilities and threats could be very difficult.

Interviewee 17 mentioned that the e-government programme had helped to facilitate appropriate cross-organisational information governance, as well as good practice and information sharing. This included maintaining information security policies, defining and reviewing roles and responsibilities, monitoring threats to security, reviewing and managing security incidents, assessing major initiatives to improve information security and sharing good practice. Indeed, the role of the e-government programme as a bridge of cybersecurity is important in the context of a national project, which aims to provide services from different governmental departments to all stakeholders (government, citizens and business). The core issue for achieving this mission is having a comprehensive plan of organisational cooperation, as there are shared and vertical services among government organisations.

Many (15) interviewees expressed mostly negative sentiments about the level of cooperation and communication among government agencies. A representative comment came from interviewee 14, who stated that "Audit reports are not delivered to the (e-government's)

information security unit from government organisations and ministries. Security reports should be sent regularly every six months, but government agencies do not comply with this." Interviewee 26 also clarified that e-government managers were really facing problems in communicating with other government organisations. Generally, the government agencies did not comply with e-government programme instructions, which included preventing their employees from accessing unsecure websites and applications, carrying out regular cybersecurity audit and sending reports to MoICT. Added to this, they did not provide timely responses for the e-government programme when reporting a security weakness in an e-service. Furthermore, when the NITC sent out information on security awareness training, there was no cooperation or serious reaction from different government agencies. Unfortunately, without the authority to conduct security awareness and training courses for all government employees, or at least, to ensure that each government department is offering such courses to their staff, the e-government programme cannot have a clear overview of employee cyber-awareness. In addition, interviewee 14 remarked that decision makers are mostly concerned about launching the e-services and it is only after their launch that they think about their security and the quality of the e-service. Interviewee 3 said that his department had to deal with complaints about e-services and try to solve any problems, whilst also having to respond to the citizens that have issues at hand. Most complaints concern system downtime, delays etc., in particular, when the citizens make a registration, coding and technical errors frequently occur. These different errors affect citizens' trust in e-services, by negatively impacting on their perceptions of cybersecurity within e-government systems and on websites. According to interviewee 15,

> 25% of complaints are informal and related to human factors or faults, and 75% of complaints are related to technical and formal issues, such as system errors, functionality or procedures. Following complaints and responding to them as fast as possible will improve citizens' trust in government, which will lead to citizens' online trust in government e-services.

In terms of cyberwarfare, cyber-attacks from other countries, interviewee 26 stated that national information security cannot be ensured or reinforced to a required level without international cooperation with other governments, research centres, universities, and the private sector. He continued by explaining that cyber-attacks are a significant threat to the national security of Jordan, so a high priority has been placed on countering this threat in order to defend the national infrastructure.

4.2.2.3 E-services security management

The issues relating to e-services security management explored included information security strategy and policy. In doing so, the aim was to gain some understanding of how effective the cybersecurity strategy, initiated in 2011, has been so far. Interviewee 26 noted that preventing security breaches to secure national systems was not enough, for there also needed to be a focus on detection and response as well. Furthermore, he emphasised that there are three pillars to cyber-security: people, technology and operations. He commented,

> Because the National Information Assurance and Cyber Security Strategy (NIACSS) has been developed by the government, it covers all information domains in Jordan. However, its successful implementation is not just down to the government, for it also involves international partners and the private sector. In the case of the private sector, it is really important that their policies should comply with and compliment those of the NIACSS. (26)

On the subject of what future steps the e-government programme creators are planning to take, interviewee 16 commented that the Jordanian government works with the private sector in establishing a programme covering cyber security and information assurance for the Critical National Infrastructure (CNI). The CNI, she continued, includes information assets and systems crucial to the operation of ISPs, health providers, telecoms, and the finance sector. Without such security, services critical to the daily lives of citizens would be at greater risk. The "CNI programme is needed to secure systems of critical value to Jordan. E-government should cooperate and work closely with those parties who manage and operate CNI in order to regulate and provide security guidance for all domains" (16).

The interviews revealed certain challenges and obstacles to information security in response to the questions on the technical, formal, informal challenges that the interviewees faced in their departments and how they responded to such challenges. Interviewees 7 and 8, information security employees, pointed out that that there is no regular or real updating of the cybersecurity policy. In addition, they also indicated that in most organisations (e.g. Ministry of foreign affairs, Ministry of Justice, Ministry of Interior), there is lack of commitment and compliance with the plan established for effective information security implementation, policy and strategy. Moreover, the e-government programme has no constitutional power to force government organisations to follow information security laws and regulations or to cooperate.

Thus, it can be seen that the problems encountered are not only those relating to technical and organisational issues, but they also involve legal and constitutional barriers. This point is especially relevant in cybersecurity implementation and compliance, where ministries in Jordan enjoy a large degree of autonomy, as guaranteed by the law. However, as the e-government programme spreads to fulfil the vision of the e-strategy, it becomes reasonable to expect that there will be constitutional reform regarding government systems and cybersecurity. In this context, interviewees brought to light a remarkable suggestion: that the e-government programme should become an independent entity placed under the direct authority of the prime minister, so as to have the maximum level of authority. In this case, the e-government unit would be able to enforce a national cybersecurity plan and follow up on cybersecurity compliance by all governmental organisations.

Also, according to interviewee 2, the key challenges that the e-government programme is facing are the culture and mentality of Jordanian people. Most citizens do not have online banking and do not even trust the security of e-payment systems. In addition, there were processes based on old instructions and procedures, which do not match the development or new technologies. Besides that, the human factor is playing a key role as well, because of the lack of cybersecurity awareness and training means that employees do not have the required skills. The same interviewee suggested a number of steps to tackle the issues,

> We need to consider end point security, including the proper use of anti-virus software on staff computers. Also, we need to bar the use of flash memory drives to prevent data loss. The awareness of staff to security needs to be raised, for example, by making videos available to both staff and citizens. (2)

Interviewee 14 highlighted inflexibility and non-compliance as two major concerns,

> The errors are in administration, procedures, and decisions, which are not flexible and complicated - these are the main obstacles in e-services progress. Moreover, there is no compliance by government agencies with the policy and procedures of the MOICT. (14)

Interviewee 2 also suggested that the decision-making process needs to be logical and organised, whilst media and marketing have to be more active. Also, the ministry should follow up with statistical reports of e-services usage from all governmental initiation points and not just use the UN statistics of the annual report. The critical need to restructure the e-government

programme was also emphasised and the need to put an effective strategy in place was discussed, as well as the necessary infrastructure for e-services to be created.

Interviewee 1 also contributed a range of points regarding cybersecurity. He first mentioned that the security policy needed continuous updating and a compliance officer. Citizens trust government IT capabilities, but do not trust government itself, he added and they believe that systems are not all secure. Furthermore, interviewee 1, attributed the lack of cooperation of government employees to a fear of being replaced by technology and losing their jobs (when automation of services in their organisations takes place). In general, change is resisted, he said. He also advocated the use of staff assessment, for example each employee would have to take a test and failing it, should have consequences for their future employment.

Conversely to other interviewees, interviewee 8 suggested that objectives of cybersecurity should not be at a governmental level or ministry level, but a nation-wide level with a national security plan. Thus, he deemed it as very important to give authority to the ministry (MoICT) to mandate government agencies to follow the instructions and regulations regarding information security. The MOICT, in this case, could also make awards to the ministry or organisation with the best security level. Moreover, information security should be one of the standards for organisation evaluation.

Agreeing with the same point raised by the information security department manager at the MOICT, that government employees are afraid of the process automation as it may lead to their jobs being lost, Interviewee 21 declared that the core problems occur, because of the human factor. The findings highlighted that most of the obstacles are at the informal level as most attacks occur due to employee mistakes. As suggested by the interviewees, indeed, serious steps need to be taken by the MoICT, which include boosting cybersecurity and the associated budget, holding regular training and awareness courses as well as assigning certain employees as cybersecurity ‘champions’. Interestingly, he also advocated increasing the number of mandatory available e-services and reducing the manual services or only informational ones.

Interviewee 6, in this regard, focused on the problem of distributed databases, stating that,

> Some government agencies have common data, but they don’t have shared databases, which affects their performance and delays the work. For example, there is no link between the Amman Municipality and

> the Department of Lands. Buying and selling lands and properties, or changing the owner name needs the systems to be connected, but they are not. Also, the link between the ministry of justice and the courts is constantly experiencing errors, which, for example, means that certificates of no criminal conviction are not being delivered where needed.

Interviewee 18 also mentioned that advertising of e-government initiatives in the media (TV, radio, social, etc.) is very limited, whilst awareness and training (for the citizens) are almost non-existent. There is a pressing need to teach users (i.e. the public) how to use the e-service via learning videos. In order to do so, firstly, funding should be there for marketing. Secondly, complicated procedures have to be simplified. Submitting an application (e.g. pay tax) electronically involves several steps, i.e. data entry and review, (optional) payment and feedback. The portal of citizens should make the process easier by filling in certain data in advance and allowing authenticated users to view their personal information securely. Via a single sign-on, "My e-Government" citizens can be notified on time regarding any important events (e.g. expiration of their identification documents) or changes in their application status. Thirdly, it is time to stop the manual services and leave the electronic option only for citizens, which will force them to use e-services (but provide a support or help desk for citizens, perhaps at a post office, for example for people who do not have Visa. As mentioned by others, interviewee 6 also stated that e-payment is an obstacle. He reported that nearly 25% of citizens have a Visa card, 5% use e-payment, and only 1% have online banking. One answer he suggested was to enrol all banks in the e-payment gateway system (e-fawateer.com in Arabic), as a number of banks are not yet included.

Interviewee 11 emphasised that there is no marketing and there is insufficient budget for it. One suggestion by this interviewee was to make online chat available as a helpdesk for citizens. Also, the media department in the ministry should cooperate with marketing in the e-government programme. Training and awareness was, for interviewee 11, urgently needed for employees and citizens as well. This interviewee agreed with interviewee 16 that the laws, regulations, procedures and policies required updating alongside IT development. Citizens do not trust e-services, because of the many errors, may be when trying to log on, or because the system is down so often. They give up and decide to visit the relevant department in person. Hence, he said that all available e-services needed to be reengineered and where necessary fixed.

On the other hand, interviewee 15 claimed that systems security was adequate, but sometimes the citizens do not use the e-services, because the service (e.g. traffic violations) was not fully automated, so service delays occurred because part of it was manual. He argued that they should social media to make announcements about e-services, in particular, targeting young people. Procedures, laws, and regulations delay the services' completion, as well as the lack of funding. The interviewee reported how the complaints they receive made them aware that the citizens are looking for a good complete e-service, but there are many problems. He also believed that the governmental institutions should report statistics on e-services usage, but they rarely contact the MOICT with these, but is aware of issues owing to its contact with the complaints centre.

4.2.2.4 Cyber-security projects

As well as listening to interviewees' voices regarding their perceptions of the challenges and obstacles they face, further data were collected about what projects were on-going to address these issues. These are summarised in the table below.

Table 10: Key obstacles and challenges

Obstacles/ challenges/problems within the Technical, Formal and Informal levels	Cybersecurity scope	Number of interviewees mentioning the problem
Technical infrastructure and not using the latest technologies and updated systems regularly due to budget problems	Cybersecurity cannot be addressed effectively without being in line with new technologies. Latest SW and applications for different cybersecurity aspects have to be in place and updated regularly.	4
System errors or faults in outcomes that give bad impressions to the citizens	As an initial step in order to implement cybersecurity plan and strategy, information systems should be error free and provide the desired outcomes.	4
The procedures and the processes around which e-services are designed are based on old administrative tasks and do not match with new technologies (ICTs)	There is interaction between the different levels of cybersecurity (Technical, Formal and Informal). Problems at the formal level have a knock on effect onto the technical level. Thus, there is a critical need to update the cybersecurity strategy and plans periodically.	8
Errors in administration, procedures, and decisions that are not flexible and complicated	Cybersecurity processes and procedures should be simplified in order to reduce the number of means of validating the identity of the users/citizens.	6

Media and marketing efforts are not sufficient.	All media outlets should be utilised to gain insights into citizen's cybersecurity perceptions and opinions on various issues. In addition, there is a need to communicate public information about the government's cybersecurity approach to citizens so as to enhance their online trust in e-government services.	8
Non compliance by government agencies	The e-government programme needs to have a sustainable approach for monitoring the compliance of government organisations in all cybersecurity policies and plans.	5
Weak cooperation among government departments and lack of trust	Cooperation among government organisations is fundamental to enhance service delivery in an effective and secure way. IS interoperability of the e-government programme provides benefits, i.e. when there is interaction between entities through technical, semantic, and organisational means.	5
Human factor; absence of cybersecurity awareness and training	The e-government programme leaders need to arrange for regular cybersecurity training and awareness courses for all government employees. Also, the level of public cybersecurity awareness remains low and the government needs to set a plan to raise it, thereby	10

	increasing citizen confidence in how to use e-services securely.	
Citizens online culture and mentality	Successful e-government implementation highly depends on building citizens' online trust. Trust in the e-government programme is connected to the belief that it can deliver the required outcome securely. It may be necessary for the government to incorporate mandatory e-service engagement within the e-government programme in order to change some citizens' hostility to the online environment.	7

When asking interviewee 18 about any on-going projects relating to the cybersecurity of the e-government programme, it became evident that projects on cybersecurity had a reactionary character: they had been started because many attacks had occurred in government institutions. Many incidents happened because of employees' mistakes, like using removable drives, and downloading files from different websites. Hence, there needs to be strict rules regarding the use of hardware and software, with subsequent security training and awareness about these rules being essential.

Moreover, interviewee 18 referred to an army project on cybersecurity and explained that this was involving data gathering and identifying appropriate governmental organisations as well as military ones. Then, an evaluation would be conducted for a management framework (based risk assessment and the ISO27001 checklist) and a representative assigned from each organisation (response team of information security incidents). It was a great step towards starting cooperation between government and military institutions as the technical infrastructure is a fundamental aspect of cybersecurity approach and should be properly in place within all government entities. Interviewee 18 went on to explain that the aim was to secure the technical infrastructure (HW/SW applications) and support organisations with any missing element and provide cybersecurity training courses. He noted,

> The MOICT is expecting a lot of benefit from this project, because it (the military) has the power plus money, and any funding or change request will be approved as it is managed by the army. It is a serious action towards e-government cybersecurity.

Also, interviewee 18 explained that this cybersecurity project is co-hosted by the military, NITC, the central intelligence department (the 'FBI' of Jordan) and the MOICT. It is a project for national security with two parts: the development of the public sector in complying with ISO 27001 and the military part (details here have been omitted for national security considerations).

Another important project was highlighted by interviewee 16, who mentioned the upgrade to the Secure Government Network (SGN). By the end of 2017, there were 110 government institutions enrolled in the government network and 19 in the Government Services Bus (GSB). He added that upgrading the SGN should be a continuous process and enrol all government agencies should be kept up to date with the latest ICT and applications.

A third project was brought up by interviewee 25 – the National Optical Fibre Network. This will link all schools with the education ministry, for example, and all hospitals with the Ministry of Health, and so on. The possibilities for fibre optics are countless. Even under extreme load, signals will not be distorted. In sum, the government of Jordan has recognised the importance of broadband in national development and set up a plan to establish a national fibre network.

Optical networks are vulnerable to several types of security breaches or attacks, typically aimed at disrupting the service or gaining unauthorised access to carried data, e.g. eavesdropping. Depending on the aim of the attack, security breaches can induce financial losses to the organisations or cause network-wide service disruption, possibly leading to huge data and revenue losses. Hence, awareness of security vulnerabilities and attack methods is a prerequisite for designing effective optical network security solutions. A fourth project is for the Private Cloud. Interviewee 10 clarified that the e-government programme is starting to apply a cloud computing environment that is divided into G2C, G2B, and G2G. Only one of these is complete, namely G2G, with the other two still being work in progress. Interviewee 10 added that cloud computing will change the way information and services are managed and provided significantly. It can help the government ensure resilient and trusted collaboration. Government organisations need the ability to enjoy the best of the cloud and on-premises solutions and they must ensure that it is secure.

The fifth and last project brought up by the interviewees was the smart ID card for citizens. Interviewee 1 explained that the Jordan smart card is a national project launched as a cooperative endeavour between the MOICT, the Ministry of Interior and the Department of Civil Status and Passports. The aim of this project is to update the current ID card with a new version of a smart card that will have more security features (i.e. microchip). The new smart card will contain the basic personal information and those on the project are working on providing multiple applications that can be added soon to serve the citizens, such social security, national aid and health insurance, amongst others. Explaining the benefits, interviewee 1 added,

> The key benefit is to improve protection of information to minimise fraud and introducing the possibility of matching identities with their holder easily. The three top priorities for the national smart ID card

> are: improve security, resist identity fraud and establish a reliable online infrastructure for access to future e-government services. (1)

Interviewee 18 mentioned that Jordan's new electronic ID card will support digital signature infrastructure and enhance its capability of introducing new secure online services. The goal of the Jordanian government, he stated, is to develop national security, strengthen immigration rules and reduce the risk of fraud. The new ID card offers many possible applications and ensures identification, authentication, and signature.

> The government examined and checked this project several times in order to confirm its accuracy and safety as it will save lots of information. Hence, it is adopting the required and appropriate technologies that address high levels of security. Citizens will only need to carry this card in the near future in order to complete their transactions at government organisations. Usually, citizens have to complete many administrative forms and may require many documents for identification phase. Alternatively, the smart card microprocessor will store all the required data. (18)

Interviewee 26 added that the stakeholders should speed up the implementation of this particular project, stressing that smart cards represent a great move in pushing electronic services forward in Jordan.

4.2.2.5 Future Plans Policies and Procedures

Interviewee 25 explained the future general plan of the e-government programme. The programme will filter all governmental organisations and identify the five ministries that provide the most important e-services for all citizens, a process called RE-DO (reengineering digitising organisations). She continued,

> The cooperation will be between the private sector and public sector to achieve an automation project within a particular deadline and share the funding. New policies that are realistic and practical will be stated, also there will be strict principles for following up and monitoring the performance and the steps that must be taken. The new policy is called the BAT policy (Build/Automate/Transfer). The idea is to move towards the private sector to update IT infrastructure and the network to 4G. This policy is aimed at achieving three key goals: building technical infrastructure, improving information and cyber security and working with the private sector to encourage investment in IT. (25)

Improving cybersecurity is one of the key goals of this policy. Interviewee 25 explained the Digitising Jordan Plan, for which MoICT will identify the institutions that provide the most important services to citizens and it has set a deadline for 2020 to improve government e-services, in particular, their security. Furthermore, bureaucracy is a key obstacle to investment and thus, they are planning to reengineer the services and complicated governmental procedures, eventually automating them. The ministry will provide operational support and technical infrastructure, which will help the chosen organisations. Complicated procedures must be simplified with no bureaucracy to encourage investment in the ICT sector as well, as explained interviewee 25. It is clear from the interview with this interviewee that the new policy is taking on all the challenges and obstacles mentioned above and that the MOICT is aware of the cybersecurity problems the e-government programme is facing. In addition, at a higher level of importance, the MoICT has recognised that cybersecurity is an essential requirement for e-government systems and networks.

Furthermore, regarding the data collected in order to ascertain whether the government has changed anything in the policies, procedures, etc., interviewee 15 stated that government these should meet the set of regulations, rules, best practices, national information security policies and standards that direct how an entity manages, protects its communications and distributes sensitive information.

> Citizens' Complaints Centre sends a copy of the report of citizens' complaints to the quality manager, to determine which e-service has a problem (and in which part) and then takes action. For example: the e-service of providing a certificate of no criminal record or conviction has had to be re-established due to the large number of complaints, problems in the e-payment system and the delivery process. (15)

Interviewee 14 suggested entering a list of all banks in the e-payment gateway and also putting an awareness note box before taking the user to the payment window or screen. Putting a sample or picture of the payment page on screen will increase citizens' trust in paying online. Interviewee 17 said that the Change Management Department sometimes checks social media and hence, knows that an e-service has a problem from citizens' comments and posts. So, it then asks the complaints call centre to send a report to the MoICT to try to fix it.

According to interviewee 15, complaints centre reports show that most complaints are related to system functionality and technical errors. The interviewee emphasised the importance of following up citizens' complaints and responding to them. The government should be responsible for handling citizens' complaints regarding e-services as this will positively influence their cybersecurity perceptions and online trust.

The researcher asked interviewee 1 whether there were regular information security audits and what these comprised. He responded that there is no regular schedule for conducting security audit reports or for the security audit process itself. Instead, the IT department in each government institution has to send reports to the e-government programme, in particular, to the IS department, upon an MoICT request. He explained,

> Organisations should send a request to NITC for conducting risk assessment, but very few organisations do this (15% of government agencies only). There are no laws or instructions to force the organisations to undertake a regular audit. Security is not very important and comes as the third priority after functionality and ease of use. This is because security costs a lot and they don't want to spend money on it. (1)

Cyber security should be managed at the highest levels of government and as a top priority for it remains a national security threat. Cyber security must be a shared responsibility of government organisations and needs cooperation to ensure a collaborative approach to cyber capability development, protection, breaches response and recovery. The e-government programme should have a leadership responsibility for ensuring that government information systems and networks are protected against cyber threats. More urgently, legislative reform will have to take place where required to make sure that government agencies comply with cybersecurity policies and procedures.

At the NITC, interviewee 21 clarified that information security has two parts: proactive, which refers to checking everything before using it and incident handling after an adverse event. He commented that almost all their work fell into the second category.

4.2.2.6 Communications

While probing the subject of communications, both internal and external, the role of the media was also raised. Firstly, whether the e-government programme was responsible for all services

and whether they were centralised was probed. Interviewee 6 explained that the media department reviews the role of media in e-government projects, covering all aspects, including the traditional press, radio, television and new media techniques provided by the Internet. Regarding the role of the media, interviewee 6 said that the e-government programme has to measure the effectiveness of the government's communication outreach efforts and has been investigating the possibilities of using social media to enhance citizen's trust. He continued,

> The MOICT have to focus on the ways through which e-government can take advantage of the available social networks to get actual engagement with citizens, to adopt new way of interaction with individuals, and to get more insights into citizen's perceptions and opinions on various issues. (6)

Interviewee 4 said that despite the efforts of the media department of the MOICT and other government institutions in spreading the e-government initiatives and services, not all of this had been productive. This is for various reasons, such as lack of budget being assigned to media purposes as government agencies do not consider this to be a priority, thus failing to understand how the media could help promote these services.

Turning to internal communication, the researcher asked about this among government agencies as well as regarding monitoring and compliance relating to information security issues. The implementation of the security policy and continuous compliance monitoring by the information security team and systems managers should be carried out, as stated in the policy.

Interviewee 9 stated that all relevant security events have to be monitored, with employees being made aware that their actions on any internal systems and network are monitored and logged to ensure that systems are being used in an authorised manner. System administrative and errors records must also be monitored to identify any potential vulnerabilities and security issues.

Regarding monitoring e-services and usage reports, interviewee 16 revealed that,

> There are no records at the ministry, every governmental organisation holds the records of the e-services that they deliver. Each institution is

> responsible for its e-services statistics and the MOICT asks for reports, but they don't always respond or send them. (16)

Clearly, there is a decentralised approach to monitoring, which leads to questions concerning this and other aspects of governance.

4.2.2.7 Governance and risk management

In addition to the e-government programme's role as a fire fighter addressing individual risks that are often low impact, a national risk management programme is required to establish a framework for serious risk management at the national level. Accordingly, the researcher inquired about issues related to governance and risk management at the national level. Questions as to whether the government organisations that provide e-services had identified the risks, vulnerabilities and threats from different parties and whether they had implemented security controls appropriately were put. Interviewee 8 contributed by saying,

> When it comes to the cyber domain, you can never expect to reduce the risk to nil. There is no such thing as a 100% secure system. However, if we understand the scale and potential impact of these risks, we will be better able to assign the appropriate levels of resources. Effective risk assessment in government organisations is desperately needed. We need to identify the risks, the probability they will occur and the likely impact they will have, then set this against the duties and assets of the organisation.

Interviewee 1 added that as there is no risk-free system, government organisations must have disaster recovery plans as a key outcome of effective risk management programmes, as this will ensure organisations are back in operation in a short time period after incidents occur. Additionally, interviewee 4 reported that e-government administration is facing problems in dealing with risk management and governance. The ministry, she argued, needed to introduce a framework based on technical and non-technical dimensions to structure e-government risks. Governance should be a central issue since it defines the general requirements for dealing with potential risks at all levels, both regarding the IT and organisational aspects. Interviewee 7 confirmed that the MoICT is not sufficiently aware regarding this issue. He reported that in his opinion the e-government programme lacked the appropriate governance to be able to deal with information security and cybersecurity issues effectively.

4.2.2.8 Legal and regulatory framework

Further interview questions related to the legal and regulatory framework for the general security environment, including regulations to protect data and the confidentiality of information. Interviewee 21 believed that a nationwide policy should be developed, published and communicated to provide guidance on relevant international information security standards and regulations. He added,

> Information security standards, policies, regulations and legal requirements should be reviewed regularly to be up to date with the rapid change of the cyber-domain to ensure effectiveness. These standards, policies and laws have to be centralised as well at the MOICT for review, evaluation and development and to ensure compliance by government organisations.

Interviewee 16 said that they needed to have a clear review process and procedures. The review process must focus on organisational compliance with laws, policies and standards of information security. Moreover, it should provide recommended improvements or changes needed according to the law as well as organisational and technical aspects. Added to that, the review should consider feedback from government organisations' managers and stakeholders.

Two interviewees made suggestions regarding compliance. Firstly, interviewee 13 recommended that,

> Information Security Policy must be applied to meet ideal information security requirements for government organisations. To do so, it is necessary to ensure that the law is properly implemented. Specialised team should be formed with experts from the Ministry of Information and Communications Technology and the Ministry of Justice to explore this area and provide recommendations. Government organisations need to develop their own internal regulations consistent and compliant with national laws regarding information security-related issues. (13)

Second, interviewee 18 offered his own idea regarding the place of the e-government department in the government structure, "… the E-government Department should be a separate independent institution belonging to the prime ministry in order to have the power and authority they need to force government departments into compliance with the information security laws, standards and policies."

On the question of the confidentiality of information, interviewee 1 mentioned that government organisations issue security clearances to system administrators, and users using or accessing information systems. He continued,

> Staff access follows a need-to-know mechanism to ensure control and monitoring of government information systems. The national network and communications infrastructure, by law, must be secure and address sensitive information confidentiality in order to engender the trust of the government and citizens. (1)

Interviewee 10 explained that government organisations need to use encryption along with other security measures to protect classified sensitive and critical information assets. At the same time, interviewee 26 said government organisations must ensure that sensitive information is not leaked through systems and should take the necessary measures to protect systems with sensitive information. However, he then said,

> The main issue is that the ministry doesn't have the power to force other ministries and governmental institutions to be hosted by them, or to provide training courses or make regular audits. Most attacks occur, because of employee errors and human fault and there are more in the ministries that host their own servers and websites. External attacks rarely occur, and when they do, this is considered confidential, so we don't announce it.

4.2.2.9 Information assets management and classification

The researcher put questions relating to information assets management and the associated asset classification scheme being used within the e-government programme. Interviewee 2 stated that information classification within e-government systems is very important for indicating the level of sensitivity of information and for specify how it must be handled in terms of its protection depending on this level. Any noncompliance will be registered and disciplinary action will be taken. He added that asset owners are responsible for protecting, controlling and managing the organisation's assets on a day-to-day basis. He summarised this as,

> Rules covering the acceptable use of assets are clearly defined, documented and implemented. This is to ensure that employees are aware of their responsibility for the appropriate use of information resources and act responsibly and professionally; following the security standards of behaviour.

Interviewee 9 mentioned that employees have to use information, systems and equipment in line with information security policies and understand that all their actions will be monitored. Moreover, they should know that they have a legal responsibility to protect personal and sensitive information. He added,

> Illegal or unauthorised access and suspect misuse of the systems by a member of staff will be considered by the officials and could result in disciplinary action taking a place that involves a warning, suspension or discharge from the job. (9)

Similarly, interviewee 6 explained that newly hired employees should be made aware of the issues raised above as a matter of urgency and be advised to not take any action that may harm their new job status.

4.2.3 Informal level findings

The third major grouping of interview data is the informal level. The subthemes included here are employee issues, including vetting and the security culture, citizen issues, such as their security awareness and trust in online services. The aim of these questions was to gain understanding of what human challenges were faced in information system security and what steps have been taken regarding these issues by the government.

4.2.3.1 Employees

First, the researcher asked about the importance of the human factor and Interviewee 1 confirmed that many security breaches occurred because of this. That is, employees, in particular, play a key role in information security incidents occurring within government organisations. Interviewee 20 expressed the view that there is a clear lack of attention towards this issue within all government organisations. This interviewee said that they had started to send procedures by e-mail, weekly SMS, and published articles on the government websites regarding employee information security training and awareness. In fact, information on training courses for employees is being circulated to all government organisations. Unfortunately, of a total of 25 ministries, only three have responded to this initiative: The Ministries of Foreign Affairs, Labour, and Education. She added that at the Ministry of Education 4,000 computing teachers had been trained. These courses include an introduction

to information security, social engineering, secure use of the Internet as well as basic instructions and recommendations. Continuing, she stated,

> There is not sufficient response and cooperation by government organisations. All employees have to receive information security training and awareness courses and notifications of updates on security policies and procedures as well. These courses should be given to personnel in accordance with individuals' relevant roles and responsibilities. This must include updates on current security issues and threats and should highlight the importance of reporting any incidents or risks to the information security team. On the other hand, employees should take the opportunity to provide their feedback on the content, relevance and impact of the information and training they receive. (20)

As summarised in Table 4.2, employee cybersecurity training and awareness is a key weakness in the current information security approach of the e-government of Jordan. Different interviewees put forward different views/suggestions on this matter. For example**,** interviewee 2, suggested increasing awareness by making learning videos for both employees and citizens on governmental websites. Interviewee 21 stressed the urgent need for regular cybersecurity training and awareness courses, while interviewee 11 commented how this is virtually non-existent. The continued by saying that through close consultation with academia and international partners, a greater degree of security awareness could be achieved, along with establishing the Jordanian governments own expertise through a defined Capability Building Programme.

In terms of employee vetting, the researcher asked about terms and conditions in employee contracts. According to interviewee 16, as a part of their contractual commitment, employees have to agree to and sign the terms and conditions of their employment. This should state both their responsibilities for information security and acceptable use of digital assets. Based on information security policy, the security related terms and conditions of employment should make direct reference to it. She added,

> The responsibility to maintain the confidentiality of citizens and all stakeholders' information is stated within the terms and conditions of employment and should continue beyond employment. The terms and conditions of employment state that users' computers and activities may be monitored to ensure compliance with the Information Security Policy. (16)

Interviewee 26 explained that even if they have the greatest cybersecurity protection available, it is only as strong as each individual member of staff, and this is the core of the problem. Several causes of cyber-attacks had stemmed from uneducated members of staff, both at low and high security levels. Whilst staff are the greatest weakness, they are also the most targeted element.

Interviewee 26 said employees were not sufficiently informed about security issues, in particular, in terms of their duties and responsibilities. He expressed the view that employees' cyber-culture was a critical matter for protecting the organisation during their work and thus, the risk of human faults should be reduced to a minimum. Interviewee 13 mentioned that some employees had an IT or computer science background, whilst others did not. Furthermore, interviewee 12 reported that,

> New employees must get an initial briefing regarding information security and cybersecurity, in general, within the first month of employment as part of an induction schedule. This briefing provides understanding of security requirements implications, protection methods and the controls used while doing their jobs. (12)

It is acknowledged by the ministry, that organisations that continually train their staff in security policy and role-based security responsibilities will have a higher rate of success in protecting critical information resources (MoICT, 2017). However, from the evidence above, it would appear that this recognition is not always being put into practice

The other half of the informal level that relates to citizens and the findings associated with them is discussed next. Considerable effort is needed to ensure that the public understands that they need to protect themselves online. A positive cyber security culture is essential for effective cyber security, while developing and strengthening citizens and businesses is fundamental to the success of the broader cyber security capability (Da Veiga, 2016).

