A RISK ASSESSMENT STUDY ON ELECTRONIC VOTING SYSTEM

FAISAL ABDULLAH SAKHAR AL AMRY

MASTER OF TECHNOLOGY MANAGEMENT

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's full name : FAISAL ABDULLAH SAKHAR AL AMRY

Date of birth : 25 DECEMBER 1974

Title : A RISK ASSESSMENT STUDY ON ELECTRONIC

Academic Session : 2015/2016

I declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)

☑ **OPEN ACCESS** I agree that my thesis to be published as online open access (Full text)

I acknowledge that Universiti Malaysia Pahang reserve the right as follows:

1. The Thesis is the Property of Universiti Malaysia Pahang.
2. The Library of Universiti Malaysia Pahang has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified By:

(Student's Signature) (Signature of Supervisor)

A5592269 DR CHENG JACK KIE

New IC / Passport Number Name of Supervisor

Date : Date :

SUPERVISORS' DECLARATION

We hereby declare that we have checked this thesis and in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master in Project Management.

_____

(Supervisor's Signature)

Full Name : DR CHENG JACK KIE

Position : SENIOR LECTURER

Date : SEPTEMBER 2016

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries, which have been duly acknowledged. The thesis has not been accepted for any degree and is not concurrently submitted for award of other degree.

_____

(Author's Signature)

Name : FAISAL ABDULLAH SAKHAR AL AMRY

ID Number : MPR12001

Date : SEPTEMBER 2016

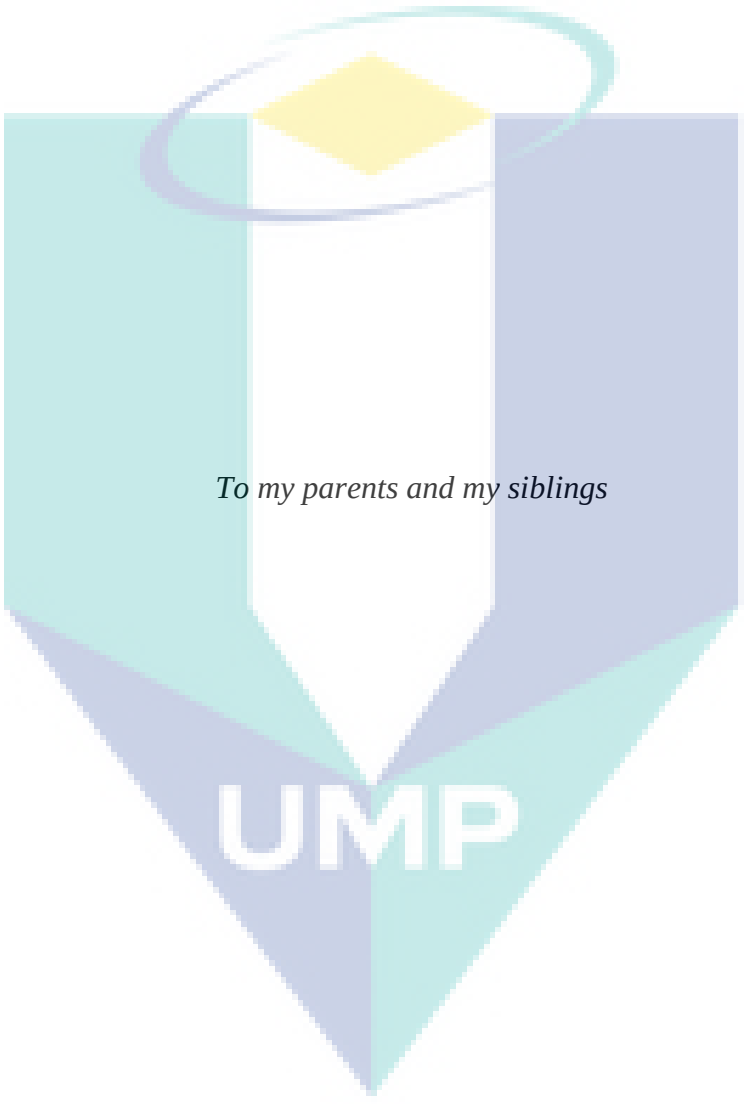
A RISK ASSESSMENT STUDY ON ELECTRONIC VOTING SYSTEM