4.2.3.2 Citizens

First, it is important to know whether the government has a mechanism for getting feedback from citizens into the informal management of IS Security, and if so, how it is used to improve security and perceptions about it. Interviewee 20 pointed out that while cybersecurity within the e-government programme is the responsibility of the government itself (and the various

departments of government), it would be more effective and successful if all citizens saw themselves as part of the effort. Despite cybersecurity being one of the most important challenges faced by governments today, he contended that the level of public cyber-awareness remains low. He added,

> E-government should utilise social media in order to publish, announce and share information about e-government initiatives. In addition, e-government can use social websites for cyber-awareness campaigns to guide the citizens how to use e-services securely and enhance their trust in governmental websites from an information security perspective. Moreover, future courses for university students about cybersecurity and information security need to be coordinated with the universities' chairmen or officials. (20)

Interviewee 22 explained the introduction of the knowledge stations project aimed at building cyber-awareness among citizens. The knowledge stations are IT centres for communities, providing Jordanian citizens with the opportunity to use ICT as an effective tool to serve the local community. He went on to say,

> This project is a practical step in the adoption of ICT applications in the communities in order to activate the use of e-government in the service of citizens in their places of residence. The stations offer computer courses, including information security courses, to citizens, but they have not been announced through appropriate channels and very few citizens know about them or have heard of them. (22)

This interviewee continued explaining that the NITC (National Information Technology Centre) was assigned the task of implementing the programme and preparing a study to determine the optimal distribution of knowledge stations to all cities in the country. Citizens who need help in using e-services or have concerns about cybersecurity when using government websites can visit the nearest station to get help from the IT qualified staff and computer science employees who are assigned there by the government. Knowledge station employees can help citizens to use e-services securely and offer related cybersecurity courses. Interviewee 22 confirmed that the establishing knowledge stations is an important project, but that there is an issue with the implementation and he concluded that so far it has not be a fruitful project, in particular, due to the lack of promotional activity.

Interviewee 26 said that e-government managers have concerns about the impact of insufficient security and privacy protections in government networks and systems. Such concerns can be a main barrier to adopting e-government services. He added,

> Citizens can be affected by a number of issues in terms of their perception of trust in government, such as the bad attitude of the public administration, corruption and transparency issues. Without confidence in the e-government services, processes, procedures, and other aspects of government, the vision of fully electronic service delivery will remain a challenging and unfulfilled target. (26)

In a comment of particular relevance to the present study, interviewee 11 stated that technical infrastructure, technical faults and errors in outcomes leave a bad impression with citizens, because of the weak online or e-services culture among citizens.

Successful e-government implementation depends on building citizen trust at a high level. Trust in the e-government programme in many previous studies (e.g. Alomari et al. (2009); Abu-Shanab (2012); Naoum and Nadhim (2014); Al-Azzam and Abu-Shanab (2012); Jiang et al. (2008); Peppa et al. (2012); Shajari and Ismail (2012)) is considered as the belief that the e-government can *deliver the required outcome securely*. However, the citizens of developing nations generally have a dearth of such trust in e-government, and in online transactions. At present, a much greater concern about cybersecurity issues is associated with using new technologies in developing countries, which is largely focused on the technical level, particularly in relation to e-government systems and websites. However, based on the relevant literature review, much more attention is required towards the informal level (human factors, cyber-awareness, cyber-culture, etc.).

Lastly, there has been no marketing or information campaign to enhance citizens' trust in e-services, because no specific budget is available for this. One interviewee proposed making an online chat service available as a virtual help desk for citizens. Citizens' lack of trust is reinforced because of many errors, for example, when they are unable to log on. He argued that there was a critical need to reengineer and fix all available e-services and added,

> As e-government's ambitious goal is to be able to develop and deliver high quality and integrated public services electronically, the government needs citizens to trust the e-government systems and network. Otherwise, they will not use e-government services.

> Therefore, government needs to make an enormous effort to regain that trust. (11)

Interviewee 6 argued that when it comes to citizens' online culture, society is not homogenous, for they have different interests, backgrounds and levels of knowledge and experience. According to him, e-government officials need to realise that there are different stakeholders, who have different requirements and messages.

The same interviewee also discussed the matter of e-government's reputation, stating that "Citizens sometimes tell their experiences of using e-services to each other. Bad feedback from a citizen will probably influence other citizens like family members, relatives and friends." (6).

On a similar note, Interviewee 2 commented that,

> The key challenges we are facing are the culture and mentality of the Jordanian people. Citizens may think that government systems and websites are not secure, because of the lack of an online culture, meaning they are not familiar with e-services.

Interviewee 15 said that the government needed to change citizens' online culture, and remind them about e-services. According to him, it should teach them how to use these e-services so, the marketing and media teams should start doing their job correctly. The e-government programme must use the social media to announce e-services and target young people, he added.

4.2.4 Additional themes – the NTIC and knowledge stations

In addition to the three overarching themes of the technical level, formal level and informal level the researcher explored two further topics in more detail: the NITC and the knowledge stations. The NTIC is the primary arm for utilising the national IT resources of the public sector and seeks to maximise its contribution towards the success of the e-government programme of Jordan. In particular, as the operator of the e-government programme, it is concerned with the operational handling of the Secure Government Network (.gov.jo) and national cybersecurity.

As above explained, the knowledge stations initiative was launched in order to provide help for the public in using e-government services through offering ICT resources and several computer courses. In addition, qualified staff are assigned to the stations who are able to deal with citizens; queries relating to e-services, including cybersecurity issues. Due to the centrality of the NITC's role in being the operational arm of the e-government programme and of handling the SGN as well as the unique role that knowledge stations play in helping citizens to use e-services (especially if they have any cybersecurity concerns), these two subthemes are explored below.

4.2.4.1 National Information Technology Centre (NITC)

One interviewee with a thorough knowledge of the NITC explained the five main responsibilities of the centre. The first one he mentioned was the security incident reporting service. The role of the NITC in this respect is to communicate with relevant parties when security breaches occur and help them in developing rapid solutions aimed at restoring their services. The Computer Incidents Response Team (CIRT) unit was initiated within the NITC in 2014. This unit helps all governmental organisations respond to and recover from cyber incidents. The CIRT unit becomes involved when a system administrator reports a possible security incident. The first step is isolating the compromised system from the network, and then, preserving the evidence. The staff member from the CIRT unit along with the system administrator who reported the incident, set up an incident handling team to investigate the extent and type of occurrence, whilst also determining the impact of the incident. This is in order to generate an official report for top management and list and actions required and recommended to mitigate future incidents. The final required step is to restore the compromised system after the official report has been filed.

The second aspect handled by the NITC is their role in raising awareness about information security. As interviewee 21 explained,

> The NITC is very active in this area, conducting campaigns to raise awareness using manuals, brochures, workshops and even sending out SMS messages to people employed in the public sector, all aimed at raising the profile of information security issues. (21)

Thirdly, according to the same respondent, the centre runs a security audit service for government organisations. Following the audit, a report is submitted to the MOICT (more

specifically to the e-government unit's information security department) addressing any security breaches, raising the level of security, and protecting the information. Fourth, as he explained, there is the security inspection service provided by the centre. Through this, government websites are inspected periodically to probe for weaknesses that may lead to hacking, which doubles as a mechanism for raising cyber-awareness to government employees, he noted. Finally, interviewee 21 explained the digital certification service for government websites, which issues certificates to pages linked to government websites confirming their identity and encrypting data entry.

The NITC, being part of the e-government programme, has the role of securing the cyberspace of the government organisations of Jordan, especially the e-government systems and network. The security department was established in the organisational structure of the NITC in 2011, working as the operator of the information security department on the e-government programme. However, this department does not have systematic procedures for interacting with other government departments in making their employees more aware of security matters, thereby addressing the human factor in this context. Internally, a number of specialised courses were being prepared for the staff members of the computer incidents response team (CIRT) unit and updating cybersecurity laws, strategies and policies was in progress.

4.2.4.2 Knowledge stations

As shown in Table 4.1, three people were interviewed in the knowledge stations department, the director of the project in the National Information Technology Centre and two station managers. As previously explained, the initiative of establishing them was aimed at providing access to ICT available for all Jordanians. This was seen as a step towards promoting sustainable human development as well as helping governmental efforts to engage the public with e-government services, particularly in local communities and remote areas. The government of Jordan with the private sector attempted to find some organisations (public and private) related to the ICT field to launch initiatives in support e-government implementation. As a result of this, the Information Technology and Community Service Centres (later renamed knowledge stations) were launched in 2001 (Knowledge stations, 2007). The NITC was responsible, on behalf of e-government programme, for execution of the project after it conducted a study for selecting the best sites for the stations.

The researchers presented a justification for the knowledge stations project as one of the government steps to change the online culture in Jordanian communities, which was typified by a lack of Internet access as well as needing ICT facilities and services in local communities. Besides this, it considered that it would be beneficial to offer knowledge to the public about e-government services from different aspects, including cybersecurity, so as to improve their online trust in these services. This prompted the researcher to ask questions regarding the aims of this initiative and the interviewees' perception of its progress. The station managers mentioned these issues, with interviewee 22 saying that since its inception, the Jordanian Knowledge Stations project has sought to achieve three main objectives. The first was to create local communities and integrate them with the e-government project by providing various electronic services to these local communities. The second aim was to qualify the members of the local communities through their participation in training programmes and courses in the field of ICT, whilst the third aim was to contribute to the progressive elimination of computer illiteracy by providing ICT education and training. Indeed, if the knowledge stations achieved those aims this would help changing citizens' online culture and could affect their view of e-government services, in particular, in terms of how secure they are.

Interviewee 23 reported that the stations were providing training courses in ICT to encourage the use of the government information systems for gaining local information. In addition, there was the goal of enhancing the use of the Internet and citizens' skills by increasing their knowledge in ICT, thus equipping them to become involved in the e-government services. Interviewee 24 explained that the Jordan Knowledge Stations Network consists of 196 knowledge stations established over 15 years and spread throughout the Kingdom. They have played a major role in preparing local communities to deal with e-government services once they were launched nationwide. She further explained that the stations provide the means to of entry or transit sites to the national network for conducting electronic transactions and as part of the e-government initiative. Interviewee 24 then opined that knowledge stations are contributing to bridging the digital divide and resulting in the utilisation of information and communication technologies in various areas of life. In other words, the stations have helped in improving citizens' online culture, and trust in e-services. The number of beneficiaries has increased to more than half a million since its inception. She explained that the percentage of males was 53% of the total number of beneficiaries, with more than 120,000 citizens have received training in information technology and have been awarded certificates, which have contributed to improving their working conditions. However, as Interviewee 24 went on to

explain, whilst about half of the citizens may know about the knowledge stations in their areas, only a small minority have benefited from the services provided and thus, their promotion is needed through advertising.

According to Kreyer, Pousttchi and Turowski (2002), the concept security can be considered in two dimensions objective and subjective. Objective security refers to a physical technical characteristic that is ensured through a specific technological solution that responds to all security objectives: confidentiality, authentication, integrity, authorisation and non-repudiation. Evaluating the objective security of a procedure by the average user is not possible. The essential condition for e-services acceptance is the perception of security, which is called subjective security. This is defined as the degree of acceptance of the procedures' security from the user viewpoint. Thus, the knowledge stations can help in enhancing the subjective security concept, by changing citizens' perceptions of security in a positive way (what citizens require to feel secure about using e-government services). For example, confidentiality and encryption are technical features that strengthen data protection. In addition to this, an important means to provide subjective security at these stations is marketing activity to enhance citizens' engagement with government e-services. Citizens demand knowledge as a condition to use e-services and staff at KSs are qualified to provide this knowledge. Moreover, according to Al-Shqairat and Altarawneh (2013), availability of transparency and traceability for the citizens using e-services at the knowledge stations has considerable advantages.

In the view of all three interviewees at the KSs, 22, 23 and 24, the stations have faced obstacles from the point of view of the employees, which are: lack of financial resources, people being unaware of their location and administrative bureaucracy exercised by top management based Amman. Then, they mentioned that around 80% of staff at the stations have suffered from a lack of job security, which had led to their constantly seeking other work. In addition, there was the weakness of the lack of coordination between the KSs and local communities. In sum, these interviewees were of the opinion that if these issues were not addressed, then this would greatly impact on the ability of the KSs to support ICT and hence, contribute to improving e-government programme participation.

4.2.5 How the interview study informed the survey

It was important for the researcher to use the findings of the interview study to inform the design of the survey study. Table 11 explains how this was achieved.

Table 11: Linking the interview findings to the survey

Key themes from the interview findings	Brief description of correspondent findings	Related survey question developed	Results from survey
Marketing and media (TV, radio, SMS, social networks)	The media department at the MOICT has employed all available media, such as the traditional press, radio, television and new media techniques provided by the Internet. E-government should utilise social media in order to publish, announce and share information about e-government initiatives. In addition, e-government can use social media websites for a cyber-awareness campaign to guide the citizens in how to use e-services securely.	Q. Do you know that this service is available online?	54.9% Yes 45.1% No
Citizens participation and adoption of e-services	Statistics report shows that the e-services usage rate is still low. This is due to a number of barriers, for example, technical errors, systems faults that may impact negatively on citizens' online trust. Moreover, citizens	Q1. Did you try to use it?	42.2% Yes 57.8% No
		Q2. Have you faced any problems that made you feel that government	34.8% Yes 65.2% No

	sometimes don't know about the available e-services or had had a bad experience when using one. Citizens are looking for secure and efficient e-services provided by the government. Thus, e-government programme developers are working on reengineering e-services.	systems/websites are not secure?	
Complaints call centre	The complaints call centre receives citizens' complaints and enquiries regarding e-government services. The centre reports show that most complaints are related to system functionality and technical errors. The government should be responsible for handling citizens' complaints regarding e-services as this will positively influence the citizens' perceptions and online trust.	Q1. Have you ever contacted the complaints call centre regarding e-services?	18.4% Yes 81.6% No
		Q2. Was any action taken to rectify the problem?	41.7% Yes 58.3% No
Citizens' cybersecurity perspective and awareness	The government needs a mechanism for getting feedback from citizens to be considered in the informal management of IS Security. This to be used to improve security and perceptions about it. It would be more	Q. How cyber-secure do you feel in sharing your data online for e-government services?	7.2% Very secure 33% Good 44.3% Moderately 11.3% Slightly 4.1% Not at all

	effective and successful if all citizens saw themselves as part of the effort.		
E-payment gateway	The e-government programme of Jordan has established a unique portal (e-Fawater.com) through which all electronic payments relating to e-services are conducted. E-payment is still an obstacle, so the government needs to enrol all banks in the e-payment gateway system.	Q. How cyber-secure do you feel in using the e-payment gateway (e-Fawateer.com)?	6.7% Very secure 31.1% Good 43.5% Moderately 11.9% Slightly 6.7% Not at all
Citizens online culture	Citizens are not familiar with e-services and generally online culture is weak. Moreover, bad experiences in using e-services has influenced their views on them and they may think government systems/networks are not secure. The key challenges the e-government is facing are the culture and mentality of Jordanian people. For example, most citizens do not have online banking and do not trust the security of e-payment systems.	Q1. What views do your relatives, friends or colleagues express regarding e-government services? Q2. In what way do these views influence you in terms of using/trusting e-services?	8.2% Very positive experiences (Very trustworthy) 10.3% Positive experiences (Trustworthy) 27.7% Moderate 27.2% Slightly negative (Untrustworthy) 26.7% Very negative 5.6% Very positive effect 16.9% Positive effect 25.1% Moderate effect

			24.1% Negative effect 28.2% Very negative effect
Knowledge stations	Knowledge stations is an important project, but there has been an issue with the implementation, leading to the conclusion that so far it has not been a fruitful project, particularly due to the lack of promotional activity. Citizens who need help in using e-services or have concerns about cybersecurity when using government websites can visit the nearest station to get help. IT qualified staff and computer science employees are assigned to these stations by the government. Knowledge stations offer different computer related courses for the public such as, cybersecurity principles.	Q1. Do you know about the government's knowledge stations for cybersecurity training and awareness?	15.4% Yes 84.6% No
		Q2. Have you ever visited or attend a course at one of them?	18.3% Yes 81.7% No

Citizens' online trust	There has been no marketing or information campaign to enhance citizens' trust in e-services, because no specific budget is available for this. The participants proposed to make an online chat service available as a virtual help desk for citizens. Citizens' lack of trust is reinforced because of many errors, for example, when they are unable to log on. It was argued that there is a critical need to reengineer and fix all available e-services and that there should be much greater concern about privacy and security issues.	Q1. How trustworthy do you perceive government systems and websites to be?	8.8% Very Trustworthy 16.1% Trustworthy 59.1% Moderately Trustworthy 11.9% Slightly Trustworthy 4.1% Not at all trustworthy
		Q2. How secure do you perceive e-government services to be?	10.8% Very secure 20.5% Good 37.4% Moderately 25.6% Slightly 5.6% Not at all

The chapter now moves on to present and reflect on the results of the survey study, which was the second research phase.

4.3 Results of the survey

This section presents the results of the survey to which 203 people responded. First, the demographics of the sample are summarised before the main findings are presented.

4.3.1 Demographic profile

Table 12 provides an overview of the demographic profile of the respondents in terms of gender, age, education level and Internet use experience. The sample can be characterised as predominantly being middle aged ranging from 30 to 39 (26.6%) or from 40 to 49 (23.2%). In terms of qualifications and Internet use experience: 67% have a bachelor's degree; and 52.2% have been using the Internet for more than 10 years.

Table 12: Demographic profile of the respondents

Respondent characteristics		**Frequency**	**Percentage**
Gender	Male	109	53.7
	Female	94	46.3
Age	<18	0	0
	18-24	20	9.9
	25-29	37	18.2
	30-39	54	26.6
	40-49	47	23.2
	50-64	35	17.2
	65+	10	4.9
Education level	School only	13	6.4
	University or college	136	67
	Postgraduate education	55	27.1
	No education	0	0

Internet use	Few years (1-5)	19	9.4
	Long time (more than 5 years)	73	36.1
	Very long time (more than 10 years)	106	52.5
	Never	5	2.5

4.3.2 Key Findings of the survey

4.3.2.1 E-services adoption (usage statistics)

As mentioned before, the survey was conducted in two ways, electronically and by the researcher in the field. The survey started by asking the respondents if they knew that the desired government service is also available online and whether they had used it before or not. Of the 55.3% of respondents that knew about the available e-services, only 42.2% of them had used them. In terms of e-services usage statistics, the most utilised was the traffic tickets service (22.8%) and the least was the residency and borders service (4.5%). The results are very much in line with the e-services usage statistics report by the MoICT and the adoption rate of e-services generally is very low. In addition, 35.2% of respondents indicated that they had faced problems, which made them feel that the government systems or websites are not secure.

4.3.2.2 Communication with citizens

The majority of respondents (81.6%) have never contacted the complaints call centre regarding e-services and regarding those who had Figure 11 shows a breakdown of issues raised.

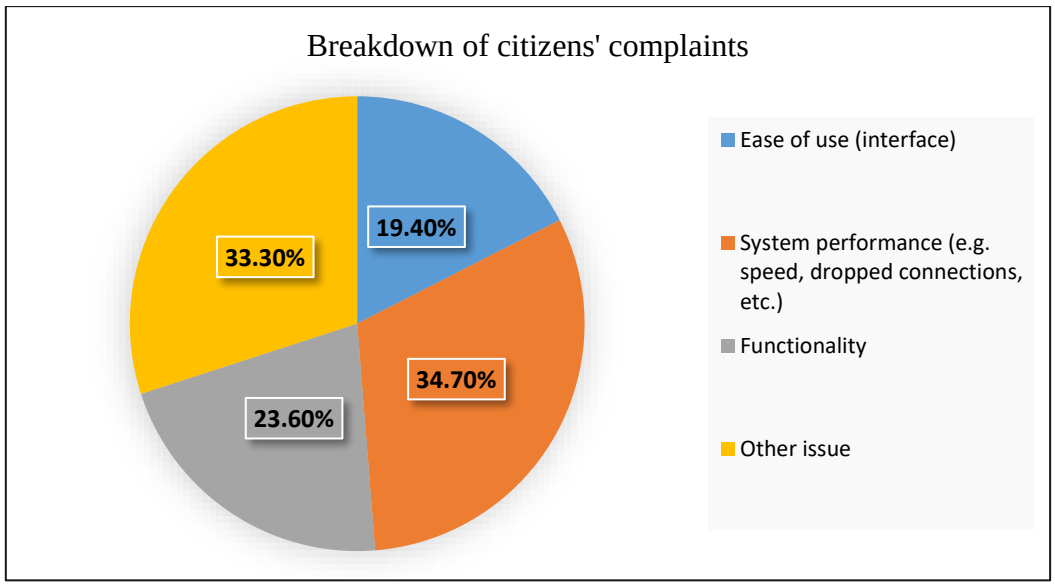


Figure 11: Breakdown of citizens' complaints

When the respondents were asked how satisfied they were with the information provided in the complaints response, about 46.3% considered it was OK and in 41.7% of the cases action had been taken to rectify the problem. The average response time for the complaints was around three days. The results indicate that citizens' complaints are related to system security issues and show how many a hoping for more effective secure e-services (see Figure 12).

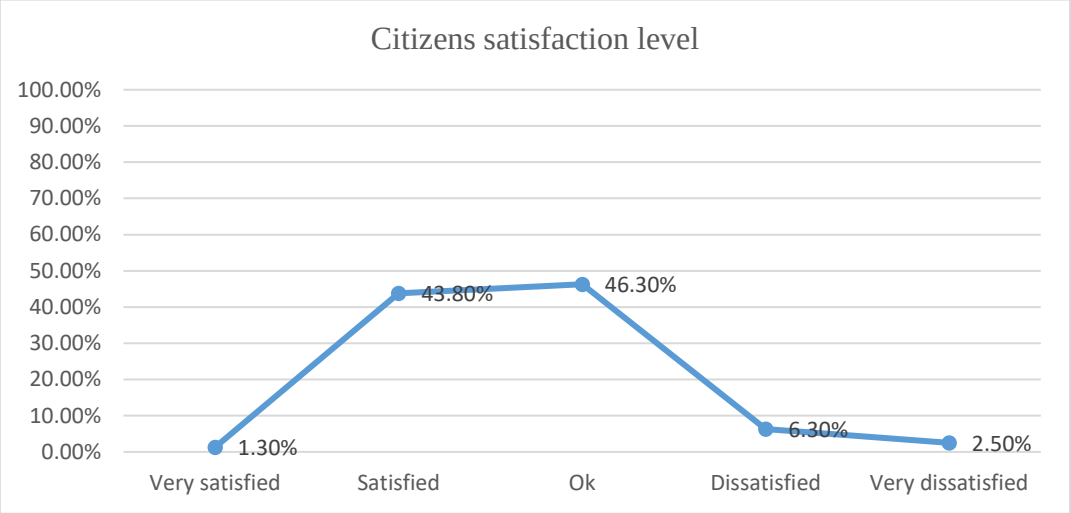


Figure 12: Citizens' satisfaction level with the information provided in the response of the complaints centre

4.3.2.3 Citizens' perceptions of cybersecurity and online trust

The results show that 44.3% of respondents felt moderately cyber-secure in sharing their data online for e-government services and 43.5% felt this when using the e-payment gateway (e-FAWATEER.com). Also, 28.5% were influenced very negatively by the views of their relatives, friends or colleagues regarding e-government services. Moreover, the results of online trust of respondents regarding government systems and websites or e-government services are clarified in Figure 13 and Figure 14.

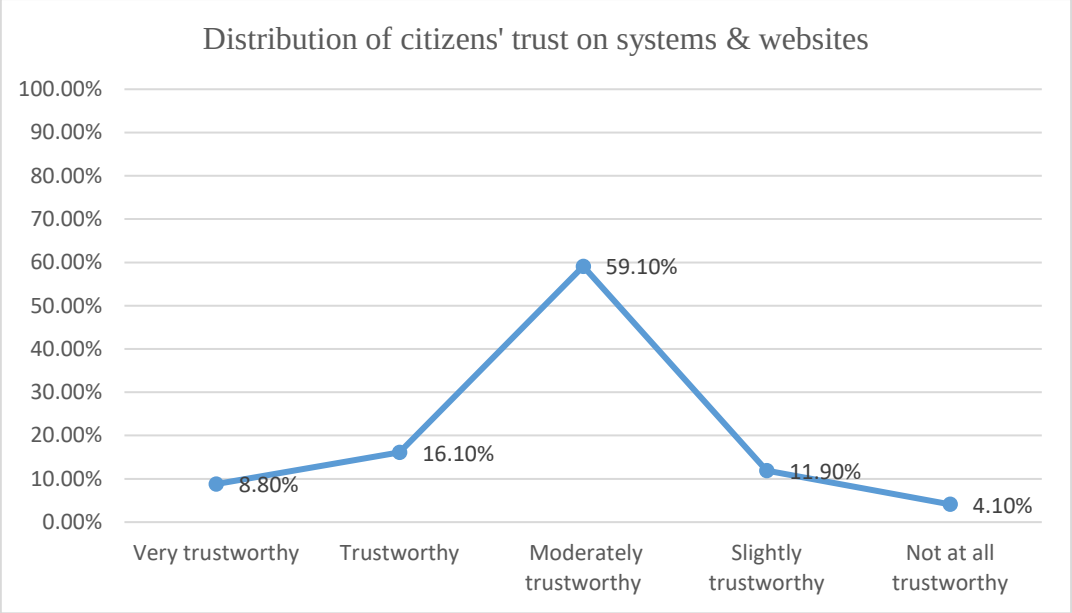


Figure 13: Distribution of citizens' trust in government systems and websites

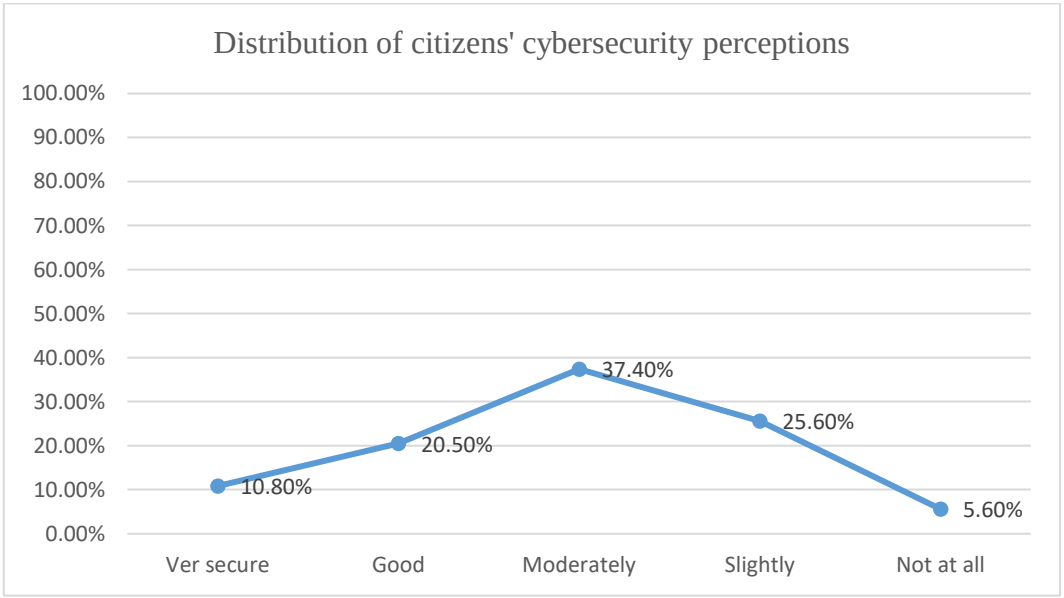


Figure 14: Distribution of citizens' cybersecurity perceptions of e-government services

The respondents also indicated what makes them feel less secure and the answers involve common items that should be taken into consideration by the MoICT, the host of the e-government programme in Jordan. These issues are:

- System errors, faults, system being down, slow functionality and low performance;

- Bad experiences when using e-government services, especially when it comes to the e-payments. Many times the systems are not updated so the payment is not shown and paper work is still the proof for payment;
- Systems look not well developed or designed and not updated (not using new ICTs), which gives the impression that cybersecurity is not a priority;
- Hacking attempts or attacks, as well recent security incidents, such as virus attacks;
- No trust in e-government services, because there is none in the government itself, as its efforts are not satisfactory for citizens;
- Services complexity and no ease of use; citizens are not familiar with them
- No clear delivery process;
- No marketing for e-government services and no security awareness regarding using these services.

4.3.2.4 Citizens awareness and training

As mentioned before, the knowledge stations programme was established in order to provide citizens with computer services and qualified employees, where they could receive help in using e-services. Thus, it was very important in the survey to include items about this issue. The majority of respondents (84.6%) did not know about these government knowledge stations, and of the 15.4% who knew about them only 18.3% had ever visited one (see figure 15).

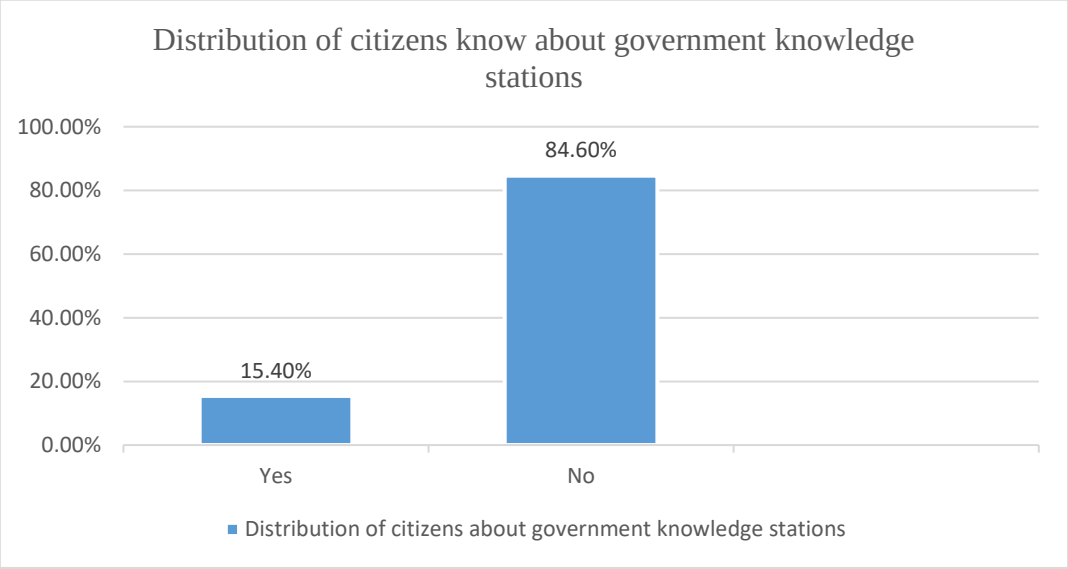


Figure 15: Distribution of citizens knowing about government knowledge stations for cybersecurity training and awareness

4.4 Conclusion

The research was designed after the relevant literature related to cybersecurity on e-government had been reviewed and cybersecurity practices based on the TFI model in terms of important security issues to be considered were identified. The research was carried out to evaluate the approach to cybersecurity by the e-government programme in Jordan, and also, to examine how it is affecting citizens' trust in e-services.

Security is one of the factors determining the success or failure of the e-government services. Information confidentiality, integrity and availability are core objectives of cybersecurity, which are essential for significant e-government adoption. However, the interview findings show that cybersecurity implementation in most government organisations is very limited. There is lack of a consistently applied information security policy, risk assessment plan and compliance with security regulations. In addition, according to the findings, there is minimal cybersecurity awareness and training.

The MoICT needs to focus more on taking a proactive approach than reacting to cyber-attacks through incident handling. Some of the core issues highlighted in this chapter on the weaknesses of the current cybersecurity approach include:

- Low level of systems and websites development; no use of updated or recent ICTs;
- Fragmentation of e-services systems and providers among different ministries. A number of ministries and government departments are not hosted by the MoICT;
- Cybersecurity is considered as an after-thought; the decision makers do not give cybersecurity a high priority at the early stage of an e-government initiative;
- Lack of cooperation and coordination among governmental organisations/departments. There is no appropriate cross-organisational approach;
- Lack of compliance by government organisations/departments with the e-government programme instructions and policies;
- The e-government programme has no constitutional power to force government organisations to follow information security laws and regulations or to cooperate;
- General lack of understanding of the importance of training and awareness of cybersecurity among both, government employees and users;
- Many incidents have happened because of employees' mistakes. Around 70% of attacks are internal.

These aspects are corroborated further by the survey results that indicate that there are lack of awareness about government e-services and ignorance about cybersecurity, and this has negatively influenced citizens' willingness to use e-government initiatives. Number of factors relating to cybersecurity are affecting some of citizens' online trust, such as facing technical problems using e-services and websites issues.

The next chapter is the discussion of the research findings and a theoretical reading of the data analysis.

5.0 Discussion

5.1 Introduction

This chapter moves on to a theoretical reading of the data analysis, for both the interviews and the survey, seeking to expand the meaning and interpretations of the data presented. That is, the aim is to acquire a deeper understanding of how an information security approach within an e-government programme can be formalised through the different security dimensions at the technical, formal and informal levels. Also, a theoretical connection is extended to how this information security approach is communicated to citizens' online trust.

Of course, the present interpretations are informed by choices in the analysis, including the coding themes identified, the format of the findings chapter and the framework underpinning the way that has been used to present the data. As Garrick and Rhodes (2000) assert, the criteria of representation, in the end, are decided by the researcher. The discussion seeks to present and consolidate these insights of research, by considering the current information security approach within the e-government programme in Jordan and abstracting from it. In this way, the discussion moves towards presenting a different theoretical framework for information systems security management within governmental entities.

In this study, the researcher have used the TFI security model in order to examine the information security approach within the e-government programme in Jordan. Whilst the technical aspects have attracted the attention of scholars in different disciplines (Ahlfeldt et al., 2007), such as e-government (Abu-Shanab, 2012) and e-commerce (Bert, 2016), the formal and informal have been left understudied in e-government research despite their relevance when studying information security (Hassan & Khalifa, 2016). In addition, the context of online trust from the perspective of cybersecurity in the adoption of government e-services is also considered.

The first section in this chapter discusses the key findings of interviews regarding the Jordanian e-government programme. The discussion develops the theoretical contribution by proposing a TFI-oriented information systems security framework for e-government programmes that specifies all security aspects, thereby consolidating technical and non-technical issues. This TFI information security model is applied to provide a deeper understanding of how

information security can be managed and ensured by the e-government programme for all government organisations/ departments. The main focus of the second section is the impact of different information security aspects on citizens' trust on e-government services. Then, in the last section, the proposed security framework is presented and discussed in detail.

5.2 Information security approach

5.2.1 Introduction

In this section, different issues of the information security approach at Jordanian e-government programme are discussed using the TFI security model. The researcher argue in line with what Dhillon and Backhouse (1997) and Dhillon and Backhouse (2001) assert, that the information security domain involves technology, processes and people, whilst adopting a wider view of technical, organisational and human aspects. In addition, I clarify the relation between these three parts and the continuous interaction in order to develop a solid theoretical foundation that will help in designing the proposed framework.

According to the National Cybersecurity Strategy 2012, the Jordanian government is committed to enhancing its cybersecurity and determining its priorities for cybersecurity for government entities, businesses and citizens. At present, it is time for the government of Jordan to review its progress in the objectives stated in the cybersecurity strategy and to set the priorities for the coming years in light of the potential threats various challenges. The rapid growth of technology and the Internet offer great opportunities for the e-government programme. The digital world is assisting the agenda of development via social inclusion, access to key services, job creation and economic growth. However, without an effective cybersecurity approach, it is not possible for the Jordanian government to improve its performance through electronic transactions and thus, provide effective wide-ranging e-services for the public. In Jordan, cyberspace is a modern environment that needs systematic and comprehensive protection at all levels (international, national, organisational and individual levels). The security of information systems is vital for making the best use of the opportunities that the new technology can offer, thereby ensuring that cyberspace is attractive for all stakeholders (government, businesses, and citizens). These increased opportunities of new technology also come with new and challenging threats to government cybersecurity in Jordan. The e-government managers must ensure that they handle these threats effectively, in

a way that makes the best use of the existing resources and workforce, while having sustainable capabilities.

As mentioned before, this research was aimed at examining the cybersecurity approach within the e-government programme in Jordan (using the TFI security model), and then, exploring how different information security issues affect citizens online trust in e-government services. In order to achieve those aims, three research questions were addressed through a data collection process using two methods. The first and key data collection method, semi-structured interviews with e-government staff, answered Q1 and Q2, whilst the complementary data collection method, a survey of citizens, meant Q3 could be addressed, as the following section will explain.

As the findings show, the Jordanian government's approach to ensuring the security of its critical information infrastructure is generally basic in that it has not connected through integrated framework. In addition, it is not comprehensive focusing more on technical issues than non-technical, and do not deal with cyber space threats in a serious manner as there is no regular security audit. The revolution in ICTs, networking technologies, and the high volume of information exchanged via the Internet and government networks make it more difficult within the current adopted approach to reach the desired level of information security. As discussed in the findings chapter, the e-government programme consists of many information systems distributed among government organisations/departments. The vulnerabilities of the present approach, combined with rapid advancements in technology, are putting the government systems and networks at higher cyber risks. In this context, the government needs a secure and reliable national information infrastructure, capable of facing different types of security attacks or unpredictable disruptions. This is necessary to maintain a high-level of online trust in these systems across government and amongst citizens.

The government has recognised the challenges posed by inappropriate users' access to cyberspace. Meeting these challenges requires coordinated and focused efforts from all government organisations and more engagement with citizens. In addition, all information security plans and procedures should adhere to a national cybersecurity strategy to ensure consistency and successful implementation of a coordinated and effective cyber-defence. To address the challenges of cybersecurity head on, and seize the opportunities that cyber space

offers, requires leadership and governance at the highest levels using a comprehensive security framework.

5.2.2 TFI model

In this subsection, the first research question is addressed, namely: *What is the approach to information systems (IS) security in the Jordanian e- government programme at the technical, formal and informal levels (to be examined based on the TFI security model)?* This part covers the three levels, extracting the theoretical conditions from the empirical findings.

5.2.2.1 Technical Level

The technical level of the proposed information security framework involves four core aspects, derived from my empirical data and the relevant literature, these being: access control, SW/HW and applications updates, information systems interoperability and a secure government network.

1. **Access Control**

According to the analysis of the empirical data, the government of Jordan recognises the need to cooperate with businesses to establish a programme responsible for information assurance and cyber security related-issues for the critical technical infrastructure (information systems and resources). Government organisations have to issue security clearances to different parties using or accessing information systems (e.g. employees, systems administrators and end-users). To do so, appropriate management and commitment of resources are necessary, particularly for security clearance validation and renewal.

In the context of access control, a role-based form is the mechanism used to determine who is entitled to access information resources within the e-government programme. The main issue in this respect is that there needs to be assurance that all government employees follow this process (of least privilege or authority), thereby delivering a secure environment that avoids unauthorised access and cybersecurity breaches. To achieve this task, the government should regulate, co-operate and work closely with those parties that manage, own, or operate critical technical infrastructure. It should do so in order to provide security guidance in both physical and virtual domains so as to secure the technical infrastructure. Based on the empirical findings, access management within Jordanian e-government systems should ensure a regular review to

the roles or groups used to control access. Through this, it can make sure that required rights are being granted to the appropriate or authorised users and revoked based on actual working requirements.

The literature review of the relevant academic articles on e-government has identified some significant issues for building a robust technical infrastructure. Information security measures were clarified in many studies (Ndou, 2004; Luo, 2010) as needing to cover all aspects, including access control, authentication, authorisation, and auditing of electronic transactions. These measures must be mandatory to ensure the CIA information security triad (confidentiality, integrity and availability) within e-government systems is fulfilled. Kim et al. (2006) further support this argument, asserting that it is an essential responsibility of e-government to manage access to information resources. Thus, there is a need for incorporating technologies that prevent unauthorised access to citizens' personal information and sensitive data.

Based on the analysis, the role-based access control (RBAC) is a sufficient access control mechanism and technique. It is considered to be an improvement on DAC and MAC. This is compatible with Chuanfan (2010) study which noted that RBAC has been used as an effective tool to manage unified resource access of large information systems by governments. Zhou and Hu (2008) describe the key five elements of RBAC, which are: users, roles, constraints, permissions, and sessions.

The access control of e-government is a core part and very pivotal in the proposed security framework to protect government information resources. Regarding the Jordanian e-government programme, the application of role-based access control is an effective mechanism for dealing with the access control of system information resources at present, which covers identification, authentication and authorisation issues. Insufficient logical access controls lower the reliability of government department data and raises the risk of unauthorised revelation of information/data (Zhou & Hu, 2008).

Theoretical condition C1: *For the e-government security framework, RBAC must be used as it is the most suitable access control mechanism for ensuring the reliability of government department data and reducing the risk of unauthorised revelation of information.*

2. SW/HW updates and security applications

Another part of my empirical data, referred to as the technical level, revealed that the e-government programme in Jordan needs a robust and regular schedule for computer system updates (HW, SW and applications), with the latest and most effective technologies utilised. As mentioned in previous sections, the appropriate identification and management of security requirements is essential for developing secure e-government systems. The cybersecurity framework should be in line with new technologies and will require regular updates to the technical infrastructure (i.e. IPS, IDS, biometric systems and cloud computing).

The majority of studies relating to cybersecurity, according to Coffey et al. (2018), state that the role of technology in providing automated safeguards and processes would help to determine the series of actions to be taken to secure information systems. Regarding which, the two main obstacles that were identified in Jordan, as shown in the analysis, are budget constraints and the lack of top management support. Hence, these aspects should be considered in the information security framework. This is consistent with what Al-Omari (2006) have asserted, that Jordan still needs more effort regarding ICT utilisation in delivering secure e-services. At the same time, my empirical data shows that Jordan has never had a lack of fundamental resources, which means that the Jordanian e-government programme needs to work primarily on updating its infrastructure. Despite resource availability, as Mohammad et al. (2009) argue that, e-government implementation in Jordan suffers from a number of challenges, internally and externally, involving both the rapid changes in technology and good leadership to adjust to IT developments. While my study confirms these previous findings, my empirical data indicate that many of cybersecurity projects are still in progress, such as, PKI, private cloud access and smart ID cards. The cybersecurity strategy of 2018 covering the period up to 2023, emphasises the urgent need for government organisations/ departments in Jordan to confirm that software work in an effective manner. Indeed, it is important to reduce the numerous errors and flaws in software that are subject to exploitation by attackers.

Online projects that provide electronic services for large numbers of users or stakeholders, such as e-government, are social-technical systems (STS), formed based on both social requirements and technical ones (Whitworth et al., 2006). In general, a lack of adopting the latest technologies is often one of the main challenges facing the implementation of e-government programmes (Lutui et al., 2017). For successful e-government programmes, service continuity

is important for both the availability and delivery of services. Also, building trust progressively and increasing confidence amongst citizens are essential.

Theoretical condition C2: E-government security framework must engage with the latest security software and applications, which should to be updated regularly in order to prevent, detect and handle different security attacks.

3. Information Systems Interoperability

Another aspect related to the technical infrastructure is information systems interoperability. My analysis, as discussed in findings chapter, involves an overview of information systems interoperability issues that are important in an e-government programme: organisational and technological. The empirical data confirmed that there are technological barriers, such as the incompatibility of information technologies, plus organisational barriers relating to authority, tasks allocation and organisational structure. Thus, the Jordanian e-government programme has to face these challenges and find solutions that will enable it to address information systems interoperability at the national level (e.g. through enterprise architecture that allows government organisations to engage in ICT outsourcing and provide shared services). At present, IS interoperability of the e-government programme is not sufficient due to lack of interaction between entities. Abbasovich and Fikratovich (2015) hold that e-government systems have to ensure the confidentiality of information resources. To achieve this, the control of all actions and events by the security system need to be centralised and integrated for all government organisations/ departments. Based on the empirical data, such an integrated framework will allow the public administration to evaluate the social impact and to detect different problems relating to the operations. The major aim is to find a proper partnership between government administrations, in turn, means to optimise security management and services quality in favour of the connected departments (administrations). Thus, the security policy and architecture within the e-government programme of Jordan should be established on a single standard, which will address information confidentiality. In particular, this is needed to provide shared services which require a concentration of resources and activities that are distributed among the organisations. This has a direct affect to satisfy citizens and enhance the corporative image due to the low level of bureaucracy connected with the given functions.

Al-Shboul et al. (2014, p.1112) confirm the findings in their study: e-government related research has not adequately addressed issues concerning the implementation and integration of e-government systems. Indeed, there is a need for better understanding of the barriers to systems interoperability within the e-government programme in Jordan and for a comprehensive framework that deals with all issues.

Theoretical condition C3: The e-government security framework needs systems interoperability to allow for the public administrations to have a unique interface for the solution of a number of complex problems.

4. The Secure Government Network (SGN)

The last element at the technical level of the information security framework is government network security. The SGN is the most important initiative for bringing together government organisations into a secure network, playing a pivotal role in providing e-services for citizens and other stakeholders. Moreover, electronic government transactions, e-mail services, and data exchange between government's entities through the Government Services Bus (GSB) are key parts of SGN. In this context, the empirical data analysis clarifies the different security applications and technologies used to secure the SGN, such as Public Key Infrastructure (PKI) and firewalls. As reported in the analysis, the isolation of internal users in the SGN of Jordan has been achieved, basically, by using firewalls. The e-government programme needs to involve regularly reviewing and monitoring the firewalls to make sure they are operating securely and remain error-free (as much as possible), so that they can defend the assets of the e-government network.

The PKI is generally operated by the NITC, which provides the encryption service for government organisations. For such a complex network like the SGN, a PKI is required to provide a mechanism for each endpoint (a computer or a device) to verify the identity of other endpoints, based on centrally provided services. Its design, implementation and operation are critical, needing to be well-protected against potential attacks or threats. Shareef (2016) highlights that it has been identified as the best e-authentication technology for e-government. Furthermore, Weise (2001) points out that in most of the cases where a PKI is required to check the identification of end entity cryptographic devices, its usage will be restricted to a single host or provider. In such a situation, the Jordanian government, as represented by the NITC,

needs to ensure that the processes and technology used are appropriately secured. For instance, the root of the PKI should be kept permanently disconnected from the network, and turned off, until it is required. Lambrinoudakis et al. (2003) propose also founding well-defined processes for registering and revoking devices into and out of the PKI. These should be assigned to related work activities to ensure that only those trusted infrastructure endpoints have actual valid certificates, with all PKI related activities being authorised and audited.

In Jordan, government departments are using Public Key Infrastructures (PKIs) to undertake internal transactions through virtual private networks (VPNs) so as to secure government information resources. However, all government departments should be connected with each other to execute a single step process. In order to exploit the internal security capabilities of government departments for government to government (G2G) relations, it is essential to connect their corporate PKIs.

Unexpectedly, my analysis has revealed that a number of ministries and government organisations, *upon their own request*, are not hosted by the MoCT, which is responsible for the e-government programme. The separation of these organisations is creating several problems in the management of cybersecurity. As the findings have clarified, the private network of the government (SGN) provides several security services protecting government websites and hence, these separated organisations are more vulnerable to security attacks. The e-government programme in Jordan have a problem in controlling cybersecurity under the central approach and those overall effect e-services that divided over a number of providers. Research on fragmentation of delivery of public services has shown that mismanagement of e-services, lack of cooperation and coordination, and lack of trust among government organisations will lead to poor cybersecurity and increase the number of cyber-attacks (Dhillon, 2007). As a result, it is an urgent requirement to connect all government departments within the SGN by technical, organisational and legal solutions. Discussing high-level security applications and technologies used to secure the SGN is very critical for the information security framework.

Abu-Shanab and Baker (2011) argue that since using e-services requires exchanging sensitive personal data through the Internet, users would use e-government services only if they felt secure and trusted that their personal information is protected. A number of studies have explored different security dimensions within the e-government network context, such as

secure communication with government through a website (Hasan & Abuelrub, 2011), trust in the use of personal information by the government workforce (Colesca, 2009), observance of information privacy (Rotchanakitumnuai, 2008), and data storage in a secure server (Henriksson et al., 2007). However, this study differs in that all aspects relating to the government network have been. Based on the findings and the preceding analysis, the theoretical demands that are posed at this level include centralisation of information infrastructure for all e-services providers.

Theoretical condition C4: The e-government security framework must involve a secure government network to connect all government organisations.

5.2.2.2 Formal Level

The formal level refers to the organisational aspects in the proposed information security framework, which are information security management and cooperation among government organisations, communications, policies, laws and risk management.

1. **Information Security Management (tasks allocation and cooperation)**

The findings have identified the responsibilities of top management within the e-government programme, responsibilities that began with making the decision to automate a public service. Indeed, the issues of cybersecurity in the request for proposal (RFP) process are highlighted in information security component. Despite that component which determined the required actions regards information system security, my analysis has uncovered the critical need to work on e-services development or re-engineering because of technical errors or faults. The annual report of the MOICT in 2017, which is responsible for the e-government programme, highlighted the future plan or required steps to enhance the cybersecurity of e-government services. These steps included re-engineering the process for available e-services, upgrading the SGN and enrolling more government organisations to the national portal. The empirical findings confirmed this focus and the government of Jordan has established many cybersecurity projects that are still in progress, such as the SGN upgrade and single sign on.

The main reason behind different problems they are facing is that the top management of the e-government programme does not act or deal with cybersecurity with the highest level of priority. Even though the current e-services are not working sufficiently, as discussed in the

example of non-criminal certification, the main concern of officials is to launch more e-services, which is potentially jeopardising both quality and information security. The lesson learned when developing a new e-service, system or any project, is that security requirements and measures should be defined in the early phase. In the context of security by design, the development of software and hardware seeks to minimise systems vulnerabilities and reduce attack probability through designing and building security in every phase of the system (Bannister & Connolly, 2014). Moreover, security technologies need to be tested in the real organisational environment to ensure that they are applied sufficiently.

Further, the need for a common infrastructure for interconnecting the information systems of different government administrations has been confirmed by the findings. The novelty of the investigation has been to focus not only on the technical part, but also on organisational one, in order to identify the structure and the relationships among different organisational units. As my analysis shows (e.g. in Chapter 4, p.104), while the tasks are allocated between the staff of the Jordanian e-government programme in an appropriate manner, the communication between the different government organisations is unstructured. In this regard, without setting a clear structure for communications between all government organisations, the e-government programme's purpose to provide e-services on behalf of different government organisations is limited. The proposed framework could prove very useful where more than one department needs to participate in an e-services requiring effective information security management. The government of Jordan needs a comprehensive plan of organisational cooperation between entities that have shared services or vertical services to address all information security or cybersecurity controls/measures. Abstracting from that finding, information security management through a comprehensive cooperation plan among government organisations is crucial at information security framework.

The extant literature highlights the different human, technological and organisational issues as well as the barriers and challenges related to information security management in e-government in developing countries, (Ndou, 2004). What the studies in these countries reveal, is that governments in developing countries can effectively take advantage of the benefits and opportunities that ICT offers, but e-government success depends on certain conditions, needs and obstacles. The common challenges of e-government go far beyond technology in that they call for organisational structures and skills and new forms of leadership (Allen et al., 2014). In general, most governments are faced with the challenge of transformation and the need to

modernise administrative practices and management systems. This can be solved by establishing an integrated infrastructure and enacting e-services re-engineering for sufficient information security management.

Cordella and Iannacci (2010) argue that the traditional model of government (i.e. the bureaucratic paradigm) described as functional rationality, vertical hierarchical control and rules-based management, is being replaced by the e-government paradigm. This new paradigm is characterised by flexibility, horizontal hierarchy, and vertical/horizontal integration. The e-government paradigm stresses coordinated network building, external collaboration and stakeholder services. Accordingly, the right government organisations should be engaged in defining security requirements when launching a new e-government initiative in order to determine the potential vulnerabilities and threats.

It is a common opinion among scholars that cooperation represents a useful vehicle for the success of e-government (Mecella & Batini, 2001b). At the architectural level, information security solutions are quite stable, where organisational obstacles hinder the required development of cooperation among different administrations (government departments). The study of Mecella and Batini (2001a), commensurate with my data analysis, has clarified that the technologies which support a cooperative information system security can be used sufficiently in any type of application. The critical point for effective information security management is to build a general framework to integrate information systems aimed at supporting vertical applications. Hence, the Jordanian e-government needs a reengineering process of procedures and services. This integrated framework would allow for different government departments (public administration PA) to evaluate the security applications and to detect problems (vulnerabilities or weakness) relating to the operation.

As shown in the analysis of formal aspects in Chapter 4, not all these public portals guarantee security issues, reliability and interaction homogeneity with the government department (independent public administration). Moreover, there has been little attention to the stakeholders (citizens, business) perspective. These problems have discouraged the citizens and other stakeholders regardless of the new services and technologies. Thus, the proposed framework is helpful for considering shared services infrastructure.

It is necessary for each government department or single public administration to optimise the realisation of their own front-office services and to define a common on-line interaction model with other government departments. This will ensure interoperability and service provider identification, e-government programme then can provide the activities that allow the authorised organisations or departments to state their own services in a secure manner. From the perspective of the user, a better identification system will allow the citizens to use any service from any provider using the proper technique on authentication and authorisation.

At present, e-government managers in Jordan are the people who are having to undertake the integration of the back-office services of the different involved government departments. Therefore, the implementation of various administrative procedures that require interaction among several government departments needs the development of a second activity. For example, the automated processes have to present a unitary secure view of the government or public administration from the end-user perspective, a concept called one-stop government. The lack of shared back-office services that is disturbed by the problems mentioned before, such as online culture, trust and top management bureaucracy, makes the implementation of such activity very difficult.

Integration across different departments will help in overcoming problems such as information security issues and increase the quality of services. As the work of Krenner (2002) shows, relying on ICT outsourcing, such as in shared services, can help the development of e-government processes significantly and provide better information security approach. In addition, the application of cooperation considers one of the most common problems of the e-government.

Theoretical condition C5: The e-government security framework must consider e-services reengineering and building an integrated framework for effective information security management.

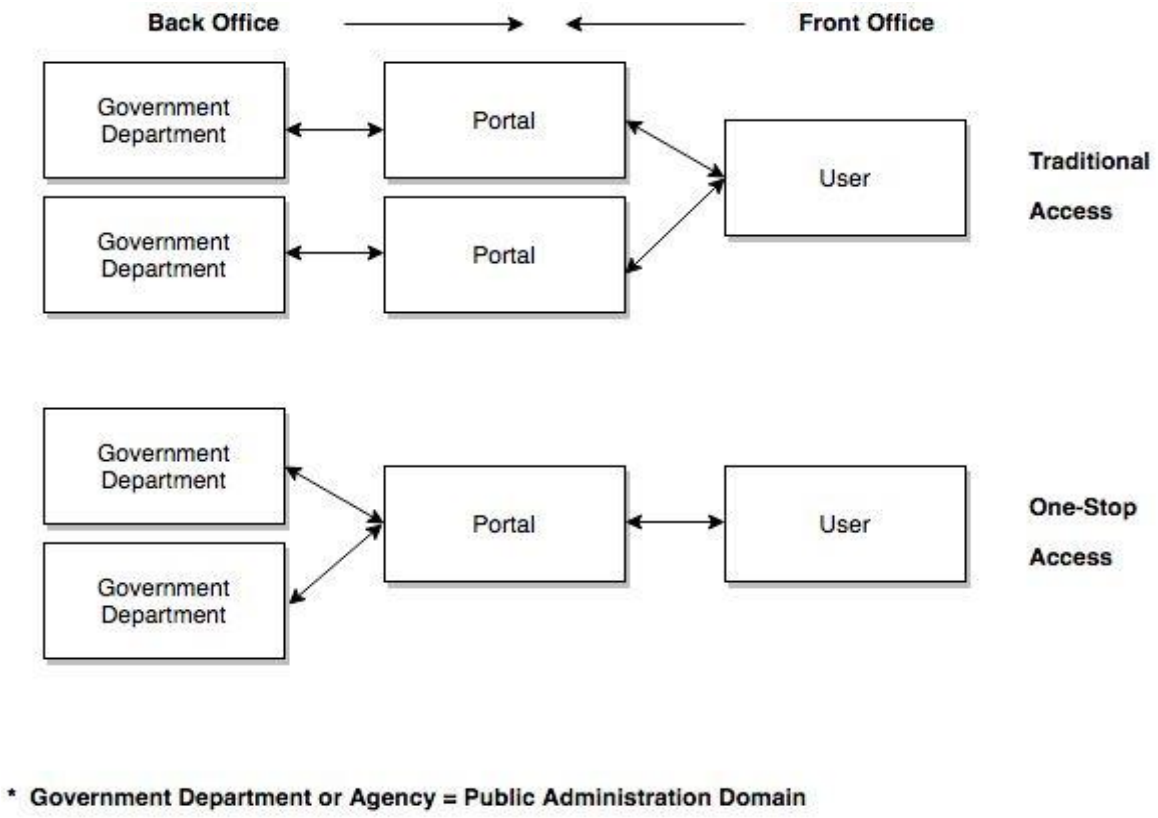


Figure 16: On-line one-stop government

2. Government Organisations Communications (compliance with e-government)

The analysis conducted in Chapter 4, at the communications part, revealed mostly negative sentiments about the level of communication among government organisations and departments in Jordan. This is due to the narrow definition and poor understanding of the concept of e-government as well as the related functions. In his study, Ndou (2004) considers this as one of the reasons why many e-government initiatives fail in developing countries. While the e-government programme is multidirectional by its very nature and consists of many different connected parts that require a wider understanding of secure communication mechanisms, it is not typically treated as such.

The e-government programme in Jordan is using ICT tools and applications, both Internet and non-Internet based, to support communications of different electronic transactions between government and citizens (G2C), government and business (G2B), and between government agencies (G2G). However, they are facing many limitations that are impacting negatively on the way of interaction.

As these transactions rely on using the Internet, the risks are elevated and the need for cybersecurity is critical for the protection of information resources and sensitive data. In terms of external communication, there are a number of security objectives (i.e. CIA triad) relating to communication between stakeholders (citizens, business) and government departments that must be met by conventional communication procedures in e-government. As Alexander and Millar (2003) note, when designing an efficient e-government system, information security is essential for consideration regarding the protection of data transferred from government organisations. That is, an e-government system is an on-line system that involves handling a lot of sensitive data that must be protected via a secure isolated government network from unauthorised users.

The Jordanian government is using a web portal called (gov.jo) making available information and communication to the public organisations and also secure e-services for citizens and businesses. Thus, cybersecurity is critical for successful e-government transactions and services. Alexander (2003) summarises the security threats and suggests security solutions that should be adopted by an e-government programme to protect the transactions via the government network (see table 13).

Table 13: Security Threats and their solution in an online system/project (based on Alexander, 2003)

Threat	**Security**	**Function**	**Technology**
Modification: Data modified or changed, thus targeting data integrity.	Encryption algorithm/hash function	Encode data to prevent tampering	Cryptography Algorithms, MD5/ SHA etc.
Interception: Unauthorised user via a network gains access to data or reads the data during transmission, which undermines data confidentiality.	Firewall	A firewall prevents certain traffic from entering the government network or server	Virtual Private Network (VPN)/firewall

Fabrication: False identity with an intention of fraud, which compromises authentication (an unauthorised party as intruder may add transactions to a network communication system).	Authentication (password and username)	Identity verification of both sender and receiver	Password/ digital signature (PKI)
Interruption: Data of the system become lost, unavailable, or unusable, which hinders availability (copyright protection of data).	Digital records	This type of data is copyrighted but not secret (read-only for the public)	Digital signal/image processing

Wang (2009) highlights a very important point that must be taken into consideration by e-government when considering communication. That is, it is essential to look at the input and the output of each sub-process in an e-government service through which data are exchanged between government departments and stakeholders. In other words, a distinction needs to be made between data transfer, for example, from citizen to department (citizen as the originator) and in the other direction (citizen as the recipient).

These transformational areas mean that an e-government service does not consist of simple business process reengineering. The Jordanian e-government programme needs to monitor/investigate the security of communications pathways of government departments with external stakeholders. For instance, according to the interview data, the media department at the MoICT has not been promoting e-government initiatives in Jordan enough to enhance citizens' online trust, promote cybersecurity awareness or teaching them how to use e-services securely. For example, from my empirical data, an important issue to consider is that social media tools are a new type of media that can help decision-makers in understanding how citizens interact with issues published by the Jordanian e-government programme and how they react or respond to them. The development of social media, such as social websites and other

social networking tools (Facebook, Twitter, etc.), encourages governments to join these sites as an attempt to seek advantages from a new way of communication. Moreover, as an easily accessible platform to the public via Internet access, social media pushes governments to rebuild their relationship with their citizens and to increase the level of citizens' engagement (Abu-Shanab, 2014).

Another part of communication in the e-government programme is G2G communication amongst internal stakeholders. Regarding communication among Jordanian government organisations or departments, collaboration and cooperation is essential. This is because it will allow government organisations and departments to share information resources, databases, staff skills and capabilities, which are not being addressed at present. This will help in improving the efficiency and productivity of organisational processes. According to Mecella and Batini (2001a), the execution of vertical and horizontal integration of information systems needs efficient communication that will enable the integration of services from different government departments to help citizens and other stakeholders have secure and easy access to e-services.

Indeed, the government of Jordan requires a radical rethink of the nature of the functioning of government organisations and the relationships between them. The Jordanian e-government programme needs to focus on a web-based relationship involving all organisational levels and processes that will allow information to flow easily *within* governmental boundaries and between departments. The e-government programme needs to provide security for the technical aspects, such as network security and computer systems security, as well as the non-technical aspects, including organisational issues and human factors. According to my data analysis, the importance of providing security in Jordanian e-government comes after many cybersecurity incidents occurred due to weakness points in the SGN and other resources, both technical and non-technical, or the deployment of insufficient cybersecurity standards and regulations. E-government has to set a standard mechanism to detect vulnerabilities, where vulnerability might be known or in the worst case, unknown within communication gateways. The proposed information security framework relies on building secure infrastructure for government electronic transactions and communications (G to G, G to C, and G to B).

Theoretical condition C6: The e-government security framework must provide secure gateways for internal and external communications among government departments and with other stakeholders (citizens and businesses).