FAISAL ABDULLAH SAKHAR AL AMRY

Thesis submitted in fulfilment of the requirements
For the award of the degree of
Master of Technology Management

Faculty of Industrial Management
UNIVERSITI MALAYSIA PAHANG

August 2016



To my parents and my siblings

ACKNOWLEDGEMENTS

I am grateful and would like to express my sincere gratitude to my supervisor Dr. Cheng Jack Kie, for her germinal ideas, invaluable guidance, continuous encouragement and constant support in making this research possible. She has always impressed me with her outstanding professional conduct, her strong conviction for science, and her belief that Master program by research is only a start of a life-long learning experience. I appreciate her consistent support from the first day I applied to graduate program to these concluding moments. I am truly grateful for her progressive vision about my training in science, her tolerance of my naïve mistakes, and her commitment to my future career. I also would like to express very special thanks to my previous co-supervisor Mr. LEE, his suggestions and co-operation throughout the study. I also sincerely thank for the time he spent on advising and suggesting me to use the AHP method in my research.

My sincere thanks go to all my lab mates and members of the staff of the Faculty of Industrial Management, UMP, who helped me in many ways and made my stay at UMP pleasant and unforgettable. Many special thanks go to members of the Institute of Postgraduate Studies (IPS) for their excellent co-operation, inspirations and supports during this study.

I acknowledge my sincere indebtedness and gratitude to my parents for their love, dream and sacrifice throughout my life. I acknowledge the sincerity of my brothers, who consistently encouraged me to carry on my higher studies in Malaysia. I am also grateful to my wife for her sacrifice, patience, and understanding that were inevitable to make this work possible. I cannot find the appropriate words that could properly describe my appreciation for their devotion, support and faith in my ability to attain my goals. Special thanks should be given to my committee members. I would like to acknowledge their comments and suggestions, which was crucial for the successful completion of this study.

ABSTRACT

This research focuses on the study of the effective practices of risk assessment for the Omani electoral systems at the Ministry of Interior (MOI). In Oman, the assessment of risk in e-voting system is a crucial matter and it is very important to handle carefully. This is the risk associated with people working with MOI or to individuals associated with the election process in Oman. The problem is how to identify the most risky factors involved e-voting and how to mitigate or permanently resolve the perceived risks. The objectives of this study focus on the evaluation of e-voting risk management culture; the assessment the risks of the old and the new e-voting system and the development of an Analytical Hierarchy Process (AHP) model to find the most risky elements of the old e-voting system. The method used was based on questionnaires, the risks relating with e-voting system was examined. Data pertaining to the old e-voting system was collected by questionnaire. Next step was the questionnaire conducted on risk assessment of the old e-voting system. After data analysis it was concluded four most risky factors involved in the voting were: Slow voting process, voter cheating by ink removal, voter cheating by using different machines and errors due to lack of knowledge. Next AHP method was used to develop a model for decision analysis on finding the risks factors that are more important than others. The new e-voting model which uses citizen ID has proven to be robust. The only weakness the results have indicated is: errors due to lack of knowledge; this can be the only risky issue for the new e-voting system. Results show that seventy nine (79) or 96. 3 % of the employees believe that errors will arise due to the Omani citizens` lack of knowledge of how to vote correctly with the e-voting. Voter cheating by using different machines; this was the second highest risk factor for the old e-voting system. However; it is almost not existent issues with the new e-voting system. Eighty two (82) of the respondents, which is 100%, claimed that they did not encounter any cheating by using different machines. The respondents indicate that the voting process is much faster in the new e-voting system when compared with old e-voting system. That is 100% of the respondents believe the system faster than its predecessor. And finally the number of respondents (employees of MOI and Election department) who agreed that paper work is good alternative is 80 individuals; which correspond to 97.6% of the employees. It is concluded that without creating solid risk assessment; the typical characteristics of sound e-voting system with minimum risks will be entirely absent.