3. Policies, Standards and Procedures

The analysis clarifies that, in Jordan, each government organisation, based on its security requirements, has the ability to develop its own security policies that fall in line with the national security policy of the e-government programme. However, government organisations need to cooperate to ensure that their policies augment, comply with, and remain consistent with e-government information security policies. A national cybersecurity policy should be developed, published and communicated to provide direction and support for information security strategy, relevant laws, regulations and standards. Information security standards and policies should be reviewed at planned intervals to accommodate the rapid change of the cyberspace environment, thereby ensuring cybersecurity and effectiveness. Information security standards and policies should also have a single owner for development, review and evaluation. At the national and organisational level, officials and any other appropriate party should be designated to help develop, spread, and review standards and policies. The reviews will help provide recommended improvements or changes needed according to law, and organisational and technical structures. The reviews should also consider feedback from interested parties, the status of preventive and corrective actions, trends related to threats and vulnerabilities, reported incidents and actions taken to respond and recover from cybersecurity incidents.

According to Peltier (2013), security controls are aimed at identifying the potential threats and vulnerabilities, while an information security policy is a plan identifying the organisation's basic assets with detailed illustration of what is acceptable, unacceptable and logical behaviour from the stakeholders to ensure information security in an effective manner. The plan must consider the performance level of the e-government programme, which when evaluated will help achieve success with respect to the security measures (Chen et al., 2013).

Based on the national cybersecurity strategy of the government in Jordan, information security policies should:

- Assign and define information security classification levels required for the government organisations;
- Comply with Jordanian laws and adopted international standards;
- Define organisational roles and responsibilities;
- Define policy distribution, training, and implementation timelines;
- Provide compliance and certification procedures;
- Provide procedures for corrective actions for non-compliance.

The data analysis has reported that those responsible for the information security framework of the e-government programme will have to put more effort into proactive security test for information resources as same as cybersecurity incidents response.

Thus, the efforts of implementing national cybersecurity standards and policies will be assigned or managed by the e-government programme. The managers at e-government programme should ensure the compliance with these standards and policies by government organisations. To do so, they need to have a flexible organisational structure in which development, review, evaluation and audit are assigned to responsible departments, such that segregation of duties is maintained. Information security policy must be developed, regularly reviewed, periodically updated and enforced to meet optimum information security requirements for government organisations (Mohajerani et al., 2015).

Theoretical condition C7: The e-government security framework must consider a national information security policy and communicate it to provide direction and support for the information security strategy, relevant laws, regulations and international standards.

4. Legal and Regulatory Regime

The analysis has revealed the need for empowering laws and regulations to support and enforce the implementation of the cybersecurity strategy for the Jordanian e-government programme. The e-government programme, as mentioned in the findings, need to create a committee formed with members, information security specialist from the MoICT and Ministry of Justice experts to conduct legal reform and provide recommendations. More importantly, and as an urgent requirement, government organisations need to have regulations that are consistent with those developed laws to cover information security-related legal issues. The cybersecurity approach

has to deal with cyber regulations in different fields, such as e-commerce, e-banking, and e-government. This depends on the governance of cyberspace to control the use of the web as a medium to promote e-services without risk (Hassan & Khalifa, 2016).

Cybersecurity should be managed at the highest levels of government and as a top priority. Tassabehji et al. (2007) assert that to evaluate the security of the e-government programme it is a critical need to examine related laws, regulations and policy as security measures.

Theoretical condition C8: The e-government security framework should incorporate ensuring that security related laws and regulations are in place as a fundamental element that can be activated as required.

5. Risk Management/ Assessment

Another element that must be considered at the formal level of the information security framework is risk management. The government of Jordan has still not established an effective framework for threat analysis and risk management at the national level. Additionally, it is important to realise that there is no fully secure information system, network or single security application/mechanism that can address all security issues and clear all vulnerabilities. Thus, developing sufficient disaster recovery plans for government organisations/ departments by effective risk management is essential. The analysis has shown that e-government administrations need to introduce a framework based on both technical and non-technical dimensions for risks assessment.

In this respect, Evangelidis (2005) describes a framework for risk assessment and modelling in e-government services. This provides an approach for effective risk assessment in e-government services. The main aims of this framework are to provide a holistic view of e-government transactions and enable the decision maker in assessing the risks involved in the development of the electronic transaction. Government electronic transaction is considered as a socio-technical system consisting of two interdependent subsystems: the social subsystem (the structure, communications and people aspects) and the technical subsystem (the technology and the required tasks). The risk assessment process within that framework consists of the following stages: context establishment, risk identification, risk analysis and risk evaluation. Zhou and Hu (2008) set out the procedures of e-government security risk management according to three steps: risk identification, risk analysis and risk control.

Indeed, strengthening risk management is an effective way to guarantee the security of the e-government system. Among e-government risk management countermeasures, it is popular to use a defence-in-depth strategy, which relies on multi-level security. In other words, this involves putting into place multi-level security protection to guarantee that if one level becomes compromised, other levels can still ensure the security of e-government system resources. For instance, if the outer firewall of one government organisation gets penetrated, the intruder cannot gain access to sensitive data or damage them because of inner firewall protection.

In brief, the relevant literature shows that many studies have attempted to categorise risks according to their nature, such as: social, operational, economic, political, technological and security (Blakley et al., 2001). From various e-government frameworks have been examined where the researchers provides the foundation for risk assessment criteria, a suitable one could be used within the e-government programme in Jordan. Basically, three fundamental stages of risk management/assessment must be followed by the Jordanian e-government programme. First, risk identification to recognise risks that exist in cyberspace or data exchange. Risk identification could be not able to find all the e-government system risks, but only find the already known risks or potential risks. Hence, risk analysis and risk control is required to solve or reduce most other unknown risks. There are many different ways of identifying risks: semi-structured interviews, brainstorming, checklists and other suitable qualitative techniques. Second, risk analysis to estimate both the probability of the occurrence of a risk and the extent of the impact if the risk happens. In addition, in the process of risk analysis, it is important to identify threat sources, including people, computer systems vulnerabilities and so on, which can potentially harm the information system. Third, there needs to be risk controlling/ evaluation to determine whether risk management is successful or not and ensuring that it can be reduced to an acceptable level. This final stage is to decide what sort of qualitative risk assessment approach is more suitable, as well as the initial presentation of the risk assessment area to the stakeholders. In the e-government programme, in respect of security risk management, managers need to follow those steps as a major part of the information security framework.

Theoretical condition C9: The e-government security framework must cover risk management in terms of identifying, analysing, and controlling the potential risks within e-government systems and services.

5.2.2.3 Informal Level

The informal level of the proposed information security framework consists of human aspects. The first subsection below discusses cybersecurity awareness and training for government employees. The second subsection is focused on citizens' awareness and education in relation to security issues as the users of e-government services.

1. Government Employees

The urgent need to conduct cybersecurity training and awareness courses periodically for government employees in Jordan has been ascertained through the data analysis. At present, cybersecurity awareness and training are virtually non-existent. Hence, the government needs set up a staff capability building programme after consultation with academia and international partners in order to increase the degree of security training and awareness. In addition, review terms and conditions in employee contracts regarding their responsibilities for information security and acceptable use of digital assets are required. Enhance employees' cyber-culture also will support the security requirements of government organisation during their work and reduce the risk of human faults to the minimum level.

There has been some little focus on the non-technical aspects in information security approaches/frameworks in the context of e-government (Wang, 2008). Many studies have identified the lack of security awareness and training as one the main issues that can have a considerable impact on the management and implementation of information security in e-government (Reffat, 2003; Robertson, 2010; Wangwe et al., 2012). A study by Hansche (2001) holds that most current security training and awareness programmes are not working as they are supposed to. Similar findings have emerged from the current study in that not enough attention has been given in the e-government programme of Jordan to the development and management of security awareness activities.

Moreover, the findings for this study reveal that most of the cybersecurity incidents occurred because of non-malicious, simply careless behaviour of employees and that security awareness plays a key role in formulating a strategic view of information security, as same as in the study of Al-Jaghoub et al. (2010). However, some researchers have reported that many governments putting efforts in this context and run cybersecurity awareness and training programme for their

employees. The researchers also discussed the obstacles and problems facing those initiatives (Harris, 2010). Jordan's government needs to put in place number of initiatives and programmes, in particular, for information security training and awareness, like those suggested above in order to provide the required level of understanding on how government employees can maintain information security. This aspect, which is critical in information security framework, can be discussed from different themes (political, social, organisational and technical) as below.

- ***Political theme***

For e-government programme in Jordan, the top management support is a fundamental requirement for establishing a successful awareness and training programme. In the relevant literature, researchers point out the importance of top management fully understanding the strategic objectives of e-government and the targeted outcomes (Hansche, 2001; Dhillon & Torkzadeh, 2006). By doing so, the support of the top management will able them to implement the e-government programme related projects with more confidence.

As Conklin and White (2006) point out, when implementing e-government projects, financial issues are a common obstacle to the development of successful e-government programme, as the funding comes from the government where political issues play a significant role. Providing the needed tools and resources to develop and implement a cybersecurity awareness and training programme is dependent on top management commitment. Hansche (2001) identifies the assurance of financial resources as one of the key barriers for an effective security awareness program. This accords with the general problem in the e-government programme in Jordan of convincing top management to invest in the information security issue. Moreover, Kotulic and Yildiz (2007) highlight a common mistake of many e-governments project, as in any organisation project, that most risks, threats or vulnerabilities do not get assessed until after a security incident has occurred, as was emerged from my case study findings. As a result, information security awareness and training initiative should be proposed in terms of a consistent project plan of Jordanian e-government security framework.

- ***Social theme***

From the social perspective, the analysis of the data indicated that the ethics and personal values of government organisations/ departments have a significant influence on the success of a security awareness effort. Zhongping et al. (2013) note that users' (employees) personal ethics

and values are considered as a critical success factors for cybersecurity awareness initiatives, because conflicts will arise, if the employee's values and those of the organisation are not in line. Harris and Richmond (2006) also argue that "morals and ethics critically affect users' motivation to act in a security-conscious way".

As cybersecurity awareness and training initiatives within the e-government programme need to target a wide range of users, they should not be designed and planned without the participation of different information systems stakeholders. Currently in Jordan, cybersecurity awareness and training efforts in e-government engage mainly the IT department, thus ignoring the staff members from all other departments within government organisations. It is a high priority as well to stimulate the information security consciousness of top management. Bulgurcu et al. (2010) suggest the involvement of IS stakeholders in cybersecurity awareness and training initiative from all levels of authority: the board, executive management, middle management, technical, security management and end-users. May and Lane (2006) also support this argument, opining that when top management launches an awareness programme, line managers should be engaged, otherwise most employees probably will not change their behaviours. As most of awareness efforts are commonly believed to target end-users in the first place, engaging all the organisational hierarchy should also be considered for more effective information security approach.

- ***Organisational theme***

From an organisational point of view, the information security training and awareness programme should be located within a security management scheme and a broader organisational context. According to this research case study's findings, top management need to consider the establishment of an information security department in all government organisations as a prerequisite to launching information security awareness and training programmes. This will have evident influence, in particular for public administration agencies because of bureaucratic organisational changes which basically related to authorities' distribution. Katsikas (2000) supports this argument, contending that the organisational structure has a significant impact on implementing a successful information security awareness and training program. In the Jordanian e-government programme, various awareness design and implementation roles and responsibilities for realising the awareness initiative were allocated to the NITC. The information security awareness and training programme should be closely related to business and security policies, practices, and procedures. The importance of

aligning information security awareness and training with the information security strategy is highlighted by Zhongping et al. (2013). The empirical data analysis shows that the lack of adequate security policy practices is a leading cause of poor information security awareness and training levels among government organisations. The lack of managing information security awareness and training programmes as formal projects with formal objectives and resources led to a failure to achieve the desired goals (Zhao et al., 2012). The empirical findings emerged the e-government programme need for a project plan involves the objectives, cost estimates, time schedules and deliverables planned in order to ensure top management commitment and financial support for security awareness and training initiative.

- ***Technological theme***

Excluding the posters, leaflets and security artefacts, in Jordan's e-government case study the proposed information security awareness and training actions were found to include various methods of technical development or integration, like the creation of mailing lists and automatic updates, promoting security forums and a periodic newsletter. Technical support has a key role to play in information security awareness and training programme implementation, as reported by Benlian (2015). As data analysis report in the context of information security management, there is no feedback mechanism at place enabling government employees to present their opinions, suggestions and concerns. The e-government programme of Jordan is facing a number of difficulties to do with the technological changes as a result of the partial implementation of the information security awareness and training plan. In this respect, the appropriate use of ICT standards and systems integration can provide the required support towards the successful implementation of the e-government security framework.

Theoretical C10: The e-government security framework must have a sufficient plan for security awareness and training initiatives for the governmental workforce at all organisational levels.

2. Citizens

In Jordan, the government needs to put in place more serious efforts towards cybersecurity awareness for the public. Despite the fact that cyberspace can offer an unlimited number of services, these services are accompanied by many risks as well, of which many Internet users are not aware. Many countries have developed and implemented cybersecurity awareness and

training initiatives to counter the perceived unawareness of the citizens and other stakeholders (E-government-Jordan, 2017).

Regarding other countries' initiatives towards promoting cyber-security awareness and training, Kortjan (2014) conducted a comparative analysis of four developed countries (the USA, the UK, Australia and Canada). They found that, in these countries, the primary purposes of such initiatives were to protect the national critical infrastructure and as a tool for accomplishing its cybersecurity objectives. Cybersecurity awareness training should be an essential part of high-level cybersecurity objectives within the national cybersecurity policies. In the paper, it was concluded that the main reason behind cybersecurity awareness and training efforts may vary from country to another. Hence, it seems reasonable to argue that Jordan should consider cybersecurity awareness and training in its own context, to get the desired benefits. The goal of cybersecurity awareness and training is to enhance the level of awareness in the nation on the risks of cyberspace, support individuals and businesses, by informing about and educating them on the issue (Alshboul, 2012). The government of Jordan's ultimate goal is an online culture that could be fostered through awareness and education programmes or initiatives.

The cybersecurity awareness and training initiatives have been assigned to NITC. This allocation of responsibilities boosts accountability in addition to providing a focal point. Therefore, it is important to exist a dedicated administration that could work as a focal point for cybersecurity awareness and the implementation of training initiatives (Al-Jaghoub et al., 2010). Indeed, there should be a strategy in place that clearly explains how the e-government programme in Jordan should approach cybersecurity awareness and education for the public.

The initiative of establishing Knowledge Stations (KSs) is one of the most interesting initiatives of the government of Jordan. This is helping it with e-government implementation by creating universal access to ICT for all citizens as part of the efforts to raise the level of online culture. As the findings clarified, 196 Knowledge stations have been distributed throughout the different regions over 15 years, conducting various computer field related training courses and other services for the public. Whilst about half of the citizens would appear to know about the knowledge stations in their areas, only very few of them have benefited from the services provided (E-government-Jordan, 2017).

The analysis indicates that there are two main roles at stations for enhancement of awareness within the public in an online environment; developing ICT capabilities for citizens and cure computer illiteracy of local people. To fulfil these roles, the stations offer IT training courses, ICT capacity building, socio-economic activities, and Internet access. As mentioned before, the knowledge stations help to enhance the subjective security concept. The citizens can visit these stations to get the help and knowledge they need to use e-government services securely by qualified staff, which can change their information security perceptions and enhance the online culture of the public. The stations are playing a key role in promoting e-government services to citizens. Citizens demand knowledge as a condition to using e-services and staff of stations are qualified to provide this.

Welch et al. (2005) defined the criteria that should be used by the government to analyse such initiatives in order to evaluate their performance, identifying the following elements.

- Host organisation: The department or organisation that will be leading the initiative.
- Target audience: The grouping of people that the initiative targets.
- Topics covered: The topics that are covered by the content of the initiative.
- Campaign tools: The methods that are to be used to deliver the message.

At the end, cybersecurity awareness should be a shared responsibility; and every individual using the cyberspace has a role to play. It is evident, in all cases that have been studied, that the governments were core in leading and resourcing cybersecurity awareness and training initiative. Knowledge stations (KSs) have been built on the partnership approach between several organisations from the public and private sectors in building, hosting, managing and implementing this initiative (Knowledge Stations, 2004), which include NITC (manage KSs under the umbrella of NITC), a royal committee, city councils, King Abdullah's development fund, among others. From the investigation into the various challenges and obstacles of knowledge stations, this study extrapolated the key aspects that form a solid infrastructure for awareness and education initiative for public in Jordan, particularly through knowledge stations.

There has been always a need for programmes, initiatives as well as campaigns to promote e-government to achieve better participation among various stakeholders for successful implementation. The campaign that motivates and raises awareness of government e-services related to security issues should be a part of e-government security framework.

Theoretical condition C11: The e-government security framework must cover cybersecurity awareness and education initiatives for the public aimed at making individuals aware of the risks and know how to protect themselves online.

5.3 Cybersecurity and online trust

5.3.1 Introduction

This section consists of two main subsections that are answer the rest of the research questions.

- *Why is the government of Jordan not attempting to enhance citizens' online trust by communicating (elements of) security countermeasures in their e-government programme (technical/formal/informal)?*
- *What are the citizens' perspectives and perceptions about the security of the e-government programme and how does this affect their adoption of e-services (online trust)?*

The first subsection clarifies the main obstacles the e-government programme is facing that led to a lack of citizens' trust in e-government services and the steps that have been taken by the government to address these. The second subsection shows the extent to which those security-related problems that affect citizens' security perceptions and trust, by linking the interview data analysis with that of the survey.

The trust obstacle has a very clear impact on the acceptance of e-government services in Jordan. The trustful relationship between e-government and different stakeholders relied on how convince is the government infrastructure to them. In other terms, the e-government authority on the other government organisations/ departments providing the e-services, how they monitor, audit and review their information security compliance (Dhillon & Torkzadeh, 2006).

It is essential to have a high level of information security training and awareness by educating government employees about the security policies, practices, competencies, addressing the main objectives of information security. This will help in obtaining a high level of confidence and trust in government organisations because that means the transactions are responsible and observable to the authenticated user and very hard to be denied later on (Dhillon & Backhouse, 2000).

The linkage to online trust is a key contribution also in this research and a part of the proposed security framework. This trusted framework can be built through the technical, formal and informal elements of the information security approach. For example, using industry solutions for online trust and security (e-security technologies). In addition, look at trust issue as a formal part of information security policy and focus on security awareness and training initiatives at the informal level (Ahlfeldt et al., 2007).

5.3.2 Government steps

Building trust through technical/ digital authentication

According to the findings, there have been many obstacles to implementing the national cybersecurity strategy of 2012 in Jordan, most notably in the area of using the latest security technologies. As the interview data have shown there are a few related projects that are in progress in order to update the technical infrastructure, including: an army cybersecurity project, SGN upgrade, private cloud development and the smart card project.

When discussing information security within cyberspace it is needed to shed light on maintaining online trust. As mentioned within the relevant literature review, many researchers (Greene, 2006; Zhao & Zhao, 2010; Ashaye & Irani, 2014) have pointed out that addressing information security within e-government infrastructure and services is crucial to preserve trust among stakeholders to exchange information over the e-government systems and network. The concept of trust involves the belief that other users could misuse or take advantage of critical information and put e-government resources at risk. Thus, the proposed framework needs to clarify the link between technical aspects and citizens' trust.

Inconsistency with the findings of this research, Zhou and Hu (2008) highlight that a unified and centralised identity authentication in e-government will help to handle citizens' data and critical information via single account. At the same time, the researcher brings up the matter that a single sign-on could raise the risk of account spoofing attacks. Furthermore, Hassan and Khalifa (2016) have proposed a technology framework for online trust consisting of: a Digital Envelope (symmetric encryption, public key encryption. biometrics, hardware security modules); a Digital Signature (hash algorithms, key exchange, public key encryption); a Digital Certificate (creating digital identities, a basic component for building security and trust for ICT applications in public networks).

Table 14: Industry Solutions for Online Trust and Security

Common e-security technologies				
	Authentication	***Confidentiality***	***Integrity***	***Non-repudiation***
Anti-virus			✓	
Firewalls	✓	✓		
Access control	✓	✓		
Encryption		✓		
Public key infrastructure	✓	✓	✓	✓

The literature review has identified several technical factors for investigating the level of the citizen's trust in interacting with government organisations/ departments electronically, including service and information quality, lack of integrity as well as privacy and security of the website infrastructure. Alexander (2003) shows that these technical factors can negatively influence citizen's belief that the used technologies within e-government systems and websites will provide secure e-services, accurate information and ensure safe e-transactions.

In general, the e-government programme of Jordan needs understand cultural or social aspects and study citizens' characteristics according two themes: trust in the government and trust in the Internet. Mohajerani et al. (2015) study listed the determinants of e-government trust as: age, perceived usefulness, perceived quality, risk perception, privacy concerns, perceived organisational trustworthiness, trust in technology, propensity to trust, years of Internet experience, Income, education and gender.

Theoretical condition C12: The e-government programme must consider technical factors of the security framework that positively influence citizen's belief that the used technologies within e-government systems and websites are sufficient to provide secure e-services and safe e-transactions.

Building trust through formal/ organisational factors

At a formal level, the analysis has revealed the obstacles that the e-government programme of Jordan is facing, which are: the bureaucracy in procedures and process, weak top management support, weak marketing and media efforts, poor level of compliance and the lack of a cooperation plan. All of these have been identified as factors that have led to a lack of citizens' trust in the ability of the government to provide effective and secure services for them.

As Colesca (2009) demonstrates, citizens' confidence in their governments relies on their confidence in the performance of different government departments. Many researchers (Tolbert & Mossberger, 2006; Tassabehji et al., 2007; Mohajerani et al., 2015) agree that trust in the government refers to the citizens' perceptions of the ability and integrity of governments to provide security services to their citizens, which is a significant dimension for the successful adoption of e-government services. In e-government research, it is evident that the reputation of government organisations and departments can influence the trust in how secure government services and transactions are (Lamsal, 2001; Molnár & Kő, 2009; Shajari & Ismail, 2012). In the context of information security, organisational reputation means that the citizens' believe that the organisations are capable of protecting their' information and providing services in a secure manner. Hence, government organisations in Jordan should work on solving all security related managerial and administrative issues with the aim of building a good reputation. They need to be perceived as being concerned about their information assets by acting effectively and efficiently. Moreover, Benbasat et al. (2010) note the impact of bad previous experience with a government department website on trust in e-government. That is, the way information is obtained through a previous experience influences citizens' confidence in using government e-services (Lamsal, 2001).

To deliver the government's information security strategy successfully in Jordan, requires demonstration of a commitment by government organisations/ departments to improve cybersecurity. According to my empirical findings, the renewed strategy 2018-2023 clarifies the strategic aim of delivering a safe information security environment in the national interest, which would enhance citizens' online trust on e-government services. Indeed, as organisational issues such as performance and service quality play a key role in building positive perceptions among citizens about how government organisations secure their systems and resources, this is a critical part of the proposed framework.

Theoretical condition C13: The e-government programme should work on solving all managerial and administrative issues related to information security to build a good reputation by acting effectively and efficiently which will enhance citizens' trust on government e-services.

Building trust through informal/ human factors

The analysis confirms that cybersecurity awareness and training could be the main determinant of online trust. Providing stakeholders with general information/ knowledge that foster citizens' perspective of cybersecurity which in result enhance their online trust on e-government services. From the existing literature, it can be seen that the citizens' characteristics (culture, beliefs, values, ethics, education) significantly affect their online trust in e-government services and their attitudes towards cybersecurity. A number of researchers (Carter & Bélanger, 2005; Al-Jaghoub et al., 2010; Howarth, 2014) have highlighted the security risks and Internet experience as important factors that affect citizens' trust in using e-government services.

As mentioned before, the knowledge stations initiative is the most important step that has been taken by the government of Jordan on this topic. However, owing the obstacles facing it, it resulted in partial failure. Based on the analysis, the key issues the government needs to address to gain the maximum benefit from knowledge stations are lack of funding, the absence of top management support and weak marketing efforts. Consequently, the government of Jordan has to present all required support for knowledge stations initiative to success due to its significant role in enhancing citizens' online trust through security awareness and education.

A study of McKnight et al. (2000) support the perspective that most individuals require having some security-related information about online services before placing their trust in them. Many studies highlight the security issue as an important factor influencing trust in e-government (Hansche, 2001; Carter & Bélanger, 2005; Carter & Weerakkody, 2008) . In addition, some researchers have reported that Internet experience, awareness and education can affect one's willing to trust in Internet technology (Colesca, 2009).

Theoretical condition C14: Part of the e-government programme should be conducting security awareness and education campaigns for the public in order to enhance their online culture and knowledge, which in turn, would improve their trust in government e-services.

5.3.3 Jordanian citizens perceptions of e-government security

This subsection discusses the findings of the survey, as a complementary phase. It is an attempt to link citizens' cybersecurity perceptions to their trust in e-government services. In fact, in many developing countries like Jordan, as most of the public is not experienced with IT and not familiar with online services, security concern is high with respect to potential risks either from governments themselves or hackers.

In their study, Carter and Bélanger (2005) confirm that advertising the benefits or security features of services to citizens would build trust between users and departments in terms of e-services' efficiency, reliability, dependability and capability. In fact, this is what the government of Jordan needs to focus on. The survey results have shown that 45.5% of the respondents did not use e-services, because they did not know about it, whereas 57.8% of them do not try to use the new available e-services. This is in line with the interviews findings regarding insufficient media and marketing efforts. Such advertising for e-services would have a positive impact on citizens' understanding of the e-government programme efficiency.

In addition, the survey analysis indicates that 27.8% of respondents, moderately, did not trust or use e-services because of negative perceptions or beliefs about them and 24.4% of them were influenced by their relatives, family members and friends' negative perceptions and beliefs. As the interview analysis has revealed, online culture, citizens beliefs and mentality has been considered the key obstacles influencing citizens security perceptions and as a consequence, their trust in government e-services. The relevant literature states that the users of e-government services and websites will probably recommend the use of e-government services to others after experiencing its applications working effectively (Carter & Weerakkody, 2008). As a result, this could help to increase the trustworthiness of the service provider (government organisations) among citizens.

Furthermore, security training and awareness would increase users' experience and knowledge of e-services, in particular about security issues in cyber space. Hence, they would recommend its use to others who may have negative perceptions to use e-government services. The survey analysis confirmed the interviews findings that the lack of security training and awareness has led to poor trust in e-government services. It is surprising that 84.6% of respondents did not know about knowledge stations. It is really problematic that such a wide ranging initiative is

not being utilised sufficiently as, based on survey analysis, 59.1% of respondents do not really perceive government systems and websites to be trustworthy. In addition, 37.4% of them perceive e-government services to be not secure. Katsikas (2000) points that despite enhancing awareness of security threats in cyber space is a recognised challenge, little effort has often been made in ensuring that attached information is provided to the citizens to make the decision to use the e-service.

The last research question is to do with examining how cybersecurity perspectives affect citizens' trust in e-government services and the survey analysis revealed problems in the current information security approach, as had been mentioned previously during the interviews, which was negatively impact on their trust. Table 15 below presents the linking the security elements mentioned previously with the surveys finding regarding citizens online trust.

Table 15: The link between security elements mentioned previously with citizens online trust

Security Aspects (technical, formal, informal) that affect citizens' security perceptions, and online trust based on the interview findings	**Survey Findings**	**Percentage of Respondents**
Technical factors (e.g. technical errors)	Citizens do not trust e-services due to the technical errors, which make them feel the systems/ websites are not secure	35.2%
Formal factors (e.g. media, advertising, organisations performance and cooperation)	Citizens do not use e-services because they don't know about these services, owing to insufficient media and marketing efforts	45.5%
	Citizens do not try e-services that they haven't used before (experience)	57.8%
	Citizens do not contact the complaints call centre or help desk (organisations performance)	81.6%
	Citizens do not fully trust e-services because they don't trust the government and	44.3%

	hence, are wary about sharing data online with them	
	Citizens do not trust the e-payment gateway	43.5%
Informal factors (e.g. awareness, education, beliefs and culture)	Citizens who moderately have negative perceptions of e-government programme	27.8%
	Citizens do not trust e-services because they are influenced by negative online culture	24.4%
	Citizens do not know about knowledge stations (KS) and available security awareness and education	84.6%
	Citizens do not really perceive government systems and websites to be trustworthy	59.1%
	Citizens perceive e-government services to be not secure	37.4%

The respondents of the survey in the second phase at this research, declared that the level of trust in e-services was related to different security technical and non-technical aspects within the e-government programme. In Jordan, e-government programme managers have to realise that their information security approach success depends on effective compliance and commitment from government organisations with basic cybersecurity standards, policies, procedures and rules. In addition, as mentioned before, cybersecurity awareness and education have a critical role to play in equipping Jordanians in protecting themselves online. Moreover the government needs to ensure that is has qualified staff with the required skills for protecting the national information resources security from various types of cyber-attacks. If this were the case, then public trust in e-government services would be greater. Overall, the proposed framework clarifies the relationships and connections between different security aspects and citizens' online trust, from which the government of Jordan can determine the areas it should be focus on.

5.4 The Proposed Framework for Securing E-government

In this section, firstly, a table covering all the theoretical conditions is presented. That is, the following table 16 clarifies the theoretical conditions for different security aspects at the technical, formal and informal levels that form the proposed security framework, as extracted from my data. In addition, there are number of general conditions that illustrate the relations between levels and linkage to online trust. This is followed by a diagram explaining how these theoretical conditions are connected and how they are indicated in the framework (see Fig 17). Next, the proposed security framework is visually presented, in order then to justify it and discuss its implications.

Table 16: Theoretical Conditions

Theoretical conditions to be satisfied	How other models/frameworks deal with that condition	My empirical data and how they support or extend other theoretical models/frameworks	Example/ Relevant References	Indication in the model
C1: for the e-government security framework, RBAC must be used as it is the most suitable access control mechanism for ensuring the reliability of government department data and reducing the risk of unauthorised revelation of information.	The RBAC model has been recommended as an effective measure to resolve resource unified access control of large information systems by the public. The RBAC involves users, roles, constraints, permissions, and sessions. It presents the idea of roles between users and access permissions. Moreover, a user connects with one or more specific roles, and a role connects with one or more permissions, with roles being created or cancelled according to actual working requirements.	My constructs of effective access control mechanism bear similarity to the RBAC model. Basically, the RBAC focuses on the relationship between the users and information resources based on their roles. However, RBAC also needs to show the relationship between users and roles. When the role of a user changes his/her permissions must be cancelled or changed.	The Access Control Policy Study of E-government Information Resource Based on the RBAC Model (Zeng Zhongping, Li Zonghua, Lu Xinhai, 2007).	T1
C2: E-government security framework must engage with the latest security software and applications, which should to be updated regularly in order to prevent, detect and handle different security attacks.	The security readiness evaluation framework is concerned about the factors that could lead to vulnerability and risk to the security of e-government initiatives. This framework contributes to security-readiness evaluation	This framework has a similar aim to my study, discussing technical infrastructure for e-government security. Nevertheless, in my study, how IT leads to different performance outcomes and the importance of regular ICTs	Security Readiness Evaluation Framework for E-government Initiatives (Lutui, R., Hopoi, S. & Maeakafa, S., 2017).	T2

	in developing countries to guide the implementation of e-government initiatives.	updating so as to be able to use the latest security technologies, which will increase confidence amongst citizens in government e-services have been added.		
C3: The e-government security framework needs systems interoperability to allow for the public administrations to have a unique interface for the solution of a number of complex problems.	This shared framework shows that different organisational problems facing e-government can be partially solved with the introduction of a Shared Services Centre (SSC). "ICT outsourcing" in "Shared Services" can significantly support the development of e-government processes.	My study differs in view the impact of systems interoperability on information security. A concentration of resources and activities within a centralised approach is vital for e-government security management effectiveness and will have a direct affect to satisfy citizens.	Shared Services Infrastructure for E-government (Corradini, F., Polzonetti, A. and Riganelli, O., 2018).	T3
C4: The e-government security framework must involve a secure government network to connect all government organisations and protect their websites and information systems under a central approach.	Many studies have explored different security dimensions within the e-government network context, such as secure communication (1), trust in the use of personal information by the government workforce (2) as well as technical infrastructure and information privacy (3).	My study involves all different dimensions of government network, organisational and technical. Centralisation of information infrastructure for all e-services providers is proposed to improve the trust of citizens by using a single gateway and focusing on using security applications, like PKI and firewalls.	(1) (Hasan & Abuelrub, 2011) (2) (Abu-Shanab and Baker, 2011) (3) (Rotchanakitumnuai, 2008)	T4
C5: The e-government security framework must consider e-services reengineering and building an integrated framework for effective information security management.	Integration framework proposed for the implementation of various administrative procedures that require interaction among several government departments. This framework highlights the importance of	In my study, I suggest this framework to integrate a large number of information systems in a way that makes different government departments able to interact with each other, sharing process, activities and services securely. This	Towards service integration in electronic government implementations (Asa'd et al., 2016).	F1

	service integration in e-government implementation.	integration will reduce different problems related to information security issues and increase the services quality.		
C6: The e-government security framework must provide secure gateways for internal and external communications among government departments and with other stakeholders (citizens and businesses).	The proposed architecture framework for e-government adoption will reduce confusion surrounding e-government infrastructure in the public sector through understanding the implementation processes, identifying requirements of information and communications areas. Besides this, highlighting the importance of organisations resources management.	The need for common infrastructure for interconnecting the information systems of different government administrations has been confirmed by my findings regarding a general overview of cooperation among government organisations. The different communications areas in e-government (G2G, G2B and G2C) have been considered in my study to identify the security threats and suggest security solutions. The novelty of the investigation has been to focus not only on the technical part, but also on the organisational one.	E-Government-an Information Security Perspective (Hassan & Khalifa, 2016).	F2
C7: The e-government security framework must include a national information security policy, update it and communicate it to provide direction and support for the information security strategy, relevant laws, regulations and international standards.	The list of security requirements has been compiled by adopting an organisational framework that facilitates the classification of e-government services according to the security requirements they need. The security policy is considered as being a mandatory security requirement for an e-	My study discusses that I have argued that information security standards and policies should be reviewed at planned intervals to accommodate for the rapid change in the cyberspace environment, thereby ensuring cybersecurity effectiveness. In addition, information security standards and policies should also have a	Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy (Costas, et al., 2003).	F3

	government infrastructure. It should ensure that all information resource users comply with the rules and guidelines relating to information security.	single owner. It is practical to develop a uniform, applicable and easily expandable security policy for e-government infrastructure.		
C8: The e-government security framework should incorporate ensuring that information security related laws and regulations are in place as a focal element that can be activated as required.	Many studies have stressed the importance of information security laws and regulations to ensure high levels of compliance. Moreover, these present another potential fundamental difference between developing countries and developed countries in terms of the existence and absence of the necessary regulations and laws that criminalise cyber-attacks and enable governments to adequately investigate and prosecute such activities.	My data supports that the government of Jordan needs to have legal reform to develop the required information security laws. There is a critical need to examine laws and regulations as a security measure which could be used to take action against the misuse of ICT resources. The existence of relevant regulations and laws has an impact on the effectiveness of e-government security management.	State of ICT Security Management in the Institutions of Higher Learning in Developing Countries (Bakari et al., 2005).	F4
C9: The e-government security framework must cover risk management in term of identifying, analysing, and controlling the potential risks within e-government systems and services.	Framework for risk assessment and modelling in e-government services provides an approach for risk management in e-government and should be evaluated within collaborating government departments.	My empirical data show that e-government administrations need to adopt an effective risk management approach based on both technical and non-technical dimensions. This framework could be used to identify different risks and threats within e-government systems and services in Jordan.	FRAMES–a risk assessment framework for e-services (Evangelidis, 2004).	F5

C10: The e-government security framework must have a sufficient plan for security awareness and training initiatives for the governmental workforce at all organisational levels.	The studies show that skilled staff and adequate continuous security awareness and training programmes have been recognised as an important factor for the success of an information security approach. Moreover, they point out that increasing the level of computer skills through training or ICT specific education can help in improving managerial perceptions of ICT initiatives within public organisations.	In my study, the findings show that many security incidents occurred due to employees' individual faults and lack of knowledge. Based on the empirical data, insufficient skills and training can lead to misuse of the electronic information resources and potential security attacks. The qualified employees with the required skills and knowledge will support the implementation of the information security framework.	Reinventing local governments and the e-government initiative. Public Administration Review (Ho, 2002).	I1
C11: The e-government security framework must cover cybersecurity awareness and education initiatives for the public aimed at making individuals aware of the risks and know how to protect themselves online.	User awareness is always viewed as a focal component and challenge in any information system, and a significant issue in the context of e-government security. Cybersecurity awareness and education framework for public proposed that would assist in encouraging citizens to adopt e-services and be familiar with.	My data support that there should be a strategy in place that clearly clarifies how the e-government programme in Jordan should approach cybersecurity awareness and education for the public. The government of Jordan's ultimate goal is an online culture that could be fostered through awareness and education programmes.	A conceptual framework for cyber-security awareness and education in SA (Noluxolo Kortjan, Rossouw von Solms, 2014	I2
C12: E-government programme must consider technical factors of the security framework that positively influence citizens' belief that the used technologies within e-government systems and	A technology framework is proposed for online trust, which consists of: a Digital Envelope (symmetric encryption, public key encryption. biometrics, hardware security modules); a	Based on the survey findings, technical errors or systems faults may impact negatively on citizens' perceptions about how capable are the government systems, websites and network of dealing with	Building Trust and Confidence for Critical E-government Services, ITU Telecommunication Development Bureau (BDT), (Alexander, 2003).	O1

websites are sufficient to provide secure e-services and safe e-transactions.	Digital Signature (hash algorithms, key exchange, public key encryption); and a Digital Certificate (creating digital identities, a basic component for building security and trust for ICT applications in public networks).	critical information securely. Using different security mechanisms listed in the technology framework may decrease the number of those technical errors, thereby having a positive impact on citizens' online trust.		
C13: The e-government programme should work on solving all managerial and administrative issues related to information security to build a good reputation by acting effectively and efficiently which will enhance citizens' trust on government e-services.	In e-government research, it is evident that the reputation of government organisations and departments could influence the trust in how secure are the services and transactions.	In my study, organisational issues, such as performance and service quality, have been found to play a key role in building positive perceptions among citizens about how government organisations secure their critical information. Based on my analysis, to deliver the government information security strategy successfully in Jordan requires demonstrate of commitment by government organisations and departments to improving cybersecurity.	Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions (Beldad et al., 2012).	O2
C14: Part of the e-government programme should be conducting security awareness and education campaigns for the public in order to enhance their online culture and knowledge, which in turn, would improve their trust in government e-services.	A number of researchers have highlighted the security risks and Internet experience as important factors that affect citizens' trust in using e-government services. Moreover, they have proposed several factors that when taken into consideration can increase citizen trust and thus,	From a different point of view, my data shows that the lack of security awareness and knowledge might influence citizens' willingness to use government e-services. Encouraging citizens to use government e-services through security awareness and education will increase their	Encouraging Citizen Adoption of e-Government by Building Trust (Warkentin et al., 2002).	O3

	encourage the adoption of government e-services. The proposed e-government adoption model considers culture, experience (familiarity) and technology acceptance as being such factors.	familiarity (experience) and subsequently, their trust in these e-services.		
C15: Formal aspects involve considering effective and sufficient technical matters that will manage, control and protect.	Researchers found that numerous activities of management, particularly those security related, rely on IT infrastructure and alignment and human resources management, which have a significant impact on the quality of management of information security. Some have argued that a more holistic approach to information security is needed and suggesting ways in which managers can play an effective role in information security.	In my study, the proposed framework highlights the interrelation between different levels. The main purpose of the aspects at the formal level is to manage, control, monitor and review the technical aspects. The technical aspects cannot work in a sufficient manner and be useful without effective management at the formal level.	Information security management needs more holistic approach: A literature review (Soomro, Z.A., Shah, M.H. and Ahmed, J., 2016).	R1
C16: Formal aspects must take informal aspects into account and improve security awareness, skills and education to mitigate potential risk and threats.	Researchers have suggested that information security management is about more than just processes and must relate to human behaviour. A small number of them have repeatedly suggested that there is a need to obtain a better understanding of the human element and social aspects.	In my study, I have clarified that the managerial activities will be achieved by government employees at all organisational levels. As a consequence, it is essential to take human aspects into account such as skills, awareness, ethics, beliefs, behaviours and culture.	Current directions in IS security research: towards socio-technical perspectives' (Dhillon and Backhouse, 2001).	R2

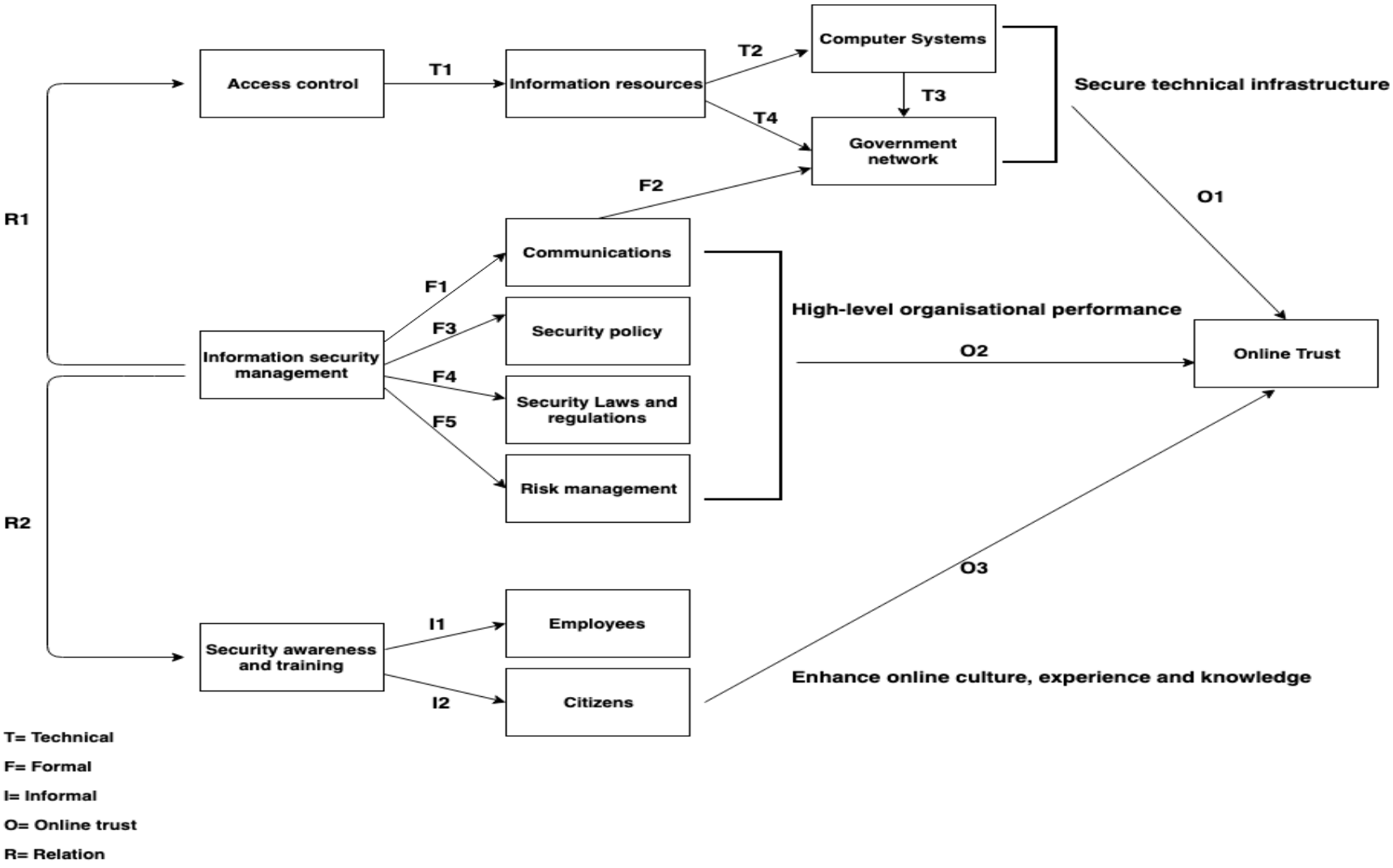


Figure 17: The connection between different theoretical conditions

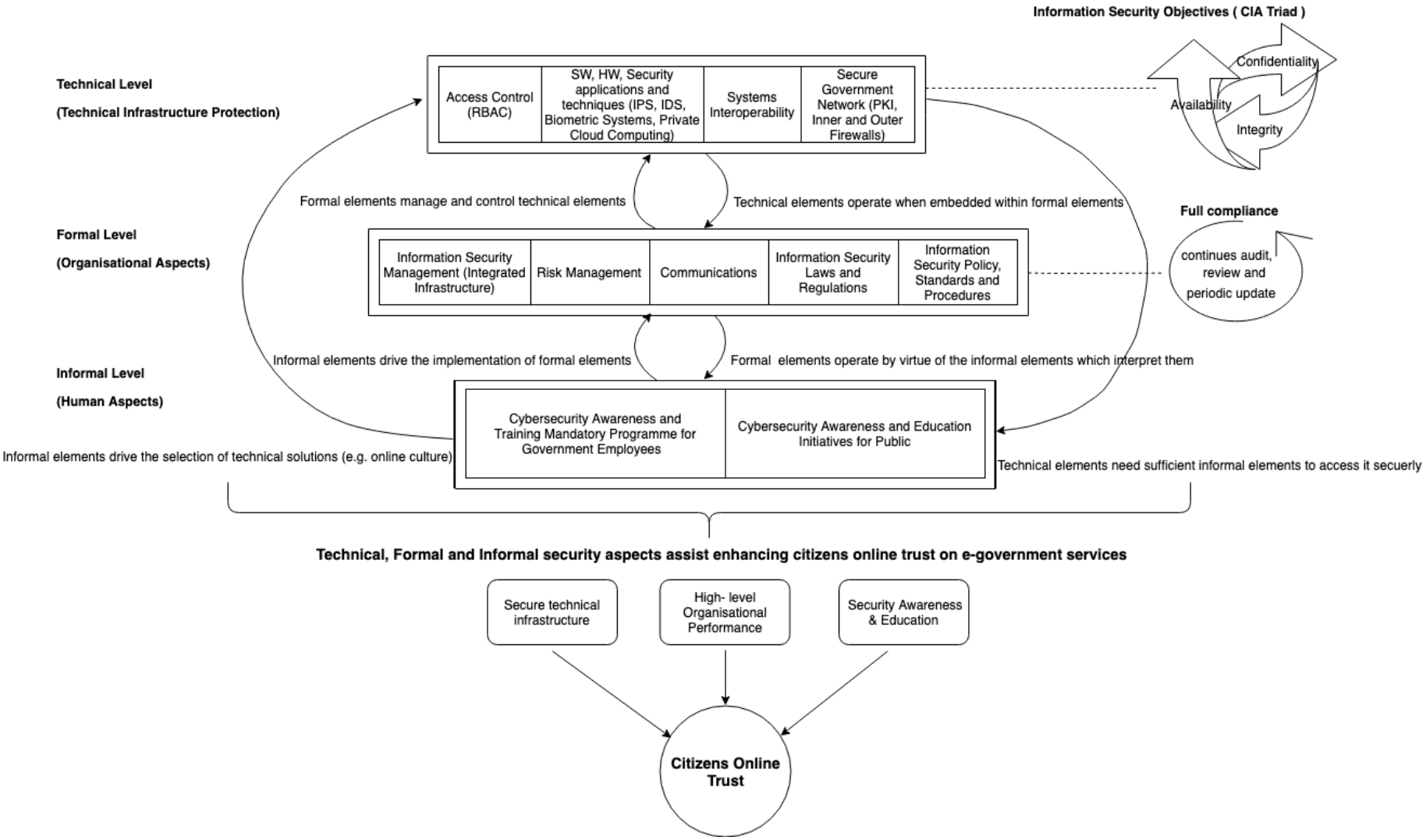


Figure 18: The proposed information security framework for the e-government programme based on the TFI model with linkage to citizens' online trust

Justification of the framework

The implementation of information security standards and principles in an e-government environment is a multidimensional, complex issue that involves people, technology and processes. As mentioned before, e-government security is considered to be one of the crucial factors for reaching an advanced stage of e-government. As the number of available e-government services for different stakeholders is increasing, a higher level of security is required and a comprehensive framework is needed to guide the government organisations in the management of cybersecurity in e-government. In any country, in order to decrease data breaches to a minimum and get the maximum protection of sensitive data when using e-government systems, there should be a security framework to achieve this goal.

In the relevant literature review, the security models of e-government can be based on layers (Alfawaz et al., 2008), cloud computing (Zissis & Lekkas, 2011), on service-oriented architecture (Cândido et al., 2009), access control policy (Chang et al., 2012) or on an information security model (Zhong, 2010). Furthermore, information security models are analysed based on the security issues, either technical or non-technical (Alharbi, 2013). The technical models are concerned with software, hardware, applications and problems relating to availability, confidentiality or integrity. The non-technical models cover organisational aspects (policies, standards, communications, regulations, security management) and human ones (awareness, training, online culture, trust and ethical issues). The existing security models and theories are summarised in Table 17:

Table 17: Information security models and theories

Technical Models	
Bell-LaPadula, (BLP) Model	Focus on confidentiality
Biba Model	Focus on integrity
Clark-Wilson Model	Focus on integrity
The Chinese Wall	Focus on Privacy and integrity
Lambrinoudakis Security Framework	Focus on availability and authentication
InfosecModel	Focus on availability, integrity and confidentiality (CIA triad)
Non-Technical Models	
Theory of Reasoned Action (TRA)	Focus on human action, the relationship between attitudes and behaviours
Theory of Planned Behaviour (TPB)	Focus on links one's beliefs and behaviour

Technology Acceptance Model (TAM)	Focus on how users come to accept and use a technology
Diffusion of Innovation (DOI)	Focus on rate new ideas and technology spread
Motivational Model (MM)	Focus on internal factors to perform certain actions and behaviour, termed Intrinsic Motivation
Social Cognitive Theory (SCT)	Focus on people learning from one another, via observation, imitation, and modelling
Model of PC Utilisation (MPCU)	Focus on acceptance of technology in the context of personal computer utilisation
Unified Theory of Acceptance and Use of Technology (UTAUT)	Focus on all the above non-technical theories

Most of the models mentioned above focus only on one aspect and discuss information security within a single point of view. Technical models investigate technical security controls that address either confidentiality, integrity, availability or users' authentication. For example, in terms of technical frameworks, the Lambrinoudakis security framework is aimed at identifying the requirements of information system security when providing e-government services. In particular, whilst this framework discusses denial of service attacks concerning availability of information, it is used to ensure authentication only (Alharbi et al., 2014). Another model services is the InfoSec model (a multi-layered model), which is considered attractive because of its capability of minimising various security vulnerabilities (Alharbi, 2013). Whilst this model can address availability, integrity and confidentiality of information (CIA triad), it is not concerned with how to construct related policies and procedures. Moreover, a risk management approach should take into account human aspects, like users' behaviour and culture, into consideration, but these are not addressed in this model.

In the literature review, amongst non-technical models, the UTAUT model (Unified Theory of Acceptance and Use of Technology) was elicited as being developed to measure the user acceptance of any technology (Hassan & Khalifa, 2016). However, the impact of the use in terms of security concerns will determine the user acceptability of e-government services where human aspects take a place sometimes in the compromised security of e-services.

Two important studies have proposed an information security framework that combines, i.e. both, technical and non-technical parts. First, Ahlfeldt et al. (2007) presented an extended InfoSec model based on the TFI model, through expanding the administrative part and including elements of formal and

informal levels. The weakness in this work is the narrow investigation domain, being only applied within the healthcare sector. Moreover, the authors do not discuss the added formal and informal elements or the interrelation among them in detail (i.e. policies, risk management, awareness, and behaviour). Second, Hassan and Khalifa (2016) presented an e-government unified security framework (e-GUSF), which relies on the combination of existing models to secure e-government services and how this can affect the formation of citizens' trust in those services. This framework can be beneficial for newly launched e-government projects and for examining security readiness issues of a country to create communication with different stakeholders.

The proposed information security framework in this study can be evaluated within e-government programmes, theoretically and practically. Figure 18 illustrates the proposed framework that holistically addresses information security at the technical, formal and informal levels. Moreover, it is proposed that this framework is an appropriate one for gaining citizens' online trust, as well as that of other stakeholders. In order to build such a framework for information security a close sight to the interrelation between the security levels and aspects was required as well.

Implications of the proposed framework

The implications of the proposed framework are very important for e-government programmes. As mentioned before, providing secure e-government services is a critical and challenging issue so that the users and the government trust the information system and feel confident in using it.

Based on the analysis, the essential step towards the proposed framework is to provide the information security department of the e-government programme with the required laws and regulations to monitor all information systems security across departments and give instructions to different government organisations on how to prevent, detect and respond to cyber-attacks. This emerges from the empirical data serious problem that exists in compliance: cybersecurity practices and instructions differ from one government organisation or department to another. The e-government programme needs the authority to achieve the following: a) ensure the security practices are followed by all staff across departments, b) gain a better overview of cybersecurity audits, with the reports being consolidated and analysed by the e-government programme, c) have the capacity to respond to and fix any reported issues in an e-service swiftly so that any technical errors that could lead to a cybersecurity incidents can be prevented, and d)

conduct mandatory security awareness and training courses for all government employees, thereby ensuring that each government department is offering such courses to their staff.

The technical level concerns critical technical infrastructure (computer systems and networks) protection. The SW, HW and security applications must ensure the main objectives of information security. The non-technical part, also called the administrative part, involves formal and informal levels. The formal level covers organisational aspects (internally and externally), whereas the informal level, concerns of human aspects and this is further divided into employees (government users) and citizens (other e-government services stakeholders). The main contribution is that the proposed framework can be used to protect government information resources and provide secure e-government services in a more comprehensive way. The framework clarifies in detail information security elements that should be taken into consideration within each level and the interrelation among the three levels (technical, formal and informal). Furthermore, as mentioned before, it presents a link to online trust on e-government services through technical, formal and informal security elements

The implementation of the proposed framework consists of several steps. The initial step is protecting the technical infrastructure of the e-government programme in terms of the required critical security measures to provide secure e-services and e-transactions among government organisations/ departments. The crucial goal of the selected security solutions is to address the CIA security triad (confidentiality, integrity and availability). In other words, identifying the users of and priorities for e-services, determine how and when to access information. New security technologies, applications and mechanisms have to be in place and updated regularly in order to protect information resources, involving the computer systems and the network of government. In addition, there needs to be assurance information systems interoperability through shared technical infrastructure among government organisations and departments.

At the formal level, based on security requirements, the government has to set up a national security strategy that defines various defence mechanisms, identifies strategic objectives, decides upon national priorities, and an implementation road map of government vision to address information assurance and cybersecurity measures. Information security policy then should be developed at the national level as a mandatory document outlining the requirements of government organisations information security management system (ISMS). For instance, security direction, security objectives, legal or regulatory requirements, commitment criteria and security incident response. Secure communications infrastructure

among government organisations also should be achieved using PKI, integrated systems and other techniques. In addition, a single sign-on (SSO) is the best means to provide a secure centralised communication gateway with citizens. As the formal elements determine how the technical elements are operated, it is essential to conduct a regular security audit and address any problems identified from this, which is the core of information security management. In addition, risk management which takes into account the informal issues (i.e. users' behaviours, social aspects) as one of the threat sources is important for building security awareness all users of e-government systems and services. In terms of government employees, cybersecurity awareness and training programmes will reduce the number cybersecurity breaches occurring from employees' individual mistakes and ignorance about security practices. Hence, with this framework considering informal issues alongside formal ones is essential. Moreover, the framework clarifies the link between each level of information security approach and online trust.

This framework is aimed at building an e-governance system that joins management and operational control systems. This relation is dynamic and the security of an e-government information systems has to consider both technical and human dimensions. The biggest concern of information security today is the socio-technical relation between systems and users.

My analysis has revealed that information security management involves three main steps in this context: collecting data from devices, analysis and finding any suspicious activity (intrusion detection system). Al-Omari (2006) highlights that there are challenges and limitations in Jordan that prevent e-government progression, involving cybersecurity, such as technical infrastructure constraints. Abu-Shanab (2014) corroborates this view, arguing that the common obstacles facing e-government programmes in developing countries like Jordan are the lack of both technical support for government websites and knowledge about e-government services. Recent literature has also addressed information security management as a common key barrier to the adoption of e-government services (Perez, 2014). Nevertheless, few of the existing studies have covered security dimensions within e-government systems and/or presented a comprehensive framework for different security issues. As a result, the proposed framework can be useful in order to handle all these problems.

Furthermore, the key purpose of the national cybersecurity strategy is to provide all concerned permitted users more secure information systems and networks that they need to operate, manage, or communicate with. The government hopes that this will provide a trusted computing or electronic environment within

the e-government programme. Cybersecurity strategy 2018-2023 identifies strategic objectives, national priorities, and an implementation road map. The strategic objectives support the government's vision for the future. This vision can be realised by adopting the comprehensive framework proposed in this dissertation.

The implementation road map can guide the e-government programme through identifying priorities and achieving the following strategic objectives: First, preventing cyber-attacks to critical information resources to strengthen the e-government programme security in Jordan. Second, reducing vulnerabilities to minimise the risk of system failure and attacks. Third, working on security incident recovery time regardless of source, purpose or type of attack. Fourth, enhancing government organisations prosperity by increasing confidence and trust in government information systems, and by extension, government e-services. Fifth, increasing information security awareness and its importance for national security through a national information security awareness and training programme for all the government workforce. To achieve the objectives listed above, the government of Jordan could benefit from adopting the comprehension strategy set out in the proposed framework.

However, there are some barriers for information security framework implementation in Jordan which could differ from country to another. In terms of technical conditions, lack of budget is the main barrier. Security budget is lagging behind the security challenges faced by governments. There is no average IT security budget for the e-government programme in Jordan, this despite the growing costs of data breaches. In Jordan, with the contracting of IT security spending, there is a lot still required in the technical infrastructure to go toward implementing the proposed framework starting with the latest SW/HW and security applications to protect critical data. In fact, the cost argument has been mentioned a lot within the research findings. The government have to realise that in many cases the incidents will cost far more in the end than if they had updated the infrastructure regularly in the first place. For instance, if something negative occurred to the government network the lost resources will exceed the cost of firewall devices and other protection SW/applications. Without the sufficient budget, it is not possible to apply the technical theoretical conditions which are; using the latest SW, update government network and systems interoperability.

In terms of formal conditions, with limited budgets, top management is less likely to prioritise investment in applying security framework. Within the relevant research findings, management support is a key

obstacle in implementing the security framework. It is important for security managers to receive support for adopting security controls from the administration, operating and executive officers. As the framework clarified the relation between technical level and formal level, technology is most effective when it is supported by sufficient information systems security policies, practices and procedures. When the security policy developed (or updated) it needs to be accessible and comprehensible to the staff. To achieve this, moving from policy to implementation, an awareness program is required to complement the introduction of the new or revised policy. Staff, including chief managers, need to be made aware of the importance and benefits of the security policy and their role in adherence to the policy. Moreover, identifying different risks in the risk assessment process is vital to develop and implement the security policy. For the managers, to gain their support and understanding, putting out scenarios and role reversal situations that front-line staff faced with. An information security policy that is not supported by managers or followed by the staff will reduce overall management effectiveness. Effective information security management then will lead to implementing the rest of formal theoretical conditions as secure communications, set related laws and regulations, conduct regular security auditing and risk assessment. This is because when the managers support information security policy they will ensure compliance with security standards and procedures by different government organisations.

At the informal level, there is a huge shortage in skilled staff and cybersecurity experts which could disturb the implementation of theoretical conditions. According to the research findings, the unskilled staff are mostly responsible for security breaches and direct damage within the government organisations in Jordan. Lack of trained staff is a common problem, not just in Jordanian e-government programme struggling to implement security framework. The e-government programme needs to make sure that they have people with cybersecurity skills at the first place. In order to do this, a more detailed approach to security training and awareness for senior management and all staff is required. In general, only IT staff within government organisations in Jordan are likely to be familiar with security activities and be involved with security procedural and technical aspects of the organisation. This often puts the IT staff in a critical situation facing considerable decisions that are not always clearly identified, and they may need support and confirmation for taking actions. As a result, to implement a comprehensive security framework successfully all staff and departments should be involved, not only IT staff. The main concern is the resistance to change by long-term employees. Employees must realise the benefits of the security framework, training and awareness to gain new security skills. Otherwise, they will unknowingly ruin the framework implementation efforts.

On the other hand, citizens should know that the government is using new security procedures and activities, when they see this type of change, it is a sign for good management and effective planning. Despite the discussions of citizens concern about security and privacy, still many countries like Jordan did not mention a security or privacy policy in their e-government websites. Few countries include a statement about security in some of their governmental sites such as United States, UK, Australia and Taiwan (UN, 2016). There are many areas of concern for information security between the government and the citizens, especially with a high level of bureaucracy in the government. The progress between e-government development and confidence of the citizen in the security of their information is closely connected. Therefore, the e-government programme needs to put serious efforts on online culture to implement the security framework successfully.

As the e-government programme has changed the nature of the relationship between the citizens and the government. This change has also wider impacts on society. Implementation will bring new challenges to existing social and cultural concepts. To obtain the desired advantage of the security framework, government organisations should ensure the open flow of information, subject to security constraints. Implementing the framework of information security is an opportunity to express national identity and culture by provide cybersecurity education and minimise the digital divide. The use of the Internet and the latest technology increase the domain of social influence but this comes with risks and threats. Thus, the balance must be addressed to obtain the maximum potential benefits of e-government in the most secure environment possible. The most important tool for implementation for e-government security is a willing human factor through culture and education.

In fact, barriers are many, including the budget, management objectives and lack of citizen acceptance. These obstacles can be divided into the following categories: technology issues, organisational weakness, funding arrangements, human resources, and the local environment. However, it is important to overcome these concerns and it would be highly advisable to use techniques from other countries and governments to identify areas for improvement. The government of Jordan have to increase the innovation and learns from the mistakes and successes of other countries. In other words, the framework design and implementation should be flexible enough to adapt to any future changes.

5.5 Summary

In this chapter, it has been argued that the most effective way to minimise and mitigate the risk of information security attacks in cyber space is to build a solid foundation through using efficient security mechanisms, technologies, regular security audit, sufficient risk assessment, incidents response plan and awareness initiatives. This starts with developing a strategy regarding how the government is going to achieve this. From the interview analysis, it is apparent that the e-government programme in Jordan needs to adopt a more coherent and comprehensive information security framework in order to cover all potential risks and threats. Moreover, this framework has to be easy to understand an implement by the employees across all government organisations.

In this research, I have contended that the use of a holistic framework to secure e-government services could play an essential role in fostering the trust of citizens in e-government initiatives. This was evident from gathering of the survey data that probed the main themes identified in the interviews findings. However, addressing information security in e-government is certainly more than just technical issues. The proposed information security framework could be useful in terms of renewing e-government programmes to provide trustworthy and reliable communication between them and different stakeholders. The contribution to the combination of technical and non-technical issues based on the TFI information security model may extend to expand the formal and informal levels. It might also be an addition to present linkage to citizens' online trust, as the survey findings declare that different security aspects affect some of the citizens.