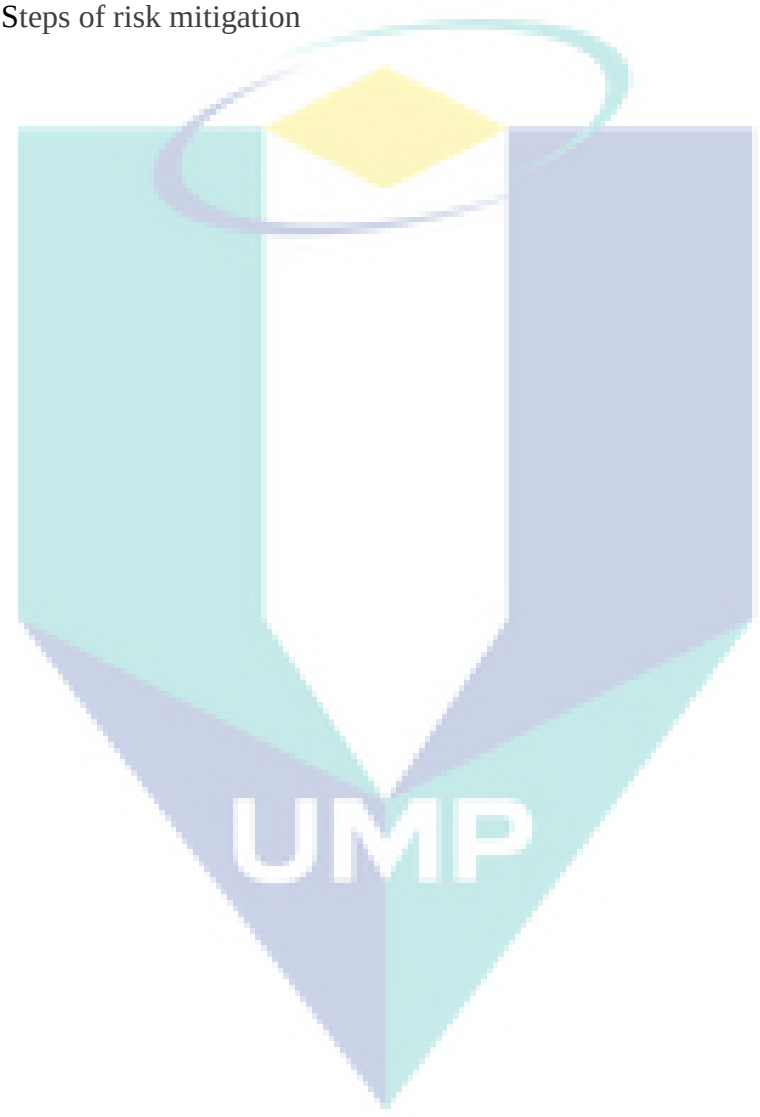
ABSTRAK

Kajian ini memberi tumpuan kepada penilaian keberkesanan pengurusan risiko bagi sistem pilihan raya di Oman yang diaplikasikan oleh Kementerian Dalam Negeri (MOI). Di Oman, pengurusan risiko sistem e-voting adalah sangat penting dan perlu ditangani dengan teliti.Risiko tersebut berkait rapat dengan pegawai yang bekerja dengan MOI dan juga individu yang terlibat dengan proses pilihan raya di Oman.Objektif kajian ini bertumpu kepada penilaian terhadap budaya pengurusan risiko e-voting di Kementerian Dalam Negeri; penilaian risiko sistem e-voting lama melalui analisis statistik serta pembangunan model AHP yang boleh menentukan elemen yang paling berisiko di dalam sistem e-voting yang lama. Kajian ini juga membincangkan pengurangan risiko pilihan raya dengan melaksanakan sistem e-voting baru menggunakan ID warganegara. Kaedah yang digunakan adalah berdasarkan kepada soal selidik terhadap risiko yang berkaitan dengan sistem e-voting di analisa. Data yang berkaitan dengan sistem e-voting lama dikumpulkan daripada soal selidik dan penilaian risiko sistem e-voting yang lama dijalankan. Kesimpulan analisisdata menunjukkan empat faktor yang paling berisiko terlibat dalam pengundian ialah: proses pengundian yang perlahan, menipu pengundi dengan penyingkiran dakwat, menipu pengundi dengan menggunakan mesin dan kesilapan lain kerana kekurangan pengetahuan. Seterusnya, kaedah AHP digunakan untuk membangunkan satu model bagimenganalisaantara risiko tersebut, risiko yang manakah lebih penting berbanding dengan yang lain. Aplikasi sistem e-voting baru yang mengunakan ID warganegara terbukti lebih robust atau kukuh. Keputusan menunjukkan bahawa ralat berpunca daripada kekurangan pengetahuan adalah satu-satunya isu yang berisiko sistem e-voting yang baru. Hasil kajian menunjukkan bahawa (79) atau 96.3% daripada pegawai di MOI percaya bahawa kesilapan sering timbul akibat kurangnya pengetahuan cara mengundi yang betul dikalangan rakyat Oman. Pengundi menipu dengan menggunakan mesin yang berbeza merupakan faktor risiko kedua tertinggi bagi sistem e-voting yang lama. Walau bagaimanapun; masalah ini hampir tidak wujud dengan pengunaan sistem e-voting yang baru. Lapan puluh (82) daripada responden, iaitu 100%, mendakwa bahawa mereka tidak menghadapi sebarang penipuan dengan menggunakan mesin yang berbeza. Responden menunjukkan bahawa proses pengundian adalah lebih cepat dengan sistem e-voting yang baru. Sistem maklum balas juga menjadi lebih cepat (sebanyak 100% responden). Bilangan responden yang bersetuju bahawa kertas kerja adalah alternatif yang baik adalah 80 individu; dimana 97.6% daripadanya adalah pegawai MOI. Kajian ini dapat menyimpulkan bahawa dengan mewujudkan dasar pengurusan risiko yang kukuh; risiko pengaplikasian sistem e-voting dapat dikurangkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES



LIST OF ABBREVIATIONS

AHP	Analytic Hierarchy Process
DOD	Department of Defense
ROP	Royal Oman Police
MOI	Ministry of Interior
GCC	Cooperation Council for the Arab States of the Gulf (Saudi Arabia,UAE,Kuait,Bahran,Qatar and Oman)