In sum, the Jordanian e-government programme needs to focus on delivering the strategic objectives and national priorities of information security strategy by taking the following action:

- Review and update all security related strategies, standards, policies, laws, and support provided in coordination with all stakeholders;
- Manage and coordinate the required efforts to implement the cybersecurity-related projects;
- Manage the critical national infrastructure protection programme;
- Manage the risk management programme in accordance with international standards and then identify information security policies and standards, which are needed to establish consistent and enhanced national information security approach;

- Audit all information systems of government organisations and procedures to assure compliance with national security policies and standards;
- Establish and manage the National Computer Emergency Response Team (JO-CERT) located at NITC, the operations centre of the e-government programme. This would help the e-government programme to deliver continuous network monitoring as well as providing threat intelligence and incident response capability;
- Coordinate with all government departments (including Military, Public Security Department, Civil Defence Department, and General Intelligence Department) regarding information assurance and cybersecurity;
- Raise the concern of cybersecurity within government organisations and the need to make provision for this within their budgets;
- Provide technical assistance to government organisations to guarantee the required protection of information systems and networks;
- Promote awareness and training sessions to government employees to help them comply with national security standards and policies as well as facilitating the implementation of the information security strategy.

6.0 Conclusion

6.1 Introduction

This chapter provides a conclusion based on the key research findings derived from the previous chapters, concentrating mostly on the aim and significance of the study and the theoretical and practical contributions to knowledge. Limitations and suggestions for future work are also presented.

6.2 Significance of the Study and overview

This research investigated the key problems in the information security approach of the Jordanian e-government programme based on the TFI security model while also connecting it to citizens' online trust. In this context, this study provides important insights into e-government programmes as it combines both technical and non-technical security elements. Addressing technical, formal and informal security aspects is important to implement effective and reliable government e-services, and the study proposes a new comprehensive information security approach to e-government programmes, one that leads to citizens' trust in their e-services and is informed by their perceptions on cybersecurity.

The research objectives were oriented towards gaining insights into the information security approach taken within e-government programmes and explore the connection between the security of e-government programmes and citizens' trust in public e-services. This study applied the TFI security model, combining technical, formal and informal security aspects, at the e-government programme in Jordan. By abstracting from the Jordanian case, this study examined how the security of e-government programmes can be framed in a comprehensive information security framework (of a TFI-orientation) and how this must be connected to citizens' trust for both improving their engagement with e-services and considering cybersecurity.

In order to answer the research question of "what is the approach of information security in the Jordanian e-government programme?", the research investigated the issues of technical infrastructure protection, organisational procedures and processes adopting information security standards, and the human role in security breaches, risks and threats. Then, what steps have been taken by the Jordanian government regarding information security to enhance citizens' online trust by communicating technical/formal/informal security elements in their e-government programme. Lastly, to what extent

citizens' perspectives on the e-government programme regarding cybersecurity, affects their trust in e-services.

6.3 Research Outcomes

6.3.1 Information Security Framework for e-Government Programme

This research has focused on the major information security elements on the e-government programme that have an impact on citizens' trust in government services in a Jordan context.

6.3.1.1 Technical Level

The findings show that the technical elements for information security at the e-government programme of Jordan are considered to protect the national technical infrastructure. For example, using an appropriate mechanism for access control (RBAC), creating a secure government network and using essential security technologies (PKI, IDS, IPS, firewalls, encryption, etc.). However, updated software, security mechanisms and applications are not completely in place and still in progress such as biometric systems and cloud computing. Most of the interviewees emphasised the need to keep in line with the latest technologies to secure government organisations/ departments, systems, and networks. Thereby, the government of Jordan can appreciate more the huge benefits offered by information technology and cyber space. The national information security strategy of 2018 was provided as a result of the e-government programme leaders' review of the current challenges and threats for information security. At present, an implementation roadmap is required to ensure and maintain a resilient and trusted cyber space environment that supports technical infrastructure security. The government of Jordan has identified the main national Information security priorities which will help to accomplish the national objectives for the protection of national infrastructures against various security attacks. The findings revealed that there is a fragmentation of e-services (systems and providers among different ministries). A number of ministries and government departments are not hosted by the MoICT; this makes it hard for the e-government programme to control or manage different security issues and minimizing damages and recovery time from cyberattacks that do occur.

6.3.1.2 Formal Level

The findings of this research with respect to formal or organisational issues showed that lack of cooperation and coordination among governmental organisations/departments is one of the key challenges facing the e-government programme and this has implications for information security. Lack of coordination also jeopardises a deeper understanding of the key role of information security in online transactions in terms of availability, reliability and increased transparency in the governance context. Added to this, lack of compliance by government organisations/departments within the e-government programme can be further observed. Considerable steps should be taken to develop information security management and implement systematic policies and procedures consistent with international standards.

This research shows how cybersecurity must be a high priority at the early stage of an e-government initiative and at the start of designing an e-service. The findings showed that a national unified approach to cybersecurity can be applied through the publication of national cybersecurity standards and policies within the information security framework that is managed by the e-government programme. Building a sufficient governance structure to ensure effective information security is critical. While risk management is being addressed at the national level to protect the government network and its critical infrastructure, it is necessary to have well-defined and tested incident management processes, capabilities, mitigation activities and containing the impact of cybersecurity attacks. Risk analysis, threats identification and response to security incidents should be achieved through a national computer emergency response team that will be established across government organisations and departments. Moreover, enacting laws and regulations needed to operate national information security as defined in the national strategy of the e-government programme is equally necessary.

6.3.1.3 Informal Level

In the context of Jordan, the research findings indicate a lack of understanding of the importance of training and awareness of cybersecurity among both government employees and users. As many incidents have happened because of employees' mistakes, building cybersecurity training and awareness programmes are a critical priority in order to grow the skills and capacity of the public workforce. Developing and maintaining these programs would strengthen government organisations and provide great potential that contributes to critical information resources protection. This can be achieved through close consultation with academia and different partners.

Moreover, security awareness and education for citizens will raise their satisfaction and confidence levels to use e-government services. Knowledge stations were a wonderful example of an e-government initiative in this context that can help further in improving citizens perceptions of e-government security and providing citizens with the required knowledge and the support they need to use e-services confidently.

6.3.2 Cybersecurity and Online Trust

Based on the survey findings, a low level of online trust among Jordanian citizens on e-government services was revealed. Most of the participants are using face-to-face interactions with the government. Additionally, the survey showed that citizens' perceptions in terms of information security were one of the key factors affecting their trust in e-services whereas some participants believe that government systems and websites are not trustworthy and government organisations would not able to protect them from cyberattacks.

This research examined the building of citizens' trust in e-government services through a comprehensive information security framework that involves technical, formal and informal issues. At the technical level, for example, using the updated ICTs, latest security techniques and higher website-quality in e-services to serve the public would provide an opportunity to build some trust between citizens and government organisations.

At the formal level, the organisational performance, showing how government e-services are sufficient, reliable and increase transparency will enhance citizens' trust in those e-services. Keeping citizens well-informed and updated as well about available e-services provided by the government will contribute to enhancing the level of acceptance to use e-government initiatives.

Lastly, in the informal level, human aspects can deliver a number of benefits to the e-government programme in the context of information security. Focusing on cybersecurity awareness and education and improving online culture will provide the citizens with an opportunity to be familiar with technology and the online world and would help them develop trust in government e-services.

6.4 Contribution to Knowledge

6.4.1 Theoretical Contributions

This research presented a key contribution by developing a TFI-oriented theoretical framework for information systems security in the context of e-government. While most previous studies have a technical focus, this study integrates and discusses both technical and non-technical elements in the domain of e-government programmes and also connects them to enhancing the trust and confidence of citizens on government e-services.

These contributions advance our knowledge on e-government information security and also connect security to a focus on citizens' trust. The main contributions *to the theory* are:

First, this research expands the TFI security model (as shown in chapter 5, p.191) to cover different information security elements. The formal (organisational) level is divided into internal and external, a distinction that is both useful and meaningful because security requirements may differ if the transaction is among government organisations or with external stakeholders. The informal is further divided into human and social, a subtler distinction that is significant because it requires us to consider both government employees and the public for effective and sufficient information security management. The proposed framework develops these TFI-model adjustments based on the empirical data discussed in chapter 5 and these are informed by a review of the relevant literature. This framework can be validated and tested in e-government programmes. Second, the findings describe how different security elements interact and have a positive relationship for effective information security. In the end, this dissertation contributes to knowledge by providing insights into the citizen perceptions regarding the security of government systems, websites and e-services. It provides evidence that there is a link between their security perceptions and their online trust and confidence to use government e-services.

6.4.2 Practical Contributions

The research findings have important practical contributions, especially in terms of improving e-government programme effectiveness and performance in Jordan from a security management point of view (and in other countries that would be looking to adopt a framework for e-government programme security). Moreover, provide guidance for the e-government programme to deal with different obstacles related to information security issues by applying the proposed framework.

The findings point to a lack of cooperation and coordination among governmental organisations, and lack of compliance by government organisations with security standards and policies are the main problems in the government information security approach. Thus, the government has to focus more on improving the performance of government organisations and their collaboration in cybersecurity. However, there is a lack of security awareness and training, which means that serious actions should be taken toward the improvement of human aspects of cybersecurity. This is projected to enhance employees' skills. In addition, emphasis on the social will increase public knowledge for how to use government e-services in a secure manner.

Furthermore, the findings show that there is a lack of trust in the security of the e-government programme of Jordan, which leads to an unwillingness to use its services. As a result, the e-government officials must put more effort to clarify the potential benefits of e-services in terms of improving reliability and accessibility, and enabling more efficient government service delivery, along with explaining how it will protect user data.

In general, this study has made a new contribution to the research and has expanded the limits of knowledge in the domain of e-government programmes cybersecurity. The study points out that effective information security can help to narrow the gap of familiarity with e-services and improve the online trust of citizens. One of the most practical notes that emerged was that social networks (new media means or tools) would be the best platform to promote the effectiveness of e-services among citizens, especially in terms of information security in cyber space.

6.5 Research Implications

This study expands the information security literature into the e-government context. The findings indicate that using an effective and comprehensive information security approach is crucial for the success of e-government programmes, as any programme's main aim is to provide e-services through cyberspace. This comes with a set of combined risks and threats but also presents opportunities. E-government programme success is directly affected by citizens' participation, and of course, the findings reveal that citizens are willing to trust and use government e-services only if they feel that they are secure from cyberattacks and their data is protected.

The implication for research is that information security extends the understanding toward trust in the e-government area by analysing the different effects of technical, formal and informal security elements. Similarly, the findings show that the use of a comprehensive information security framework would increase government e-services quality, performance and transparency. It is important to invest in information security and expand citizens' knowledge and understanding of the level of security and how their data are protected. This will contribute to building up citizen trust for the utilisation of e-services. Of course, there remains plenty of scope for further research.

6.6 Limitations of Research

This research presented a framework for enhancing information security of e-government services by combining technical, formal (organisational) and human aspects. The proposed framework has been driven from the TFI security model and developed using interviews and data collected from the staff of the e-government programme in Jordan, then a survey with a sample of Jordanian citizens has given the researcher indications on how the trust-citizen considerations should be integrated within the scope of a TFI-oriented model. Nevertheless, this research has a number of limitations that should be mentioned.

The main limitation is regarding the interviewees who were employees at the MoICT in the e-government programme and have limited time to give to the researcher due to their responsibilities and work. Added to this, a few employees opted out of the interviewing process altogether; this prevented the researcher from conducting more interviews.

The other limitation of the research is regarding the survey: due to cultural reasons or perhaps unfamiliarity with e-services altogether, many citizens declined to participate, even though full anonymity was applied across all stages. It was also required to get legal permission from different government departments (Traffic & Licensing, Civil Services and Tax) in order to conduct the survey with the citizens within different government services. Getting such legal approvals was a time-consuming process, otherwise, more citizens would have participated.

In addition, there are some limitations to e-government research more generally. First, there is still no standard definition of e-government as this is defined by the objective of the activity (for example, the transfer of government services and information) or by the technology used (Torres et al., 2005). E-government means different things to different groups (such as citizens, government, and business).

Therefore, there are different observer-relative definitions and each reflects the relationship with a particular stakeholder (Grant & Chau, 2006). Second, the e-government concept cannot be ambiguous or poorly defined, as it can prompt a commotion at the public level when government expectations are above realistic levels, which may prevent people from seeing what is going wrong in e-government projects (Lev (2000); Lissack (2000)). This commotion can be dysfunctional and can sometimes interrupt corrective action, but it can have a function if it gathers interest and gives people a shared vision upon which to act. Third, a government technology project is required to meet certain criteria and make substantial change. In other words, some level of interaction is required, as Layne and Lee (2001) explore in their model showing the stages of e-government growth.

The last limitation of this research which can be considered as an opportunity for future work is that the proposed framework was generalised from empirical data in Jordan. Despite the literature which shows some studies that proposed different information security models in e-government, the comprehensive security model based on TFI was not applied to the context of e-government before. Thus, it is important to validate the proposed framework in other different e-government programmes and use different samples, this could help to compare the findings. Of course, further research on e-government security can also expand the proposed TFI-oriented framework further.

6.7 Future Research

For future research, it is recommended that the proposed framework combining technical and non-technical security issues must be tested in different countries or e-government programmes. In addition, further work is needed in the implementation of information security framework to make the most of the security advantages as a tool to enhance citizens' trust in e-government programme by upgrading public understanding of the benefits and use of ICTs. Following an increasing number of cyberattacks that disrupt online services and computer systems, it is vital that governments are aware of the potential risks and vulnerabilities in their own information systems, manage them carefully, be prepared against different threats, but also involve the citizens more in the safeguarding of these e-services (so that citizens themselves don't become victims – e.g. through cyber-enabled identity theft, fraud, etc.). Identifying cyber threats and being able to protect e-government data from online attacks is critical for effective and sustainable e-services. The fact is that the cost of remediation of cyber-attacks can be extremely high, but the reputational damages can also be serious and further affect citizens' online trust in e-services. Suffering

from cyber-attacks repeatedly and having a reputation for weak security can cause a series of stakeholders that rely on e-services to lose trust in them.

References

Abbasovich, V. A. & Fikratovich, K. K. (2015) E-Government, Open Data, and Security: Overcoming Information Security Issues With Open Data. *IJEIR*, 4(2), 227-231.

Abu-Shanab, E. (2014) Antecedents of trust in e-government services: an empirical test in Jordan. *Transforming Government: People, Process and Policy*, 8(4), 480-499.

Abu-Shanab, E. & Ghaleb, O. (2012) Adoption of mobile commerce technology: an involvement of trust and risk concerns. *International Journal of Technology Diffusion (IJTD)*, 3(2), 36-49.

Abu-Shanab, E. A. (2016) E-government familiarity influence on Jordanians' perceptions. *Telematics and Informatics*, 34(1), 103-113.

Abu-Shanab, E. A. (2012) Digital Government Adoption in Jordan_ An Environmental Model. *International Arab Journal of e-Technology*, 2(3), 129-135.

Abu-Shanab, E. A. & Baker, A. a. N. A. (2011) Evaluating Jordan's e-government website: a case study. *Electronic Government, an International Journal*, 8(4), 271-289.

AbuAli, A., Alawneh, A. & Mohammad, H. (2010) Factors and rules effecting in e-government. *European Journal of Scientific Research*, 39(2), 169-175.

AbuAli, A. & Almarabeh, T. (2010) A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research*, 39(1), 29-42.

AbuShanab, E. & Pearson, J. (2007) Internet banking in Jordan: The unified theory of acceptance and use of technology (UTAUT) perspective. *Journal of Systems and Information Technology*, 9(1), 78-97.

Ahlfeldt, R.-M., Spagnoletti, P. & Sindre, G. (2007) Improving the Information Security Model by using TFI., *In New Approaches for Security, Privacy and Trust in Complex Environments*Springer US, 73-84.

Åhlfeldt, R.-M., Spagnoletti, P. & Sindre, G. (2007) Improving the information security model by using tfi, *IFIP International Information Security Conference*. Springer.

Akhter, F., Hobbs, D. & Maamar, Z. (2005) A fuzzy logic-based system for assessing the level of business-to-consumer (B2C) trust in electronic commerce. *Expert Systems with Applications*, 28(4), 623-628.

Akhter, F., Maamar, Z. & Hobbs, D. (2008) A Fuzzy Logic-Based Approach for Supporting Decision-Making Process in B2C Electronic Commerce Transaction. *Selected Readings on Electronic Commerce Technologies: Contemporary Applications: Contemporary Applications*, 258.

Al-Azzam, A. & Abu-Shanab, E. (2012) Trust Dimensions and the adoption of E-government in Jordan. *International Journal of Information Communication Technologies and Human Development (IJICTHD)*, 4(1), 39-51.

Al-Jaghoub, S., Al-Yaseen, H. & Al-Hourani, M. (2010) Evaluation of awareness and acceptability of using e-government services in developing countries: The case of Jordan. *The Electronic Journal Information Systems Evaluation*, 13(1), 1-8.

Al-Mashari, M. (2007) A benchmarking study of experiences with electronic government. *Benchmarking: An International Journal*, 14(2), 172-185.

Al-Omari, H. (2006) E-Government Architecture In Jordan: A Comparative Analysis. *Journal of Computer Science*, 2(11), 846-852.

Al-Osaimi, K., Alheraish, A. & Bakry, S. H. (2008) STOPE-based approach for e-readiness assessment case studies. *International Journal of Network Management*, 18(1), 65-75.

Al-Rashidi, H. (2013) *The role of internal stakeholders and influencing factors during the phases of e-government initiative implementation*Brunel University, School of Information Systems, Computing and Mathematics.

Al-Shboul, M., Rababah, O., Al-Shboul, M. d., Ghnemat, R. & Al-Saqqa, S. (2014) Challenges and Factors Affecting the Implementation of E-Government in Jordan. *Journal of Software Engineering and Applications*, 07(13), 1111-1127.

Al-Shqairat, Z. I. & Altarawneh, I. I. (2013) The Role of Partnership in E-Government Readiness: The Knowledge Stations (KSs) Initiative in Jordan, *User Perception and Influencing Factors of Technology in Everyday Life*IGI Global, 192-210.

Alexander, B. & Millar, A. (2003) *Tactical Nuclear Weapons: Emergent Threats in an Evolving Security Environment*.Potomac Books, Inc.

Alexander, N. (2003) Building Trust and Confidence for Critical E-government Services, . *ITU Telecommunication Development Bureau (BDT).* .

Alfawaz, S., May, L. J. & Mohannak, K. (2008) E-government security in developing countries: a managerial conceptual framework, *International Research Society for Public Management Conference.* Queensland University of Technology, Brisbane: QUT Digital Repository.

AlGarni, K. (2015) *Information Security Policy for E-government in Saudi Arabia: Effectiveness, Vulnerabilities and Threats*.Rochester Institute of Technology.

Alharbi, N. (2013) E-government security modeling: explain main factors and analyzing existing models. *International Journal of Social, Human Science and Engineering* 7 (9).

Alharbi, N., Papadaki, M. & Dowland, P. (2014) Security challenges of E-government adoption based on end users' perspective, *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for* . IEEE, 78-82.

Alhyari, S., Alazab, M., Venkatraman, S., Alazab, M. & Alazab, A. (2013) Performance evaluation of e-government services using balanced scorecard: An empirical study in Jordan. *Benchmarking: An International Journal*, 20(4), 512-536.

Allen, D. K., Karanasios, S. & Norman, A. (2014) Information sharing and interoperability: the case of major incident management. *European Journal of Information Systems*, 23(4), 418-432.

Almarabeh, T. & Adwan, O. (2013) A Detailed Study of E-government Readiness in Jordan. *International Journal of Computer Science Issues*, 10(6), 88-96.

Alomari, M., Sandhu, K. & Woods, P. (2009) E-government adoption in the Hashemite Kingdom of Jordan: factors from social perspectives, *In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for (pp. 1-7)* . IEEE, 1-7.

Alomari, M., Woods, P. & Sandhu, K. (2012) Predictors for e‐government adoption in Jordan. *Information Technology & People*, 25(2), 207-234.

Alshboul, R. (2012) Security and Vulnerability in the E-Government Society. *Contemporary Engineering Sciences*, 5(5), 215-226.

Anderson, J. M. (2003) Why we need a new definition of information security. *Computers & Security*, 22(4), 308-313.

Andress, J. (2014) *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*.Syngress.

Ashaye, M. O. R. & Irani, Z. (2014) E-government Implementation Benefits, Risks, and Barriers in Developing Countries: Evidence From Nigeria. *US-China Education Review*, 13.

Backhouse, J. & Dhillon, G. (1996) Structures of responsibility and security of information systems. *European journal of information systems*, 5(1), 2-9.

Backhouse, J. & Halperin, R. (2009) Approaching interoperability for identity management systems, *The Future of Identity in the Information Society*Springer, 245-268.

Bakry, S. H. & Muhaya, F. (2011) Assessing the benefits of e-government, *Second Kuwait Conference on e-Services and E-Systems, Kuwait.*

Banerjee, P. & Chau, P. Y. (2004) An evaluative framework for analysing e-government convergence capability in developing countries. *Electronic Government, an International Journal*, 1(1), 29-48.

Bannister, F. & Connolly, R. (2014) ICT, public values and transformative government: A framework and programme for research. *Government Information Quarterly*, 31(1), 119-128.

Gartner's four phases of e-government model (2000).

Bélanger, F. & Carter, L. (2008) Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, 17(2), 165-176.

Belanger, F., Hiller, J. S., Soliman, K. S. & Affisco, J. F. (2006) A framework for e-government: privacy implications. *Business process management journal*, 12(1), 48-60.

Beldad, A., van der Geest, T., de Jong, M. & Steehouder, M. (2012) A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government information quarterly*, 29(1), 41-49.

Benbasat, I., Gefen, D. & Pavlou, P. A. (2010) Introduction to the special issue on novel perspectives on trust in information systems. *MIS Quarterly*, 34(2), 367-371.

Benlian, A. (2015) IT Feature Use over Time and its Impact on Individual

Task Performance. *Journal of the Association For Information Systems*, 16(3), 144-173.

Bert, A. d. (2016) The influence of privacy concerns on m-commerce engagement.

Bertot, J. C., Jaeger, P. T. & Grimes, J. M. (2010) Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government information quarterly*, 27(3), 264-271.

Bjorck, F. (2005) *Discovering information security management*.Department of Computer and Systems Sciences, Stockholm University.

Black, I. (2006) The presentation of interpretivist research. *Qualitative Market Research: An International Journal*, 9(4), 319-324.

Blaikie, N. (1993) *Approaches to social enquiry: Advancing knowledge*.Polity.

Blakley, B., McDermott, E. & Geer, D. (2001) *Information security is information risk management*.

Bose, R. (2004) Information technologies for education & training in e-government, *In Information Technology: Coding and Computing, 2004. ITCC 2004. International Conference on Proceedings (Vol. 2, pp. 203-207).* IEEE, 203-207.

Boudreau, M.-C., Gefen, D. & Straub, D. W. (2001) Validation in information systems research: A state-of-the-art assessment. *MIS quarterly*, 1-16.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 34(3), 523-548.

Burn, J. & Robins, G. (2003) Moving towards e-government: a case study of organisational change processes. *Logistics Information Management*, 16(1), 25-35.

Campbell, T. (1997) Technology, multimedia, and qualitative research in education. *Journal of Research on Computing in Education*, 30(2), 122-132.

Cândido, G., Barata, J., Colombo, A. W. & Jammes, F. (2009) SOA in reconfigurable supply chains: A research roadmap. *Engineering applications of artificial intelligence*, 22(6), 939-949.

Canhoto, A. I. & Backhouse, J. (2007) Profiling under conditions of ambiguity—An application in the financial services industry. *Journal of Retailing and Consumer Services*, 14(6), 408-419.

Carson, D., Gilmore, A., Perry, C. & Gronhaug, K. (2001) *Qualitative marketing research*.Sage.

Carter, L. & Belanger, F. (2004) The influence of perceived characteristics of innovating on e-government adoption. *Electronic Journal of E-government*, 2(1), 11-20.

Carter, L. & Bélanger, F. (2005) The utilization of e‐government services: citizen trust, innovation and acceptance factors*. *Information systems journal*, 15(1), 5-25.

Carter, L. & Campbell, R. (2011) The impact of trust and relative advantage on internet voting diffusion. *Journal of theoretical and applied electronic commerce research*, 6(3), 28-42.

Carter, L. & Weerakkody, V. (2008) E-government adoption: A cultural comparison. *Information Systems Frontiers*, 10(4), 473-482.

Chang, C.-M., Hsu, M.-H. & Yen, C.-H. (2012) Factors affecting knowledge management success: the fit perspective. *Journal of Knowledge Management*, 16(6), 847-861.

Chang, H. H. & Wong, K. H. (2010) Adoption of e-procurement and participation of e-marketplace on firm performance: Trust as a moderator. *Information & Management*, 47(5-6), 262-270.

Chaudhuri, A. & Holbrook, M. B. (2001) The chain of effects from brand trust and brand affect to brand performance: The role of brand loyalty. *Journal of Marketing*, 65(2), 81-93.

Chen, S. C. & Dhillon, G. S. (2003) Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management*, 4(2-3), 303-318.

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L. & Chow, W. S. (2013) IT capability and organizational performance: the roles of business process agility and environmental factors. *European Journal of Information Systems*, 23(3), 326-342.

Cherdantseva, Y. & Hilton, J. (2013) *A reference model of information assurance & security*.

Chuanfan, L. (2010) Research on role-based access control policy of e-government, *2010 International Conference on E-Business and E-Government*. IEEE.

CISCO (2017) *Annual Cybersecurity Report.* Available online: http://b2me.cisco.com/en-uk-annual-cybersecurity-report-2017 [Accessed

Coffey, J. W., Haveard, M. & Golding, G. (2018) A Case Study in the Implementation of a Human-Centric Higher Education Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice*, 2018(1), 4.

Colesca, S. E. (2009) Increasing e-trust: A solution to minimize risk in e-government adoption. *Journal of applied quantitative methods*, 4(1), 31-44.

Coll, R. K. & Chapman, R. (2000) Choices of methodology for cooperative education researchers. *Asia-Pacific Journal of Cooperative Education*, 1(1), 1-8.

Conklin, A. & White, G. B. (2006) E-government and cyber security: the role of cyber security exercises, *In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 4, pp. 79b-79b).* IEEE, 79b-79b.

Conklin, W. A. (2007) Barriers to Adoption of e-Government, *In System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on (pp. 98-98).* IEEE, 98-98.

Cook, K. (2001) *Trust in society*.Russell Sage Foundation.

Cordella, A. & Iannacci, F. (2010) Information systems in the public sector: The e-Government enactment framework. *The Journal of Strategic Information Systems*, 19(1), 52-66.

CountryEconomy (2014) *Jordan - Population.* Available online: http://countryeconomy.com/demography/population/jordan [Accessed

Cousins, P. D. (2002) A conceptual model for managing long-term inter-organisational relationships. *European Journal of Purchasing & Supply Management*, 8(2), 71-82.

Cremonini, L. & Valeri, L. (2003) *Benchmarking security and trust in Europe and the US*.Rand Corporation.

Creswell, J. (2009) *Research design: Qualitative, quantitative, and mixed methods approaches*.SAGE Publications, Incorporated.

Crotty, M. (1998) *The foundations of social research: Meaning and perspective in the research process*.Sage.

Curtin, R., Presser, S. & Singer, E. (2000) The effects of response rate changes on the index of consumer sentiment. *Public opinion quarterly*, 64(4), 413-428.

D'Arcy, J. & Greene, G. (2009) The multifaceted nature of security culture and its influence on end user behavior, *Proceedings of IFIP TC8 International Workshop on Information Systems Security Research, Cape Town*.

Da Veiga, A. (2016) A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument, *2016 SAI Computing Conference (SAI)*. IEEE.

Dada, D. (2006) *The failure of e-government in developing countries: A literature review*.

Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. (1989) User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8), 982-1003.

Dawes, S. S. (2002) *The future of e-government*.

Deloitte, K. p. (2000) *Deloitte Research: At the Dawn of e-Government: The Citizen as Customer*.Deloitte Consulting.

Demchak, C., Friis, C. & LaPorte, T. M. (2000) Webbing governance. *Handbook of public information systems*, 155, 179.

Dhillon, G. (1995) *Interpreting the management of information systems security*The London School of Economics and Political Science (LSE).

Dhillon, G. (2007) *Principles of Information Systems Security: text and cases*.Wiley Hoboken, NJ.

Dhillon, G. & Backhouse, J. (1997) *Managing for secure organizations: a review of information systems security research approaches*.

Dhillon, G. & Backhouse, J. (2000) Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.

Dhillon, G. & Backhouse, J. (2001) Current directions in IS security research: towards socio‐organizational perspectives. *Information Systems Journal*, 11(2), 127-153.

Dhillon, G. & Torkzadeh, G. (2006) Value‐focused assessment of information system security in organizations. *Information Systems Journal*, 16(3), 293-314.

Dimitrova, D. V. & Chen, Y.-C. (2006) Profiling the Adopters of E-Government Information and Services The Influence of Psychological Characteristics, Civic Mindedness, and Information Channels. *Social Science Computer Review*, 24(2), 172-188.

Dirks, K. T. & Ferrin, D. L. (2001) The role of trust in organizational settings. *Organization Science*, 12(4), 450-467.

E-government-Jordan (2015) *Jordan E-government.* Available online: http://www.jordan.gov.jo/wps/portal/E-Gov/Home/Mission [Accessed

E-government-Jordan (2017) *Jordan E-government.* Available online: https://jordan.gov.jo/wps/portal/%5c?lang=ar#/ [Accessed

Eibl, C. J. & Schubert, S. E. (2008) Development of E-learning design criteria with secure realization concepts, *International Conference on Informatics in Secondary Schools-Evolution and Perspectives*. Springer.

Eisenhardt, K. M. & Graebner, M. E. (2007) Theory building from cases: Opportunities and challenges. *Academy of management journal*, 50(1), 25-32.

Evangelidis, A. (2005) FRAMES–a risk assessment framework for e-services. *Electronic Journal of e-government*, 2(1).

Fang, Z. (2002) E-government in digital era: concept, practice, and development. *International journal of the Computer, the Internet and management*, 10(2), 1-22.

Fishbein, M. & Ajzen, I. (1975) *Belief, attitude, intention and behavior: An introduction to theory and research*.

Garrick, J. & Rhodes, C. (2000) *Research and knowledge at work: Perspectives, case-studies and innovative strategies*.Psychology Press.

Grant, G. & Chau, D. (2006) Developing a generic framework for e-government. *Advanced Topics in Information Management*, 5, 72-94.

Greene, S. S. (2006) *Security policies and procedures*.New Jersey: Pearson Education.

Gregoire, Y., Tripp, T. M. & Legoux, R. (2009) When Customer Love Turns into Lasting Hate: The Effects of Relationship Strength and Time on Customer Revenge and Avoidance. *Journal of Marketing*, 73(6), 18-32.

Gregor, S. (2002) A theory of theories in information systems. *Information Systems Foundations: building the theoretical base*, 1-20.

Grimsley, M. & Meehan, A. (2007) e-Government information systems: Evaluation-led design for public value and client trust. *European Journal of Information Systems*, 16(2), 134-148.

Groves, R. M., Couper, M. P., Presser, S., Singer, E., Tourangeau, R., Acosta, G. P. & Nelson, L. (2006) Experiments in producing nonresponse bias. *International Journal of Public Opinion Quarterly*, 70(5), 720-736.

Gunter, B. (2006) *Advances in e-democracy: overview*.

Hadi, F. & Muhaya, F. T. B. (2011) Essentials for the e-government security, *In Information Society (i-Society), 2011 International Conference on (pp. 237-240).* IEEE, 237-240.

Hakim, C. (2000) *Research design: successful designs for social and economic research*.Psychology Press.

Halperin, R. (2006) Identity as an emerging field of study. *Datenschutz und Datensicherheit-DuD*, 30(9), 533-537.

Halperin, R. & Backhouse, J. (2007) Using structuration theory in IS research: Operationalizing key constructs. *ICIS 2007 Proceedings*, 127.

Hansche, S. (2001) Designing a security awareness program: Part 1. *Information Systems Security*, 9(6), 1-9.

Harris, M. A. (2010) *The shaping of managers' security objecitves through information security awareness training*.Virginia Commonwealth University.

Harris, M. A. & Mishra, S. (2006) *Human Behavioral Aspects in Information Systems Security*.

Harris, S. M. M. A. & Richmond, V. A. (2006) *Human Behavior Aspects in Information Systems Security*.

Harrison, L. (2013) *Political research: an introduction*.Routledge.

Hart, D. & Teeter, M. (2003) *The new e-government equation: Ease, engagement, privacy and protection*.

Hart, P. & Saunders, C. (1997) Power and trust: Critical factors in the adoption and use of electronic data interchange. *Organization science*, 8(1), 23-42.

Hasan, L. & Abuelrub, E. (2011) Assessing the quality of web sites. *Applied Computing and Informatics*, 9(1), 11-29.

Hassan, R. G. & Khalifa, O. O. (2016) E-Government-an Information Security Perspective. *International Journal of Computer Trends and Technology (IJCTT)*, 36(1), 1-9.

Hayes, B. (2010) Conducting a Security Audit: An Introductory Overview. Security Focus.

Hedström, K., Dhillon, G. & Karlsson, F. (2010) Using actor network theory to understand information security management, *IFIP International Information Security Conference*. Springer.

Heeks, R. & Bailur, S. (2007) Analyzing e-government research: Perspectives, philosophies, theories, methods, and practice. *Government information quarterly*, 24(2), 243-265.

Henriksson, A., Yi, Y., Frost, B. & Middleton, M. (2007) Evaluation instrument for e-government websites. *Electronic Government, an International Journal*, 4(2), 204-226.

Holden, S. & Ha, L. (2002) Do the facts match the hype? Public demand for, and government attitudes about, e-government, *PA Times,3.*2002

Hong, I. B. & Cha, H. S. (2013) The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management*, 33(6), 927-939.

Horsburgh, S., Goldfinch, S. & Gauld, R. (2011) Is public trust in government associated with trust in e-government? *Social Science Computer Review*, 29(2), 232-241.

Howarth, F. (2014) *The Role of Human Error in Successful Security Attacks.* Available online: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ [Accessed

Hung, S.-Y., Chang, C.-M. & Yu, T.-J. (2006) Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. *Government Information Quarterly*, 23(1), 97-122.

Ihmouda, R., Alwi, N. H. M. & Abdullah, I. (2015) SUCCESSFUL FACTORS ON E-GOVERNMENT SECURITY SOCIAL-TECHNICAL ASPECT. *ARPN Journal of Engineering and Applied Sciences*, 10(20), 9640-9649.

Imamverdiyev, Y. (2013) An application of extreme value theory to e-government information security risk assessment, *2013 7th International Conference on Application of Information and Communication Technologies*.

Irakleous, I., Furnell, S., Dowland, P. & Papadaki, M. (2002) An experimental comparison of secret-based user authentication technologies. *Information Management & Computer Security*, 10(3), 100-108.

Isenberg, P., Elmqvist, N., Scholtz, J., Cernea, D., Ma, K.-L. & Hagen, H. (2011) Collaborative visualization: definition, challenges, and research agenda. *Information Visualization*, 10(4), 310-326.

Islam, S., Mouratidis, H. & Jürjens, J. (2011) A framework to support alignment of secure software engineering with legal regulations. *Software & Systems Modeling*, 10(3), 369-394.

ISO (2005) *2005: IEC 27002 (2005) Information technology, security techniques, code of practice for information security management.*ISO, Geneva.

IT-GOVERNANCE (2017) *What is cyber security?* Available online: What is cyber security? [Accessed

Jap, S. D., Manolis, C. & Weitz, B. A. (1999) Relationship quality and buyer-seller interactions in channels of distribution. *Journal of Business Research*, 46(3), 303-313.

Jiang, L., Srivastava, S. C. & Teo, T. S. H. (2008) Trust and Electronic Government Success: An Empirical Study. *Journal of Management Information Systems*, 25(3), 99-132.

Joo, J. & Hovav, A. (2016) The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru. *Information Technology for Development*, 22(1), 94-116.

Katsikas, S. K. (2000) Health care management and information systems security: awareness, training or education? *International journal of medical informatics*, 60(2), 129-135.

Kazemi, M., Khajouei, H. & Nasrabadi, H. (2012) Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, 6(14), 4982.

Khanyako, E. & Maiga, G. (2013) An information security model for e-government services adoption in Uganda, *In IST-Africa Conference and Exhibition (IST-Africa), 2013 (pp. 1-11).* IEEE, 1-11.

Khasawneh, S., Jalghoum, Y., Harfoushi, O. & Obiedat, R. (2011) E-Government Program in Jordan: From Inception to Future Plans. *IJCSI International Journal of Computer Science Issues*, 8(4), 568-582.

Khayun, V., Ractham, P. & Firpo, D. (2012) Assessing e-Excise sucess with Delone and Mclean's model. *The Journal of Computer Information Systems*, 52(3), 31.

Kidd, T. T. & Hiltbrand, R. K. (2007) Intrusion Detection and Information Security Audits.

Kim, D. J., Song, Y. I., Braynov, S. B. & Rao, H. R. (2005) A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. *Decision support systems*, 40(2), 143-165.

Kim, J.-W., Kim, K.-T. & Choi, J.-U. (2006) Securing e-government services. *Computer*, 39(11), 111-112.

Kim, Y. H., Kim, D. J. & Hwang, Y. (2009) Exploring online transaction self-efficacy in trust building in B2C e-commerce. *Journal of Organizational and End User Computing (JOEUC)*, 21(1), 37-59.

Klischewski, R. (2011) Architectures for Tinkering?: Contextual Strategies towards Interoperability in E-government. *Journal of theoretical and applied electronic commerce research*, 6(1), 26-42.

Kolkowska, E. (2009) *A Value Perspective on Information System Security: Exploring IS security objectives, problems and value conflicts*.

Kor, A.-L., Orange, G., Elsheikh, Y., Cullen, A. & Hobbs, D. (2008) e-Government in Jordan: challenges and opportunities. *Transforming Government: People, Process and Policy*, 2(2), 83-103.

Kortjan, N. a. V. S., R. (2014) A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, 52(1), 29-41.

Krenner, J. (2002) Reflections on the requirements gathering in an one-stop government project, *Electronic Government*Springer, 124-128.

Lacey, R. & Morgan, R. M. (2009) Customer advocacy and the impact of B2B loyalty programs. *Journal of Business & Industrial Marketing*, 24(1-2), 3-12.

Lambrinoudakis, C., Gritzalis, S., Dridi, F. & Pernul, G. (2003) Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*, 26(16), 1873-1883.

Lamsal, P. (2001) *Understanding trust and security*.

Lauer, T. W. (2004) The risk of e-voting. *Electronic Journal of E-government*, 2(3), 177-186.

Layne, K. & Lee, J. (2001) Developing fully functional E-government: A four stage model. *Government information quarterly*, 18(2), 122-136.

Lee, A. (1999) Inaugural editor's comments. *Mis Quarterly*, 23(1), 1.

Lee, J.-S. & Back, K.-J. (2009) AN EXAMINATION OF ATTENDEE BRAND LOYALTY: UNDERSTANDING THE MODERATOR OF BEHAVIORAL BRAND LOYALTY. *Journal of Hospitality & Tourism Research*, 33(1), 30-50.

Lee, J. & Lee, Y. (2002) A holistic model of computer abuse within organizations. *Information management & computer security*, 10(2), 57-63.

Lee, S. M., Tan, X. & Trimi, S. (2005) Current practices of leading e-government countries. *Communications of the ACM*, 48(10), 99-104.

Lenk, K. (1998) Reform Opportunities Missed: Will the innovative potential of information systems in public administration remain dormant forever? *Information Communication & Society*, 1(2), 163-181.

Lev, B. (2000) Knowledge management: fad or need? *Research-Technology Management*, 43(5), 9.

Lewick, R. & Bunker, B. (1996) Developing and maintaining trust in work relationships. *Trust in organizations: Frontiers of theory and research*, 1, 114.

Lissack, M. R. (2000) Knowledge management redux: Reframing a consulting fad into a practical tool. *Emergence, A Journal of Complexity Issues in Organizations and Management*, 2(3), 78-89.

Liu, F., Zhang, L. & Gu, J. (2007) The application of knowledge management in the internet—witkey mode in china. *International journal of knowledge and systems sciences*, 4(4), 32-41.

LSEIdentityProject (2007) *LSE Identity Project Web resources London School of Economics and Political Science*

Available online: http://identityproject.lse.ac.uk/ [Accessed

Luo, P. (2010) Researches on Information Security Evaluation of E-Government System, *In 2010 International Conference on E-Product E-Service and E-Entertainment.*

Lutui, R., Hopoi, S. & Maeakafa, S. (2017) Security readiness evaluation framework for Tonga e-government initiatives.

Majdalawi, Y. K., Almarabeh, T., Mohammad, H. & Quteshate, W. (2015) E-Government Strategy and Plans in Jordan. *Journal of Software Engineering and Applications*, 8(4), 211-223.

Manheim, J. B., Rich, R. C., Bahry, D. L. & Schrodt, P. A. (1991) *Empirical political analysis: Research methods in political science*.Longman New York.

Marchionini, G., Samet, H. & Brandt, L. (2003) Digital government. *Communications of the ACM*, 46(1), 25-27.

May, L. & Lane, T. (2006) A Model for Improving e-Security in Australian Universities. *JTAER*, 1(2), 90-96.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995) AN INTEGRATIVE MODEL OF ORGANIZATIONAL TRUST. *Academy of Management Review*, 20(3), 709-734.

Mazza, R. (2009) *Introduction to information visualization*.Springer Science & Business Media.

Mecella, M. & Batini, C. (2001a) Enabling italian e-government through a cooperative architecture. *IEEE computer*, 34(2), 40-45.

Mecella, M. & Batini, C. (2001b) A review of the first cooperative projects in the italian e-government initiative, *Towards the E-Society*Springer, 831-843.

Miller, T., Birch, M., Mauthner, M. & Jessop, J. (2012) *Ethics in qualitative research*.Sage.

Miyamoto, T. & Rexha, N. (2004) Determinants of three facets of customer trust - A marketing model of Japanese buyer-supplier relationship. *Journal of Business Research*, 57(3), 312-319.

Mofleh, S. I. & Wanous, M. (2008) Understanding factors influencing citizens' adoption of e-government services in the developing world: Jordan as a case study. *INFOCOMP Journal of Computer Science*, 7(2), 1-11.

Mohajerani, S., Shahrekordi, S. Z. & Azarlo, M. (2015) The impact of privacy and security concerns, trust in technology and information quality on trust in e-government and intention to use e-government, *e-Commerce in Developing Countries: With focus on e-Business (ECDC), 2015 9th International Conference on*. IEEE.

Mohammad, H., Almarabeh, T. & Ali, A. A. (2009) E-government in Jordan. *European Journal of Scientific Research*, 35(2), 188-197.

MoICT (2014) *Annual Report.* Available online: http://www.moict.gov.jo/Pages/Studies-and-Report-.aspx [Accessed

MOICT (2017a) *Annual Report.* Available online: http://moict.gov.jo/uploads/Annual%20Report%202017%20FINAL%20r%20(PR).pdf [Accessed

MOICT (2017b) *E-government programme.* Available online: http://moict.gov.jo/content/eGovernment-Program [Accessed

Mok, C. (1996) *Designing business: Multiple media, multiple disciplines*.Macmillan Publishing Co., Inc.

Molnár, B. & Kő, A. (2009) Improving the Security Levels of e-Government Processes within Public Administration through the Establishment of Improved Security Systems. *CIT. Journal of Computing and Information Technology*, 17(2), 141-155.

Montagna, J. M. (2005) A framework for the assessment and analysis of electronic government proposals. *Electronic Commerce Research and Applications*, 4(3), 204-219.

Moon, M. J. (2002) The evolution of e‐government among municipalities: rhetoric or reality? *Public administration review*, 62(4), 424-433.

Moore, G. C. & Benbasat, I. (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research*, 2(3), 192-222.

Moorman, C., Deshpande, R. & Zaltman, G. (1993) FACTORS AFFECTING TRUST IN MARKET-RESEARCH RELATIONSHIPS. *Journal of Marketing*, 57(1), 81-101.

Morgan, R. M. & Hunt, S. D. (1994) THE COMMITMENT-TRUST THEORY OF RELATIONSHIP MARKETING. *Journal of Marketing*, 58(3), 20-38.

Morgeson, F. V., VanAmburg, D. & Mithas, S. (2010) *Misplaced trust? Exploring the structure of the e-government-citizen trust relationship*.

Musso, J., Weare, C. & Hale, M. (2000) Designing web technologies for local governance reform: good management or good democracy? *Political Communication*, 17(1), 1-19.

Mutz, D. & Flemming, G. (1999) *How good people make bad collectives: A social-psychological perspective on public attitude*.

Naik, K. S., Ramachandra, G. & Reddy, M. B. (2014) An Extended Security Framework for E-Government. *International Journal of Advanced Research in Computer Science*, 5(1), 152-154.

Naoum, R. S. & Nadhim, Z. A. (2014) An Enhanced Model for e-Government (A Comparative Study between Jordanian and Iraqi Citizens). *International Journal of Advanced Computer Research*, 4(1), 11.

Ndou, V. (2004) E-government for developing countries: opportunities and challenges. *The electronic journal of information systems in developing countries*, 18.

Neuman, W. L. (2005) *Social research methods: Quantitative and qualitative approaches*, *13*.Allyn and Bacon Boston.

Nguyen, N., Leclerc, A. & LeBlanc, G. (2013) The Mediating Role of Customer Trust on Customer Loyalty. *Journal of Service Science & Management*, 6(1), 96-109.

Normalización, O. I. d. (2005) *ISO/IEC 27001: Information Technology, Security Techniques, Information Security Management Systems, Requirements*.ISO/IEC.

Obeidat, R. A. & Abu-Shanab, E. A. (2010) Drivers of E-Government and E-Business in Jordan. *Journal of Emerging Technologies in Web Intelligence*, 2(3), 204-211.

Odat, A. & Khazaaleh, M. (2012) E-government challenges and opportunities: a case study of Jordan. *International Journal Of Computer Science Issues (IJCSI)*, 9(5), 361-367.

Oliveira, T., Alhinho, M., Rita, P. & Dhillon, G. (2017) Modelling and testing consumer trust dimensions in e-commerce. *Computers in Human Behavior*, 71, 153-164.

Olson, H. (1995) *Qualitative" versus" quantitative research: the wrong question. CAIS/ACSI 95*.

Onwubiko, C. (2009) A security audit framework for security management in the enterprise, *International Conference on Global Security, Safety, and Sustainability.* Springer Berlin Heidelberg, 9-17.

Oscarsson, P. (2002) *Information Security, Data Security, IT Security*.

Ozkan, S. & Kanat, I. E. (2011) e-Government adoption model based on theory of planned behavior: Empirical validation. *Government Information Quarterly*, 28(4), 503-513.

Panko, R. R. & Beh, H. G. (2002) Monitoring for pornography and sexual harassment. *Communications of the ACM*, 45(1), 84-87.

Peltier, T. R. (2013) *Information security fundamentals*.CRC Press.

Peppa, V., Poutoka, A. & Metaxas, G. (2012) *E-government adoption and the impact of Greek farmers' cultural issues on trust towards agricultural e-government services*.

Pereira, T. S. M. & Santos, H. (2010) A Conceptual Framework to Manage and Audit Information Systems Security, *Semana de Engenharia*2010.

Perez, T. J. (2014) Municipal E-Government Security: Insights from a Study of Orange County, California, *In 2014 47th Hawaii International Conference on System Sciences (pp. 1997-2005).* IEEE, 1997-2005.

Popa, M. & Doinea, M. (2007) Audit Characteristics for Information System Security. *Informatica Economică*, 11(4), 103-106.

Ramtohul, A. & Soyjaudah, K. (2016) Information security governance for e-services in southern African developing countries e-Government projects. *Journal of Science & Technology Policy Management*, 7(1), 26-42.

Ratnasingham, P. (1998) Trust in web-based electronic commerce security. *Information Management & computer security*, 6(4), 162-166.

Reffat, R. (2003) *Developing a successful e-government*. Proceedings of the Symposium on E-government: Opportunities and Challenge, Muscat Municipality, Oman, IV1-IV13: Muscat Municipality, O., IV1-IV13.

Reichard, C. (1998) The impact of performance management on transparency and accountability in the public sector. *Ethics and accountability in a context of governance and new public management*, 7, 123-137.

Reynolds, M. & Regio, M. (2001) *E-government as a Catalyst in the Information Age, Microsoft E-Government Initiatives*.

Riedl, R. (2004) Rethinking trust and confidence in European e-government, *Building the E-Service Society*Springer, 89-108.

Robertson, J. (2010) *10 principles of effective information management.*

Rogers, E. M. (1983) Difiusion of innovations. *New York: Free Press*, 18(20), 271.

Rogers, E. M. (1995) Lessons for guidelines from the diffusion of innovations. *The Joint Commission journal on quality improvement*, 21(7), 324.

Rotchanakitumnuai, S. (2008) Measuring e-government service value with the E-GOVSQUAL-RISK model. *Business Process Management Journal*, 14(5), 724-737.

Rousseau, D. M., Sitkin, S. B., Burt, R. S. & Camerer, C. (1998) Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3), 393-404.

Rowley, J. (2011) e-Government stakeholders—Who are they and what do they want? *International journal of Information management*, 31(1), 53-62.

Saleh, Z. I., Obeidat, R. A. & Khamayseh, Y. (2013) A Framework for an E-government Based on Service Oriented Architecture for Jordan. *I.J. Information Engineering and Electronic Business*, 3(1), 1-10.

Samonas, S. & Coss, D. (2014) THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, 10(3).

Sarabdeen, J., Rodrigues, G. & Balasubramanian, S. (2014) E-Government users' privacy and security concerns and availability of laws in Dubai. *International Review of Law, Computers & Technology*, 28(3), 261-276.

Schmid, B. F. (1999) *Elektronische märkte-merkmale, organisation und potentiale. HeSa99, pp. 31-48*.

Scholl, H. J. (2006) Is e-government research a flash in the pan or here for the long shot?, *In Electronic Government (pp13-24)*Springer Berlin Heidelberg.

Scholl, H. J. & Barzilai-Nahon, K. (2007) *Similarities and differences of e-Commerce and e-Government: Insights from a pilot study*.

Schware, R. & Deane, A. (2003) Deploying e-government programs: The strategic importance of "I" before "E". *info*, 5(4), 10-19.

Seidenspinner, M. & Theuner, G. (2007) Intercultural aspects of online communication a comparison of mandarin‐speaking, US, Egyptian and German user preferences. *Journal of Business Economics and Management*, 8(2), 101-109.

Seifert, J. & Petersen, R. E. (2002) The promise of all things E? Expectations and challenges of emergent electronic government. *Perspectives on Global Development and Technology*, 1(2), 193-212.

Seifert, J. W. (2003) A primer on e-government: Sectors, stages, opportunities, and challenges of online governance: Library of Congress Washington DC Congressional Research Service.

Setiadi, F., Sucahyo, Y. G. & Hasibuan, Z. A. (2013) Balanced E-Government security framework: An integrated approach to protect information and application, *In Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2013 International Conference on (pp. 95-98).* IEEE, 95-98.

Shajari, M. & Ismail, Z. (2012) Trustworthiness: a key factor for adoption models of e-government services in developing countries. *2012 International Conference on Education and Management Innovation (IPEDR), Singapore*, 30, 22-26.

Shankar, V., Smith, A. K. & Rangaswamy, A. (2003) Customer satisfaction and loyalty in online and offline environments. *International Journal of Research in Marketing*, 20(2), 153-175.

Shannak, R. O. (2013) The Difficulties and Possibilities of E-Government: The Case of Jordan. *Journal of Management Research*, 5(2), 189-204.

Shapiro, D. L., Sheppard, B. H. & Cheraskin, L. (1992) Business on a handshake. *Negotiation journal*, 8(4), 365-377.

Shaqrah, A. A. (2010) The Influence of Internet Security on E-Business Competence in Jordan. *International Journal of Technology Diffusion*, 1(4), 13-28.

Shareef, S. M. (2016) Enhancing Security of Information in E-Government. *Journal of Emerging Trends in Computing and Information Sciences*, 7(3), 139-146.

Singer, E. (2006) Introduction: Nonresponse bias in household surveys. *International Journal of Public Opinion Quarterly*, 70(5), 637-645.

Siponen, M. T. & Oinas-Kukkonen, H. (2007) A review of information security issues and respective research contributions. *ACM Sigmis Database*, 38(1), 60-80.

Sloan, P. & Oliver, D. (2013) Building Trust in Multi-stakeholder Partnerships: Critical Emotional Incidents and Practices of Engagement. *Organization Studies*, 34(12), 1835-1868.

Smith, S. & Jamieson, R. (2005) Key Factors in E-Government Information System Security, *18th Bled eConference* Bled, Slovenia: SCI, 96-120.

Spagnoletti, P. & Resca, A. (2008) The duality of Information Security Management: fighting against predictable and unpredictable threats. *Journal of Information System Security*, 4(3), 46-62.

Spence, R. (2007) *Information visualization : design for interaction*, 2nd edition. New York: Addison Wesley.

Sprecher, M. H. (2000) Racing to e-government: Using the Internet for citizen service delivery. *Government Finance Review*, 16(5), 21-22.

Stamper, R., Liu, K., Hafkamp, M. & Ades, Y. (2000) Understanding the roles of signs and norms in organizations-a semiotic approach to information systems design. *Behaviour & Information Technology*, 19(1), 15-27.

Straub , D. W. & Nance, W. D. (1990) Discovering and disciplining computer abuse in organizations: a field study. *Mis Quarterly*, 45-60.

Straub, D. W. & Welke, R. J. (1998) Coping with systems risk: security planning models for management decision making. *Mis Quarterly*, 441-469.

Symonds, M. (2000) Government and the Internet: the next revolution. *The Economist*, 355(8176), 3.

Tagert, A. C. (2010) *Cybersecurity challenges in developing nations*Carnegie Mellon University.

Tallon, P. P. (2007) A process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems*, 24(3), 227-268.

Tambouris, E., Gorilas, S. & Boukis, G. (2001) *Investigation of electronic government.*

Tapia, A. H., Maldonado, E., Ngamassi Tchouakeu, L.-M. & Maitland, C. F. (2012) Coordinating humanitarian information: The problem of organizational and technical trajectories. *Information Technology & People*, 25(3), 240-258.

Tassabehji, R., Elliman, T. & Mellor, J. (2007) Generating citizen trust in e-government security: Challenging perceptions. *International Journal of Cases on Electronic Commerce (IJCEC)*, 3(3), 1-17.

Taylor, S. J. & Bogdan, R. (1998) *Introduction to qualitative research methods: A guidebook and resource*.John Wiley & Sons Inc.

Thomas, C. W. (1998) Maintaining and restoring public trust in government agencies and their employees. *Administration & society*, 30(2), 166-193.

Tiwana, A. & Mclean, E. R. (2003) Expertise integration and creativity in information systems development. *Journal of Management Information Systems*, 22(1), 13-43.

Tolbert, C. J. & Mossberger, K. (2006) The effects of e‐government on trust and confidence in government. *Public Administration Review*, 66(3), 354-369.

Tornatzky, L. G. & Klein, K. J. (1982) Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *Engineering Management, IEEE Transactions on*(1), 28-45.

Torres, L., Pina, V. & Acerete, B. (2005) E-government developments on delivering public services among EU cities. *Government Information Quarterly*, 22(2), 217-238.

Traunmuller, R. & Lenk, K. (2002) Electronic government: where are we heading?, *In Electronic Government (pp. 1-9)*Springer Berlin Heidelberg.

Trochim, W. M. (1998) Donald T. Campbell and research design. *The American Journal of Evaluation*, 19(3), 407-409.

Tung, L. L. & Rieck, O. (2005) Adoption of electronic government services among business organizations in Singapore. *The Journal of Strategic Information Systems*, 14(4), 417-440.

UN (2014) *UNITED NATIONS E-GOVERNMENT SURVEY.* Available online: http://www.unpan.org/e-government [Accessed

UN (2016) *UNITED NATIONS E-GOVERNMENT SURVEY.* Available online: https://publicadministration.un.org/egovkb/en-us/reports/un-e-government-survey-2016 [Accessed

Upadhyaya, P., Shakya, S. & Pokharel, M. (2012) E-government security readiness assessment for developing countries: Case study: Nepal Govt. organizations, *In 2012 Third Asian Himalayas International Conference on Internet (pp. 1-5).* IEEE, 1-5.

US (2006) *"National information systems security glossary.* Available online: http://apec.isu.edu/Glossary.aspx?term=2883&alpha=I [Accessed

van Deursen, N. (2014) HI-risk: a socio-technical method for the identification and monitoring of healthcare information security risks in the information society. *Institute for Informatics and Digital Innovation, Edinburgh Napier University, Edinburgh, UK*.

Venkatesh, V. & Davis, F. D. (2000) A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, 46(2), 186-204.

Verdegem, P. & Verleye, G. (2009) User-centered E-Government in practice: A comprehensive model for measuring user satisfaction. *Government Information Quarterly*, 26(3), 487-497.

Vriens, D. & Achterbergh, J. (2004) Planning local e-government. *Information Systems Management*, 21(1), 45-57.

Vroom, C. & Von Solms, R. (2004) Towards information security behavioural compliance. *Computers & Security*, 23(3), 191-198.

Wang, J.-f. (2009) E-government security management: key factors and countermeasure, *In Information Assurance and Security, 2009. IAS'09. Fifth International Conference on (Vol. 2, pp. 483-486).* IEEE, 483-486.

Wang, J. (2008) Design of e-government security system based on information security model, *2008 International Conference on Information Management, Innovation Management and Industrial Engineering*. IEEE.

Wangwe, C. K., Eloff, M. M. & Venter, L. (2012) A sustainable information security framework for e-Government–case of Tanzania. *Technological and Economic Development of Economy*, 18(1), 117-131.

Warkentin, M., Gefen, D., Pavlou, P. A. & Rose, G. M. (2002) Encouraging citizen adoption of e-government by building trust. *Electronic markets*, 12(3), 157-162.

Weise, J. (2001) Public key infrastructure overview. *Sun BluePrints OnLine, August*, 1-27.

Welch, E. W., Hinnant, C. C. & Moon, M. J. (2005) Linking citizen satisfaction with e-government and trust in government. *Journal of public administration research and theory*, 15(3), 371-391.

West, D. M. (2004) E‐government and the transformation of service delivery and citizen attitudes. *Public administration review*, 64(1), 15-27.

White, G. B. (2010) *Center for Infrastructure Assurance and Security-Attack and Defense Exercises*.

Whitworth, B., De Moor, A. & Liu, T. (2006) Towards a theory of online social rights, *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer.

Wimmer, M. & von Bredow, B. (2001) E-government: Aspects of security on different layers, *In Database and Expert Systems Applications, 2001. Proceedings. 12th International Workshop on (pp. 350-355).* IEEE, 350-355.

Wimmer, M. & Von Bredow, B. (2002) *A holistic approach for providing security solutions in e-government*.

Wimmer, M. A. (2002) A European perspective towards online one-stop government: the eGOV project. *Electronic commerce research and applications*, 1(1), 92-103.

Wimmer, M. A. & Tambouris, E. (2002) Online one-stop government, *Information Systems (pp. 117-130)*Springer US.

Wiredu, G. O. (2012) Information systems innovation in public organisations: an institutional perspective. *Information Technology & People*, 25(2), 188-206.

Xiang, L. (2010) The analysis and construction E-government information security assurance system, *In 2010 Second International Conference on Communication Systems, Networks and Applications.*

Yaghoubi, N., Beiglo, S. & Zare, R. (2011) A survey on factors effecting continuity the use of government e-services. *Australian J. Basic Appl. Sci*, 5(8), 209-220.

Yaghoubi, N., Kord, B. & Shakeri, R. (2010) E-government services and user acceptance: the unified models' perspective. *European Journal of Economics, Finance and Administrative Sciences*, 24, 36-49.

Yang, T.-M. & Maxwell, T. A. (2011) Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), 164-175.

Yildiz, M. (2007) E-government research: Reviewing the literature, limitations, and ways forward. *Government Information Quarterly*, 24(3), 646-665.

Yong, J. S. (2005) *E-government in Asia: enabling public service innovation in the 21st century*.Marshall Cavendish.

Zaimes, G. N., Kalampouka, K. & Emmanouloudis, D. (2012) *The Scope of e-Government in the European Union and Potential Applications to the Water Framework Directive/Avrupa Birligi'nde e-Devletin Kapsami ve Su Çerçeve Yönergesi Için Potansiyel Uygulamalar*.

Zeleti, F. A. & Mustonen-Ollila, E. (2011) *ICT Education and Access: As Strategies to Generate and Distribute eGovernment Content*. Slovenia.

Zhao, F., José Scavarda, A. & Waxin, M. F. (2012) Key issues and challenges in e‐government development. *Information Technology & People*, 25(4), 395-422.

Zhao, J. J. & Zhao, S. Y. (2010) Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, 27(1), 49-56.

Zhong, W. (2010) Research on e-government security model, *2010 International Conference on E-Business and E-Government*.

Zhongping, Z., Kaifeng, Y. & Peipei, Z. (2013) Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management, *2013 Fourth International Conference on Digital Manufacturing & Automation*.

Zhou, Z. & Hu, C. (2008) Study on the e-government security risk management. *International Journal of Computer Science and Network Security*, 8(5), 208-213.

Zissis, D. & Lekkas, D. (2011) Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), 239-251.