OS	Operating system
DRE	Direct-recoding electronic voting machine
EAAA	E-Authentication Activation Application

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

This introductory chapter shortly explains the background of the study, problem statement, research questions, and research objectives, and the significance of study.

1.2 BACKGROUND

The term risk which can be understood as a situation involving exposure to danger or the possibility of suffering harm or loss is in fact an inherent part of business and public life. According to the definition in the Online Business Dictionary (2014), risk is "a probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action". While risk assessment can be defined according to Tchankova (2002) as a continuous process that depends directly on the changes of the internal and external environment of the organization evaluate risks pervcied. Filho (2006) defines risk management as the process developed under a decision analytical framework, leading to quality decisions with an optimal profile of outcomes associated with uncertain events (desirable or undesirable). Sayri (2014) defines risk management as the process of identifying risk, planning, assessing the risk and then conducting control measures.

There has not been any significant change on the nature of the definition of risk assessment but it has been extensively used in many areas of science and social studies. Poor or inadequate risk assessment is the major cause of information technology project

failures according to a number of researchers (Nelson, 2007, Taylor et al., 2012, Whittaker, 1999).

Most of the researchers concluded on different time periods of 2007, 2012 and 1999 that problems of budget overruns due to the underestimation of the actual cost during budgeting and project failures are frequently associated with poor risk analysis and management Sayri (2014).The Analytic Hierarchy Process (AHP) has offered a widespread application in decision-making problems that involves multiple criteria in systems of many levels, in which it was found suitable for creating a decision model for the e-voting system. Therefore, in this research questionnaires and AHP method was used to quantitatively construct effective tool for the assessment of managing risk involved electronic voting (e-voting) in the country of Oman. Starting with questionnaire for risk assessment that will provide ample analysis of the risks involved e-voting. After achieving sufficient knowledge of the risks related with e-voting, then an AHP model was constructed to find out the best possible way or the optimal technique of choosing appropriate risk mitigation process. AHP is a structured multi-attribute decision method (Aminbakhsh et al., 2013), which provides a proven, effective means to deal with complex decision making and allows better, easier, and more efficient weighting and analysis of selection criteria. Every organization has a purpose, and assets, and organizational objectives to be achieved.