Annexes

Annex A: List of e-services on national portal and official websites

(Source: MoICT, 2014)

On National Portal	Classification	Service Name	Entity
No	**G2C**	SMS service	**Greater Amman Municipality**
Yes	**G2C**	Issuing and renewal of Vocational licenses	
Yes	**G2C**	Detailed traffic violations	
Yes	**G2C**	Traffic fines values	
Yes	**G2C**	Fines of vocational licenses and health	
Yes	**G2C**	Property tax	
Yes	**G2C**	Inquire about vocational approval	
Yes	**G2C**	Inquiry about health and vocational fees according to handicraft code	
Yes	**G2C**	Property ownership verifications	
Yes	**G2C**	Details of Street	
Yes	**G2C**	Acquisition advertisements	
Yes	**G2C**	Regulatory amendments announcements	
Yes	**G2C**	Tenders (Website of Tendering Directorate)	
Yes	**G2C**	Driver's license violations in detail	
Yes	**G2C**	submitting a complaint	
Yes	**G2C**	Inquire about transaction status	

On National Portal	Classification	Service Name	Entity
No	G2C	Inquiry by handicraft code	
No	G2C	Calculate your Zakat	Al Zakat Fund
No	G2C	Pay Zakat	
No	G2B	Inquire about bank checks	Jordan Customs
Yes	G2B	Inquire about bank guarantees service	
Yes	G2B	Inquire about Clearance companies transactions	
Yes	G2B	Vehicle preview forms system	
Yes	G2B	Inquire about Temporary entry information	
Yes	G2B	Inquire about business customs transactions	
Yes	G2B	Inquire about customs fees for cars service	
Yes	G2B	Inquire about property preview system	
Yes	G2B	Inquire about customs Deposits service	
Yes	G2B	People With Special Needs Exemptions	
Yes	G2B	Integrated customs Tariff system	
Yes	G2B	Inquiry system for customs containers	
Yes	G2B	Electronic Questionnaires	
Yes	G2B	Tenders	
No	G2C	Inquire about financial claims system	
No	G2C	E-services	Orphans Fund Development Corporation
No	G2C	Murabaha Calculations	
No	G2C	E-library	

On National Portal	Classification	Service Name	Entity
No	G2B	specifications and standards catalogue request	Jordan Standards and organisation Metrology
No	G2B	Lists of permitted food additives	
No	G2B	Application forms for Directorate of Metrology services	
No	G2C	Equation models	Ministry of Higher Education and Scientific Research
No	G2C	Non-Jordanian universities recognized by the ministry	
No	G2C	Accredited centres for the TOEFL or equivalent for the purposes of graduate studies in Jordanian universities	
No	G2C	Prices of materials available in the civil institution	Civil Service Consumer Corporation
No	G2C	Electronic Questionnaires	
No	G2B & G2E	E-services for employees and providers	
No	G2B	Employees services	Ministry of Education
No	G2C	Clearance Application Form	
No	G2C	External transfers	
No	G2B	Access schools email accounts through National information technology centre	
No	G2C	SMS service	
No	G2C	Report abuse	
No	G2C	Scholarships	
No	G2C	Courses	
No	G2C	Jobs	
No	G2C	RSS	
No	G2C	SMS gateway	Jordan Food and Drug Administration
No	G2C	Follow-up of electronic transactions	
No	G2C	Mailing List	

On National Portal	Classification	Service Name	Entity
No	G2C	Request an appointment	
No	G2C	Tenders	
No	G2C	Circulars	
No	G2B	Food Information Management System food	Aqaba Special Economic Zone Authority
No	G2B	Economic Zone Customs Website	
No	G2B	Computerized storage system	
No	G2B	Registration system and electronic authorization	
No	G2B	Sales tax system	
No	G2B	Tenders	
No	G2C	Jobs	
No	G2C	Environmental complaints	Ministry of Environment
No	G2C	Job application	City and Villages Development Bank
No	G2B	Tenders ads	
No	G2C	Municipal Elections Management System	Ministry of Municipality Affairs
No	G2G	Questionnaires	
No	G2C	Ask the ministry	
No	G2C	The Office of the Minister	
No	G2C	Jobs	
No	G2C	Tourist attractions	
No	G2B	Investors Services	
No	G2C	Audience services	
No	G2B	Jordanian Employment offices	

On National Portal	Classification	Service Name	Entity
No	G2C	Directorates of labor and employment addresses	Ministry of Labor
No	G2C	Sites to search for jobs	
No	G2C	workers in homes operating Office	
No	G2B	Egyptian labour	
No	G2C	Ask the minister	Ministry of Agriculture
Yes	G2C	Agricultural information request	
No	G2C	online help	
No	G2C	How to calculate your loan	Agriculture Credit Corporation
Yes	G2C	Users note and feedback	
No	G2C	Loan principles	
No	G2C	Trade mark Inquiry	Ministry of Industry and Trade
No	G2C	Fees inquiries	
No	G2C	Query for commercial purposes	
No	G2B	Investors participation	
No	G2B	Certificates	
Yes	G2B	Industrial Property Statistics	
Yes	G2B	Trade mark Inquiry	
Yes	G2B	Search for Trade name	
Yes	G2B	Trademarks sorted by categories	
No	G2B	Entrance Application Form	
No	G2B	Inquire about the financial situation	Development and Employment Fund
No	G2C	Tenders	
No	G2C	Job application	
No	G2C	Customer Satisfaction Survey	

On National Portal	Classification	Service Name	Entity
No	G2C	Loan application request	
No	G2C	Model to provide a creative idea	
Yes	G2B	Direct broadcast of the Central Tenders service	Government Tendering Department
Yes	G2B	Contractors ranked by name and number service	
Yes	G2B	Contractors ranked by major service	
Yes	G2B	Eligible Consultants by name and number	
Yes	G2C & G2B	service Provide revealed self-esteem	Income and Sales Tax Department
Yes	G2C & G2B	Tax registration certificates	
Yes	G2C & G2B	Accepted tax payers statements	
Yes	G2B	Postpone tax payment for imported purposes	
Yes	G2B	certificates for import exemption	
Yes	G2C & G2B	E-services forms	
Yes	G2C & G2B	Electronic Domain registration	National Information Technology Center
Yes	G2C & G2B	Cadastral Plan service	Department of Land and Survey
Yes	G2C & G2B	Request Change Statement on Cadastral Plan	
Yes	G2C & G2B	Request Index map service	
Yes	G2C & G2B	receiving applications for approval of acquisitions and sales electronically	
Yes	G2C	SMS service	General Organisation for Housing and Urban Development
Yes	G2C	Application for Housing ownership royal Initiative service	

On National Portal	Classification	Service Name	Entity
Yes	G2C	Announcements	
Yes	G2C	Legislation and laws	Legislation and Opinion Bureau
Yes	G2C	e-Learning-	Vocational Training Corporation
Yes	G2C	Complaints and inquires	Insurance Authority
Yes	G2C	fatwa(religious cousultaion)	Ifta'a
Yes	G2C	Send an inquiry	
Yes	G2C	Calculate Zakah	
Yes	G2C	Transfer from Hijri date to Gregorian and vice versa	
Yes	G2B	Live service for opening the tenders	Water Authority
Yes	G2C	Competitive ranking	Civil Service Bureau
Yes	G2C	Royal Cultural Center activities	Royal Cultural Center
Yes	G2C	Arrivals flights	Queen Alia Airport
Yes	G2C	Departures flights	
Yes	G2C	Arrivals flights	Royal Jordanian
Yes	G2C	Departures flights	
Yes	G2C	inquire for transaction in nationality directorate	Ministry of the Interior
Yes	G2C	Non-Criminal certificate	Ministry of Justice
Yes	G2C	Public inquiries	
Yes	G2B	lawyers inquiries	
Yes	G2B	Submit applications for companies' registration for members	Company Control Department

On National Portal	Classification	Service Name	Entity
Yes	G2C	Monitoring trading program	Amman Stock Exchange
Yes	G2C	Buildings and lands tax for all municipalities	Ministry of Finance
No	G2C	Buildings and lands tax for Zarqa	
No	G2C	retirement services	
No	G2C	Inquire for retirement salary	
Yes	G2C	Calculate retirement salary	
Yes	G2C & G2B	receive an complaint for copy writer violation	National Library
Yes	G2C & G2B	Request for deposit number of national books	
Yes	G2C & G2B	inquire for information	
Yes	G2C & G2B	Request to get the deposit to a computer program	
Yes	G2C & G2B	Request for deposit number of national courses	
Yes	G2C & G2B	Request for deposit number of audio-visual works	
Yes	G2C & G2B	Request for deposit number of musical works	
Yes	G2C & G2B	ISBN Request for an international standard number	
Yes	G2C & G2B	Request for deposit number for TV show	
Yes	G2C & G2B	Request for deposit number for dialogue (scenario)	
Yes	G2C & G2B	Request for deposit number of words (sung poems)	
Yes	G2C & G2B	Request for deposit number of works of art	

On National Portal	Classification	Service Name	Entity
No	G2C & G2B	Ask for information form	
No	G2C & G2B	transactional Broadcast	
No	G2C	Exchange Rates	Jordan Central Bank
No	G2C	Inquiries for indicators and statistics service	The Department of Statistics
Yes	G2C	info@pm.gov.jo send a complaint	Prime Ministry
No	G2C	Meetings agendas for House of Representatives	The Parliament
No	G2C	Meetings minutes for House of Representatives	
No	G2C	Web Track	Jordan Post
No	G2C	Follow-up postal consignments	
No	G2C	Jordan Stamps	
No	G2C	Calculate Postage	
No	G2C	Ask for the representative (Pickup services)	

Annex B: List of previous studies and theories used in e-government research

Source (Author & Journal)	Theory Used in e-Government Research	Scope of applying theoretical framework
Developing a Successful e-Government Key Centre of Design Computing and Cognition School of Architecture, Design Science and Planning, Australia Dr. Rabee M. Reffat (2006)	Lee four-stage model adopted to illustrate a possible integrated approach for a One Stop e-Government.	The proposed model comprises of four stages of growth: cataloguing, transaction, vertical integration, and horizontal integration Findings: Critical to the success of e-Government transformation is the understanding that e-Government is about the creation of new processes and new relationships between governed and governor. e-Government requires strong political leadership in order to succeed.
A framework for the assessment and analysis of **electronic government proposals** Electronic Commerce Research and Applications 4 Jorge Marcelo Montagna (2005)	Determine different criteria to consider the value contained in government management, the three criteria for electronic government are; efficiency, effectiveness and strategic benefits. Also add a fourth criterion: contribution to transparency and institutional order	This work presents a framework for evaluating e-government initiatives. Firstly, this framework is placed in the context of general electronic government projects, which is a road that has proved to be the right one to achieve success. Findings: each dimension–criterion relationship must be considered not only from the government perspective, but also from the point of view of partners in the government action: citizen, business, government itself. Using these simple elements, it is possible to consider each project characteristics so as to evaluate its viability and the real contribution it makes to government development.

Profiling the Adopters of E-Government Information and Services The Influence of Psychological Characteristics, **Civic Mindedness, and Information Channels** Social Science Computer Review Daniela V. Dimitrova, Yu-Che Chen (2006)	A Conceptual Framework of E-Government Adoption Determinants based on Diffusion theory and TAM	Based on diffusion literature and the TAM model, the study derives the main components of the conceptual framework. The four groups of determinants begin with demographic characteristics, followed by psychological factors, civic mindedness, and, finally, a discussion of the effect of information channels on e-government adoption. Findings: The main conclusion is that sociopsychological factors affect e-government adoption. Perceived usefulness, perceived uncertainty, and prior interest in government are related to being an active user of e-government.
The Difficulties And Possibilities Of e-Government : The Case of Jordan Journal of Management Research Rifat O. Shannak (2013)	Theoretical Analysis, which offered different factors that influence e-government	An examination of the e-government literature reveals that although different researchers have identified different factors that influence e-government implementation and diffusion. Findings: these factors can be broadly classified under four headings; political factors, social factors, technological factors, and organizational factors.
E-government Adoption in the Hashemite Kingdom of Jordan: **Factors from Social Perspectives** Griffith University, Australia Mohammad Kamel Alomari, Kuldeep Sandhu, Peter Woods (2009)	Innovation Theory , and Technology Acceptance Model (TAM) for Theory of Reasoned Action	This study utilised a survey comprising 65 questions (items) to examine the different social factors in the most practical way possible and used exploratory factor analysis for the different items of the different factors. Findings: indicate that, accessibility, beliefs, perceived usefulness, complexity, trust in e-government, trust in government, and e-government adoption are the main components retain for further analysis.
Drivers of E-Government and E-Business in **Jordan** JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE Rand A. Obeidat, Emad A. Abu-Shanab (2010)	Service Oriented Architecture (SOA) , integrating distributed systems customer centric and performance driven services	The well suited architecture for achieving the aims of the new strategy of e-government; such as integrating distributed systems, delivering high-quality customer centric and performance-driven services, is planned to be Service Oriented Architecture (SOA). Findings: SOA is considered to be one of the best ways to provide interoperability and integration between various range of services, implemented by different software applications, running on a

		variety of platforms in government organizations.
Digital Government Adoption In Jordan : An environmental model International Arab Journal of e-Tchnology Emad .Abu Shanab (2012)	Technology Acceptance Model (TAM) for Theory of Reasoned Action, integrated system (one stop DG)	An empirical testing methodology was used to explore the major factors that Jordanian citizens perceive to influence e-government adoption. Findings: The study concluded to 12 factors influence e-government adoption, with mainly two factors trust and privacy, so government need to work well on both of them to improve their citizens' perceptions.
The Influence of Perceived Characteristics of Innovating on e-Government Adoption Virginia Polytechnic Institute & State University, Blacksburg, USA Lemuria Carter, France Belanger (2003)	Diffusion of Innovation Theory (DOI)	This study uses constructs from Moore and Benbasat's (1991) perceived characteristics of innovating to develop a parsimonious model of citizen adoption of state e-Government services. Perceived relative advantage, perceived image, and perceived compatibility are significant elements of e-Government adoption. The model explains 50 percent of the variance in citizen intention to use e-Government services. Findings: As e-Government grows in importance and priority for governments worldwide, an understanding of the factors that influence citizen adoption of these online services is invaluable.
E-Government Program in Jordan: From Inception to Future Plans IJCSI International Journal of Computer Science Sahar Khasawneh, Yaser Jalghoum, Osama Harfoushi, Ruba Obiedat (2011)	A One Stop portal, Service Oriented Architecture (SOA) , secure government network and four stages model	It presented the findings based on a qualitative assessment approach. Findings: The researchers concluded that even though e-government program in Jordan has started many years ago and various projects have been implemented, it has been such a slow process with many deterrents, thus stakeholders are still unable to truly see the fruit of an effective e-government program due to the fact that most projects are not yet linked together or activated.

A Detailed Study of E-government Readiness in **Jordan** IJCSI International Journal of Computer Science Tamara Almarabeh, Omar Adwan (2013)	No model or theory	Findings: Government needs a single reference, its responsibility the management of government websites in the ministries and institutions, need a comprehensive automation for all services, and the e-government services must be expanded to keep up with developments and new technology, giving attention to electronic content and its management, information security, where the citizens still do not fully trust with systems, the development of government websites need to rely on interactivity with the citizen and navigating in a flexible manner, private sector can build the service and they can cover it from profit sharing with the government.
A Framework for an E-government Based on Service Oriented Architecture for Jordan I.J. Information Engineering and Electronic Business Zakaria I. Saleh, Rand A. Obeidat, Yaser Khamayseh (2013)	A One Stop portal , Service Oriented Architecture (SOA), integration mechanism and customer centric	In this paper, we propose a stage model for E-Government interoperability based on Service Oriented Architecture (SOA) that integrates all interoperability aspects and e-government interoperability stages with SOA maturity as well as a proposed framework for E-government based on SOA. Scholars described in details the proposed layers for the framework architecture; namely: the client layer, the presentation layer, the application layer, the data layer, and outlined their interactions, then, applied this architecture for a Jordanian Case Study, in the context of implementing environmental license web service in the MOENV Findings: SOA improves the quality of E-Government application as expansibility in the service integration, Interoperability, Providing secured architecture, protects sensitive information related to citizens
E-Government Architecture In Jordan: A Comparative Analysis Journal of Computer Science Hussein Al-Omari (2006)	Enterprise Network, E-government Portal Model (Multi-Layers)	The proposed architecture for Jordan e-government portal contains all services and sub-services. The hierarchy of services have been determined after a complete scan for all Jordan governmental sites on the web aided by a general knowledge of the governmental hierarchy in Jordan. Findings: expanding the existing programs , protecting information privacy, modifications of the existing systems, set deadline for projects, use digital signature, use successful experiences

Challenges and Factors Affecting the Implementation of E-Government in Jordan Journal of Software Engineering and Applications Muhannad Al-Shboul, Osama Rababah, Moh'd Al-Shboul, Rawan Ghnemat, Samar Al-Saqqa (2014)	Theoretical Analysis, which offered different factors that influence e-government	This paper presented the results of a qualitative study into the issues surrounding the utilization and implementation of e-Government in Jordan as articulated by the key e-Government officials. Findings: Despite all its promise, e-Government in Jordan is still in its early stages and needs more research to improve the effectiveness of e-Services development and to attain wide public acceptance. need more research to improve the effectiveness of e-services and to attain public acceptance, improve people awareness, barrow ideas from other countries, partnership with private sector
E-Government Strategy and Plans in Jordan Journal of Software Engineering and Applications Yousef Kh. Majdalawi, Tamara Almarabeh, Hiba Mohammad, Wala Quteshate (2015)	No model or Theory	This research provided an overview of the past, current, and future status of e-government in Jordan by taking all aspects and sides of e-government program in Jordan which can help in the development of proposals, plans and strategies to improve the level of E-government in Jordan and give trend analysis to get the Jordan trends (positive or negative) in the UN E-government indicators. Findings: • Transforming into E-government services should not be treated as only a computerization of governmental operation but also as a restructuring process. • Using the existing academic institutions to enhance peoples' awareness by adopting training courses on E-government knowledge. • Collaboration with the private sector, which can be helpful in cost-sharing, project and technology management expertise. • Controlling and getting over the resistance to change by clarifying the transformation aims to employee.
e-Government information systems: Evaluation-led design for public value and client trust European Journal of Information Systems Mike Grimsley, Anthony Meehan (2007)	Develops an evaluative design framework for e-Government projects that complements traditional approaches to IS evaluation.	The framework is based upon Moor's concept of public value. It focuses upon citizens' and clients' experiences of service provision and service outcomes as contributors to the formation of public trust. Trust is shown to be related to the extent to which people feel that an e-Government service enhances their sense of being well informed, gives them greater personal control, and provides them with a sense of influence or contingency. The framework's development and validation are founded upon analyses of a two live case studies in south east England and London. Findings: the elements of the conceptual framework that emerged in this first study articulate the relationship between outcomes,

		services and trust in terms of three experiential dimensions: a sense of being well-informed, a sense of personal control in one's life and a sense of influence, which appear to drive trust and satisfaction. It demonstrated that these dimensions could be used to analyse evaluative comments from stakeholders in a way that pointed to issues of trust and satisfaction.
Predicting e-services adoption: a perceived risk facets perspective International Journal of Human-Computer Studies Mauricio S. Featherman, Paul A. Pavlou (2003)	Extends that approach to include measures of negative utility (potential losses) attributable to e-service adoption. Drawing from Perceived Risk Theory, specific risk facets were operationalized, integrated, and empirically tested within the Technology Acceptance Model resulting in a proposed e-services adoption model.	This research indicated that while the segment of consumers surveyed in general did not perceive the e-billpay service as having a high level of usage risk, the risks perceived were very important to them suggesting the criticality of controlling them. The sample studied had higher computing skills, were younger, and more highly educated than the general populace. Findings: results indicated that e-services adoption is adversely affected primarily by performance-based risk perceptions, and perceived ease of use of the e-service reduced these risk concerns. Implications of integrating perceived risk into the proposed e-services adoption model are discussed.
User-centered E-Government in practice: A comprehensive model for **measuring user satisfaction** Government Information Quarterly Pieter Verdegem, Gino Verleye (2009)	Describes the development of a comprehensive model for measuring user satisfaction in the context of E-Government. It rethinks the e-strategies of government and subsequently presents a conceptual model derived from ICT acceptance theory.	Both quantitative as well as qualitative research have been carried out in order to elaborate the model and to formulate adequate indicators for measuring user satisfaction. The measurement model has been tested using data from five Flemish E-Government websites. Structural equation modeling (SEM) was applied in order to investigate the goodness of fit of the model and the underlying indicators. Findings: based on the results, it becomes possible to reduce the list of indicators to nine items, still covering the full conceptual model. With this shortlist of satisfaction determinants, E-Government suppliers would be able to get a clear view on acceptance of their Internet services by the users.
Trust and risk in e-government adoption THE JOURNAL OF STRATEGIC INFORMATION SYSTEMS · France Belanger, Lemuria Carter (2008)	Propose a model of e-government trust composed of disposition to trust, trust of the Internet (TOI), trust of the government (TOG) and perceived risk	Findings from a citizen survey indicate that disposition to trust positively affects TOI and TOG, which in turn affect intentions to use an e-government service. TOG also affects negatively perceived risk, which affects use intentions as well. Implications for practice and research are discussed
Linking Citizen Satisfaction with E-Government and Trust in Government	Develop and test a two stage multiple-equation model that	Develop hypotheses about how citizens' experience with e-government, satisfaction with e-government and government Web sites, and trust in government are interrelated. Moreover, the model for e-

Journal of Public Administration Research and Theory Eric W. Welch, Charles C. Hinnant, M. Jae Moon (2004)	simultaneously predicts experience, satisfaction and trust.	government and Web site satisfaction in corporates citizen perspectives on electronic transaction, transparency and interactivity using data obtained from the Council on Excellence in Government Findings indicate that government Web site use is positively associated with e-government satisfaction and Website satisfaction and that e-government satisfaction is positively associated with trust in government. Also while citizens are generally satisfied with the electronic provision of information (transparency) there is some dissatisfaction with the transaction and interactivity of Web sites.
A Holistic Approach for Providing Security Solutions in e-Government Hawaii International Conference on System Sciences Maria Wimmer, Bianca von Bredow (2002)	Suggest a holistic concept that integrates security aspects	Postulate a holistic approach with the main focus on the processes to be carried out. Presented first deliberations on how existing security solutions can be applied in the scope of e-Administration in an appropriate manner. Findings: further security questions raised in the implementation view still have to be investigated. Additionally, further research in the field in e-Government investigating the application of existing security solutions for the other three domains of e-Government is necessary.
The utilization of e-government services: citizen trust, innovation and acceptance factors Info Systems Journal Lemuria Carter, France Bélanger (2005)	Integrates constructs from the Technology Acceptance Model, Diffusions of Innovation theory and web trust models to form a parsimonious yet comprehensive model of factors that influence citizen adoption of e-government initiatives.	The study was conducted by surveying a broad diversity of citizens at a community event. Findings indicate that perceived ease of use, compatibility and trustworthiness are significant predictors of citizens' intention to use an e-government service.
Study on E-Government Information Misuse Based on General Deterrence Theory International Business School Beijing Foreign Studies University, china Jing Fan, Pengzhu Zhang (2011)	General Deterrence Theory (GDT)	Analysis of the data collected in a survey of 21 government agencies in Shanghai with 124 questionnaires who are specialized in the processes of government information sharing, including information collection and storage, information processing, information transfer and information usage. Findings: indicated that static information security policies only can take effects when the policies are conveyed to employees clearly and the

		punishment is carried out well. Second, security awareness practice is one of the most important measures for internal officials. Third, when employees realize the organization is monitoring their information system behaviors and know consequence of information misuse or abuse behavior, the countermeasures can play more effects. Fourth, preventative software is still the strongest measure for e-government security.
Transaction Stage of e-Government Systems: **Identification of its Location & Importance** Hawaii International Conference on System Sciences Zahir Irani, Madi Al-Sebie, Tony Elliman (2006)	The Transaction stage is clearly delineated as the point at which online technology ceases to be peripheral to the agency's activity. Hence, it presents the first real organisational challenge and an appropriate research strategy is defined to uncover the problems that arise at this point.	Findings: from the review of different e-Government maturity models the Transaction stage is a critical one. First, it is an important precursor to the integration process that represents the ultimate goal of the e-Government agenda. Second, it is the point at which significant project failure rates are beginning to occur.
E-government adoption: A cultural comparison Inf Syst Front Lemuria Carter, Vishanth Weerakkody (2008)	DOI and TAM	This study seeks to determine if the same factors are salient in UK and USA. This study proposes a model of e-government adoption in the U.K. based on salient factors in the U.S. A survey is administered to 260 citizens in London to assess the importance of relative advantage, trust and the digital divide on intention to use e-government. Findings: The results of binary logistic regression indicate that there are cultural differences in e-government adoption in the U.K. and the U.S. The results indicate that of the prevailing adoption constructs, relative advantage and trust are pertinent in both the U.S. and the U.K., while ICT adoption barriers such as access and skill may vary by culture.

Antecedents of trust in e-government services: an empirical test in Jordan Transforming Government: People, Process and Policy Emad Abu-Shanab (2014)	Explore technology adoption research and propose a trust antecedents model, where trust in government, trust in technology, information quality, Internet familiarity and privacy and security concerns are hypothesized to predict Jordanians trust in e-government. Also, trust in e-government extended the Theory of Reasoned Action in predicting the intention to use e-government.	An empirical study was designed utilizing a survey instrument that measures the variables assumed to predict ITU or trust in e-government, respondents were Jordanian citizens selected randomly from schools, businesses and students from the researcher's university. Findings supported the proposed research model, where all proposed variables significantly predicted intention to use e-government services. Also, a partial least squares estimate of the model indicated a significant prediction of trust in e-government by all proposed variables except the Internet familiarity construct. The coefficient of determination for intention to use was 0.465, and for trust in e-government 0.415.
Trust Dimensions and the Adoption of E-Government in Jordan International Journal of Information Communication Technologies and Human Development Emad Abu-Shanab, Ameen Al-Azzam (2012)	No model or framework	This research utilized 105 usable responses from citizens who used and explored e-government services. It was hypothesized that trust in e-government and trust in the Internet, along with perceived risk, will significantly influence trust in E-government, and further intention to use the system. Findings: Using path analysis, results supported trust in government and the Internet and did not support perceived risk. Also, trust in e-government significantly influenced intention to use the system. Finally, path analysis indicated a significant mediation of trust in E-government, where direct and indirect effects were estimated.
Encouraging Citizen Adoption of e-Government by Building Trust **Electronic Markets** Merrill Warkentin, David Gefen, Paul A. Pavlou, Gregory M. Rose (2002)	Propose several ways in which governments can increase citizen trust and thus encourage the adoption of this new and potentially significant mode of government service. The proposed e-Government adoption model also takes in account issues of cultural variables, risk, control and technology acceptance.	Findings: among new users of online government services, characteristic-based and cognitive-based antecedents should be crucial, the nature of previous interactions with the e-Government system should be the major predictor of trust, and hence of continued use.

Annex C: Ministry Letter

Hull University Business School
The University of Hull
Hull HU6 7RX
United Kingdom

Date: 06/12/2016

Dear Ministry of Information and Communications Technology,

This letter is an invitation to consider participating in a study I am conducting at Hull University Business School. I would like to provide you with more information about this project and what your involvement would entail if you decide to take part.

The aim of the project is to first, examine how information security is approached by the Jordanian e-government programme; second, examine whether the citizens' perception about information security of the e-government programme influences their online trust on e-services, over a period of three months. The project focuses on information security and because the ministry of ICT is the responsible of e-government programme, you are best suited to speak to the various issues related to information security approach within e-government systems.

Participation in this study is voluntary. It will involve interviews with managers, head and staff of the e-government department. The interviews will last approximately 1hour in length for each one to take place in a mutually agreed upon location. You may decline to answer any of the interview questions if you so wish: Furthermore, you may decide to withdraw from this study at any time without any negative consequences by advising the researcher(s). The interviews will not be audio recorded. A copy of a formal transcript of any handwritten notes can be provided to give you an opportunity to confirm the accuracy of our conversation and to add or clarify any points that you wish. All information you provide is considered strictly confidential and will be anonymized in full. No employee names will appear in any dissertation or report resulting from this study; only anonymous quotations may be used. There are no known or anticipated risks to you as a participant in this study.

Should the ministry of ICT have any concerns about the conduct of this research project, please contact the Secretary, HUBS Research Ethics Committee, University of Hull, Cottingham Road, Hull, HU6 7RX; Tel No (+44) (0)1482 463536.

I hope that the results of my study will be of benefit to the Ministry directly involved in the study. Of course, I will be more than happy to share my findings with you and present them to you when my research is completed.

I very much look forward to speaking with you and thank you in advance for your assistance in this project

Yours Sincerely,

Nadia Khaled Ali Samara AL-Zoubi

Name of Supervisor: Dr. Dionysios Demetis

The University Of Hull
Business School
Kingston upon Hull HU6 7RX
UK

Annex D: Ministry Approval

وزارة الإتصالات وتكنولوجيا المعلومات
Ministry of Information and Communications Technology

To: president of Hull University Business School,

Referring to the official letter date 6/12/2016 provided by the student Nadia Al Zoubi to request a meeting with the E-government program staff in the Ministry for research purposes, kindly note that we have no objection to hold this meeting.

For the arrangements and the meeting agenda, please contact Ms. Huda Massadeh, E-government program (email: Huda.M@moict.gov.jo).

Wishing to your esteemed university and the student all the success.

Yours sincerely,

Eng. Nader Thneibat

Secretary General of Ministry of Information and Communications Technology

Jordan-cybersecurity

pr46ta6CgZF

Page 1: citizens survey

This is an anonymous questionnaire in the context of a PhD research project.

Note: All data collected is anonymous and cannot identify you as an individual. You are not allowed to copy or re-distribute part of this survey.

1. This survey is filled out: Required

- Electronically by a citizen
- By the researcher on the field

1.a. Select field of interaction for survey completion

Please select

2. Gender?

- Male
- Female

3. Age?

- <18
- 18-24
- 25-29
- 30-39
- 40-49

- [ ] 50-64
- [ ] 65+

4. Education Level?

- [ ] School only
- [ ] University or college
- [ ] Higher education
- [ ] No education

5. How long you been using the Internet?

- [ ] Few years (1-5)
- [ ] Long time (more than 5 years)
- [ ] Very long time (more than 10 years)
- [ ] Never

6. Do you know that this government service is also available online? *(skip this question if you're filling the survey electronically)*

- [ ] Yes
- [ ] No

6.a. Did you try to use it?

- [ ] Yes
- [ ] No

7. Which of the following e-government services have you used online?

- [ ] Tax

- [ ] Driving licence
- [ ] Traffic tickets
- [ ] Social security
- [ ] Work license
- [ ] Borders and residency
- [ ] Civil services
- [ ] Other
- [ ] None

8. Have you faced any problems that made you feel that government systems/websites are not secure?

- [ ] Yes
- [ ] No

9. Have you ever contacted the complaints call centre regarding e-services?

- [ ] Yes
- [ ] No

9.a. What was the issue of compliant about ?

- [ ] Ease of use (interface)
- [ ] System performance (e.g. speed, dropped connections, etc.)
- [ ] Functionality.
- [ ] Other issue

9.b. From the following scale, how satisfied you were with the information provided in the response?

- [ ] Very satisfied

- [ ] Satisfied
- [ ] Ok
- [ ] Dissatisfied
- [ ] Very dissatisfied

9.c. Was any action taken to rectify the problem?

- [ ] Yes
- [ ] No

9.d. How long does it take to respond to your complaint?

- [ ] 1 day
- [ ] 2 days
- [ ] 3 days
- [ ] More than 4 days
- [ ] More than a week

10. From the following scale, how cyber-secure do you feel in sharing your data online for e-government services?

- [ ] Very secure
- [ ] Good
- [ ] Moderately
- [ ] Slightly
- [ ] Not at all

11. From the following scale, how cyber-secure do you feel in using the e-payment gateway (e-fwateercom)?

- [ ] Very secure

- [ ] Good
- [ ] Moderately
- [ ] Slightly
- [ ] Not at all

12. From the following scale, what the views of your relatives, friends or colleagues express regards e-government services?

- [ ] Very positive experiences (Very trustworthy)
- [ ] Positive experiences (Trustworthy)
- [ ] Moderate
- [ ] Slightly negative (Untrustworthy)
- [ ] Very negative

13. From the following scale, in what way these views influenced you to use/trust e-services?

- [ ] Very positive effect
- [ ] Positive effect
- [ ] Moderate effect
- [ ] Negative effect
- [ ] Very negative effect

14. Do you know about government knowledge stations for cybersecurity training and awareness?

- [ ] Yes
- [ ] No

14.a. Did you ever visit or attend one of them?

- [ ] Yes
- [ ] No

15. How trustworthy do you perceive government systems and websites to be?

- [ ] Very Trustworthy
- [ ] Trustworthy
- [ ] Moderately Trustworthy
- [ ] Slightly Trustworthy
- [ ] Not at all trustworthy

16. How secure do your perceive e-government services to be?

- [ ] Very secure
- [ ] Good
- [ ] Moderately
- [ ] Slightly
- [ ] Not at all

17. What makes you feel less secure?

18. What would you like to see/receive from the government so that you may feel more cyber-secure?

23718056

Annex F: Survey Results

Annex G: Mind Map