Poolsappasi (2010) indicates that in recent days all organizations employ the automated information technology (IT) systems to focus reductions on risks. It is a must that top management of organizational unit to ensure that the organization has the capacity to fulfill its tasks. From the security point of view, the organization needs capabilities to accomplish the maintenance of the required level of safety in the face of real-world threats. Risk management plays a crucial role in determining how to protect the security of information assets of an organizational and carry on its missions from IT-related risks and effective risk management is an essential part of a successful IT project. Risk management is a process that allows IT managers to balance between cost of the protective measures and gains in mission capability. A system administrator has to make a decision and choose an appropriate security plan that maximizes the resource utilization. However, making the decision is not a trivial task.

Most organizations have tight budget for IT security; therefore, the chosen plan must be reviewed as thoroughly as other management decisions. As shown in Poolsappasit (2010) risk management is broken into three components namely risk assessment, risk mitigation, and evaluation. Risk assessment is the practice of shaping the extent of negative impacts associated with the system. The output of this process helps decision maker to identify appropriate controls for reducing the risk in the risk mitigation process.

As mentioned by Ghadge et al.(2012), risk mitigation can be either proactive management or reactive risk response. It can be greatly improved if information is readily available, is timely and accurate. The severity of loss is measured by the deviation from the expected value of the event's possible outcomes. Within this context risk identification is considered as process that reveals and determines the possible organizational risks as well as conditions, arising risks. By risk identification the organization is able to study activities and places where its resources are exposed to risks (Williams et al., 1998). Figure 1.1 illustrates risk identification elements which can be described by the following basic components: *sources of risks; hazard factors; perils;* and *exposures to risk.* Sources of risk are elements of the organizational environment that can bring some positive or negatives outcomes. Hazard is a condition or circumstance that increases the chance of losses or gains and their severity.

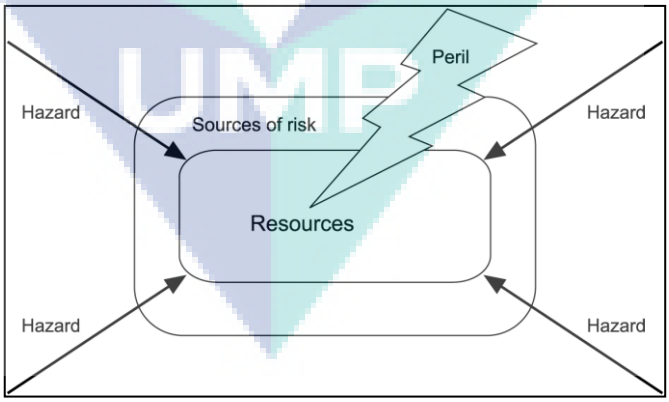


Figure 1.1. Risk Identification Frame

Source: Adopted from Tchankova, 2002

An error of the firm management about the market expansion for a given product is an example for a hazard factor activity that determines the system risk. Peril is

something that is close to the risk and it has negative, non-profitable results. Peril can happen at any time and cause unknown, unpredictable loses. Peril is the cause of losses. Resources exposed to risk are objects facing possible losses or gains. They will be affected if the risk event occurs. Nevertheless, Risk Management is becoming a key factor within organizations since it can minimize the probability and impact of information technology project threats and capture the risk opportunities that could occur during the e-voting project life cycle.

Risk mitigation is used to identify measures which when implemented will minimize the risk or even remove it from the system. After risk has been found to be unacceptable then mitigation should provide an appropriate risk-reducing measures, such as: Reducing the severity of potential consequences; reducing the probability of occurrence harmful effects or reducing the exposure to that risk. The evaluation process includes a process of risk acceptance which requires senior management to sign a statement accepting the residual risk and authorizing the security hardening operation. Traditional risk analysis perceives risk as an inevitable phenomenon that is characteristic of all future events as yet immaterialized. The concept of risk is usually expressed as a function of the uncertainty associated with such events. As suggested by Samvedi (2013) the terms 'risk' and 'uncertainty' are sometimes used interchangeably. However, more often, the concept of risk is expressed in terms of the probability of occurrence (frequency), and the severity of loss (or gain) that will be a consequence of such an occurrence.

1.2.1 ELECTRONIC VOTING SYSTEM

According to Gritzalis (2003) e-voting system can be defined as a voting system in which the election data is recorded, stored processed primarily as digital information. As stated by Haijun et al. (2013) in the recent years, governments have embraced the idea of using information technology (IT) and to recognize e-voting systems a viable method used to replace the paper ballot voting mode in elections. The e-governments is now still considered as mentioned by Moynihan (2004)where it improves many government services; which enables the adoption of electronic voting (e-voting) machines. E-voting is still popular topic worldwide; however the e-voting techniques and systems have not

been widely accepted and deployed by society due to various concerns and problems as claimed by Devi et al.(2014).

Some of the issues associated with many existing e-voting techniques include, the lack of transparency, security issues (software and hard failures), accessibility (if people can access e-voting e.g. the right to vote), and usability (e.g. ease of use of the e-voting system). These issues create major risks that can hinder the election process.

Many of these issues were present since the introduction of the electronic voting; especially with controversial presidential elections and the recent news involving the Secure Electronic Registration and Voting Experiment (SERVE). According to Schaupp and Carter (2005), SERVE were considered insecure by three of its 12 evaluators. SERVE, which was developed by the US Department of Defense (DOD), allows absentee military voters in 50 countries and seven states to cast their votes via the internet (Lemos, 2004). The first use of this new technology occurred in South Carolina's presidential primary on 3rd February, 2004. DOD plans to eventually expand the program to handle the votes of nearly six million US military personnel and civilians living abroad. However, security experts warn that existing internet technology cannot guarantee the integrity of e-voting (Lemos, 2004).

Accenture, who jointly created SERVE with the DOD, stresses that it was only designed to be an experiment to collect data on voter reactions to casting ballots online. The potential consequences can be disastrous such as grand election fraud. Since the opportunities for fraud provided by electronic voting machines surpass all the opportunities available previously. For example, a corrupt insider, working for one of the vendors of widely-used voting machines, could hide malicious code in the software.

In an attempt to solve these issues in the USA, the Help America Vote Act (HAVA), was passed by Congress in 2002 mandates reform of the election processes of all states as mentioned (Verified Voting Organization (2014) and Shaupp, 2005). HAVA provides funding to replace obsolete voting technologies such as punch cards and lever machines with more modern technologies such as precinct based optical scanners and direct recording electronic (DRE) voting machines. According to (Schaupp and Carter, 2005) a survey in the UK voters in 2002 asked them which voting method they would

prefer to use in the next general election. Eighty-seven (87%) percent said they would like to be able to vote online using their home computer or office computer (Schaupp and Carter, 2005). An application to electronic voting is given that matches the features of the best current protocols with significant efficiency improvements by using a mathematical construct which provides a cryptographic protocol (Neff, 2001).

Since there are security concerns that surround internet transactions (Schaupp & Carter, 2005) investigating such questions, are citizens willing to vote online? Would citizens prefer online voting to traditional means of casting a ballot? Their research has profound effect on e-voting systems. There are several studies (Gibson, 2001, Mercuri, 2000) that caution against the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. SERVE is a very good example of the major issues experienced in e-voting and he project was cancelled in 2004 due to its pertaining problems. Vulnerabilities in SERVE occurs because the Internet is independent of national boundaries, an election held over the Internet is vulnerable to attacks from anywhere in the world. A shown in Jefferson et al. (2004), not only could a political party attempt to manipulate an election by attacking SERVE, but so could individual hackers, criminals, terrorists, and even other countries. Some of the core issues were the lack of voter-verified Audit system, insider attacks, Lack of Control of the Voting Environment, lack of privacy etc.

However, there are other researchers who have done more studies using computer technologies to improve elections (Kohno et al., 2004, Neff, 2001, Trechsel & Mendez, 2005). The issues of transparency, security, accessibility and usability of e-voting have been considerably improved and people achieved a sense of reliance on the e-voting system. A good example of such improvement is the cases of the country of Estonia, which according to Alvarez et al. (2008) were a successful election by using e-voting was achieved.

1.2.2 Oman Government Election System

The country Oman, officially called the Sultanate of Oman, is an Arab state in Southwest Asia on the southeast coast of the Arabian Peninsula. The election process

starts before one year of election. The steps for participating elections are simple and fair. Any Omani citizens whose ages reaches 21 years before the 1st January of the election year and possess a valid citizen card or passport can register for vote. The Wally (governor) officers are responsible for the registration process. An application designed for this process and the registration is recorded through this application. A scanned copy of citizen's resident card or passport copy and a printed confirmation of registration are kept for further reference. The election applications are running on disconnected computers (offline); hence a separate application provides for the Wally officers to back up the local database and write to a CD and send to the ministry for the synchronization of the data. This activity will take place every week until the last date of voter registration.

Every week the Wally officers send the backup CD of their database. The administrators of the ministry will store all the data to a staging database. The staging database is used to load data from the sources, modify & cleansing them before finally loading the data into the data warehouse. After the storage the administrators of the ministry will crosscheck each name and ID along with the scanned copy provided to them. Once any mismatch found, they rectify the error and make the database error free. Each of the registered voters needs to cross check with Royal Oman Police (ROP) for their validity of the resident card and name correction. The cross checking is done by the Ministry of Interior (MOI) against the ROP database and with the staging database.

The old e-voting system was implemented in 2007. The only solution to the old e-voting system problems is to implement new e-voting project in Oman. The problems of the old system include the following: The voters cannot vote using either passport or ID card (The voter should only use ID card); it is difficult to tract a person since the electoral ink was used to identify the voted person, while even some of the voters refuses to mark the electoral ink. The non-elected candidates are trying to complain about the system, like the fraud voting is possible in case that the people could erase the election ink on their fingers, and choose second voting center to vote. And the final problem with the old e-voting system is the cost of backing up the servers or PC's, this can increase the cost almost double of actual amount invested on the technology. The proposed new e-voting system uses the E-Authentication technique which uses the existing National ID Card to authenticate citizens for voting in the national elections. The solution shall allow

all citizens to come to election points and get authenticated through their National ID Card before proceeding to the vote.

The registered voters are required to update any changes relating to their Wilayat (meaning Province in Arabic) due to the relocation of the area, relocation of work or marriage can submit the application to the authorities for change or update his voting Wilayatand once the application is approved, the voting Wilayat of the voter can be changed, this process is called as update. This data also need to crosscheck with the Royal Oman Police. Once the voter list is finalized it will announce officially and the list will be published for public access so any complaints related the list can be registered, if found valid a committee will take necessary actions to resolve it. Updating or editing of the details is also possible on this stage. Candidate registration should register any Omani citizen whose age reaches 21 years, is eligible for applying as candidate in elections. The applications will be scrutinized by higher authorities, once his application approved then his photographs and other details will be recorded in to the ministry database. After shortlisted the candidates, each Wilayat candidate list will be officially published and any complaints related candidate list can be officially given and necessary actions will be taken by the committee. After finalizing the candidate list, next step is to proceed for ballet paper printing. Every ballet is printed with name and photograph of each candidate in Wilayat base. The ballets are highly secured with an embossed (stamped) water mark for preventing the scanned or photo copying of the ballet. And it carries a barcode to find genuineness of the ballets.

For the blacklisted voters a list will be populated from Royal Oman Police and that list will be kept separately in database. And the time of voting while entering the user data or card if the voter is black listed it will be displayed. In the case of employees who are working for the election department and the citizens working for other embassies in GCC (Cooperation Council for the Arab States of the Gulf) countries, must conduct their votes before the actual election Day. In Oman, the management risk in e-voting system is crucial matter and it is very important to handle it carefully. This is the risk associated with people working with MOI or to individuals associated with the operation election process in Oman. The management of this risk is a key element in the MOI`s information security program and provides an effective framework for selecting the appropriate security controls for the e-voting system.

1.3 PROBLEM STATEMENT AND MOTIVATION

The phenomenon of electronic government (e-government), electronic democracy (e-democracy), and electronic politics (e-politics) give rise to other phenomenon known as electronic voting (e-voting) and which specifically, is a relatively new subject of study (officially introduced 1999 in Brazil). However, with the globalization of Internet use, the deployment of technology to improve democracy has rapidly gained worldwide attention(Kitlan, 2010). Our initial observations conducted within the MOI indicated that many institutions in Oman still do not yet understand or manage risk within in the context of e-voting systems, despite the presence and wide applications of electronic voting systems (e-voting) in this modern day.

In the country of Oman, the MOI has already implemented an e-voting system, however; it is considered as an old e-voting system that requires improvement in terms of risk assessment. The research problem here is how to identify the most risky factors and then mitigate or permanently resolve the risks? The research will focus on assessing the risk in the old e-voting system. However; review and observation within the MOI of Oman concluded that there is no documented risk assessment plan that can foresee risks, estimate impacts, and define responses to issues relating with risks involving voting process in Oman. Observations on the old system were conducted and the quality of the overall risk assessment culture was evaluated. This paves the way for the assessment the risks of the old e-voting system involving system elements, such as hardware, software, system interfaces, data and information, personnel actions, and the mission of the e-voting system. Then development of AHP model to find the most risky elements of the old e-voting system. The AHP model considers four (4) risk variables (risk Reliability, Operator authentication, Immunity to attack, Integrity of votes and Fault tolerance).

A new e-voting system making use of the e-Authentication technique, which uses the existing National ID Card to authenticate citizens for voting, was proposed. This new e-voting system supports solutions that can provide to all citizens to come to election points and get authenticated through their National ID Card before proceeding to the vote. The solution shall be hosted within the current National ID System, taking advantage of the electronic authentication of the cards while enhancing these capabilities with

functions specific to the election process, ensuring election rights and introducing vote timestamp storage in the cards. Just like the old system the new-e-voting system will also undergo risk assessment involving system elements, such as hardware, software, system interfaces, data and information, personnel actions, and the mission of the e-voting system.

1.4 RESEARCH OBJECTIVES

The objective of this research focuses on the assessment of the effective practices of risk management for the Omani e-voting system to assist the MOI. The objectives of this study are:

1. To evaluate the risk management culture on e-voting at the Ministry of Interior.
2. To assess the risks of the old e-voting system through statistical analysis.
3. To apply an AHP modeling technique that can determine the most risky elements in the old e-voting system.
4. To evaluate the risks of the new e-voting system.

1.5 RESEARCH SCOPE

This research is limited and focuses on risk management of electronic voting system (e-voting) in the government of Oman. The research will carry out the assessment of the E-voting Risks. Such assessment includes: determining the existing controls of the e-voting process; anticipating the likelihood of risk and its consequences; estimation of the level of the risk. Finally the research will prioritize risks for further action Risk management.

1.6 OPERATIONAL DEFINITIONS

An operational definition is a definition that defines the exact manner in which a variable is measured (Held, 2009). Giving the steps used in defining each variable allows others to evaluate and potentially replicate a research study.

1.6.1 Operational definitions for Risk Management Culture

1. **Risk management awareness**: *familiarly about risk management among employees*
2. **Importance of Risk assessment:** *To understand how important risk assessments are to the organization for creating awareness of hazards and risks.*
3. **Risk Assessment Capacity:** *The ability of the organization to conduct a comprehensive risk assessment.*
4. **Training on risk:** *The availability of training courses and materials for the employees.*
5. **Interest to learn about risk management:** *The initiatives taken by the employees to learn about risk and its mitigation.*
6. **Familiar with ISO31000 and ISO31010:** *The familiarly of the employees with the guidelines of ISO31000 for risk management and ISO31010 for risk assessment techniques.*
7. **Risk well understood in the department:** *At the department of electoral affairs, how well is risk understood.*
8. **Perception of employees of Risk:** *To find out if employees have a common perception on what risk means for the company / business?*
9. **Encouragement of risk identification:** *To discover if management of MOI encourage among employees to report of events in order to identify the risks.*
10. **Communicating issues related with risk:** *How effective is the communication about the risk to the employees and top decision makers.*
11. **Risk management effectiveness:** *If there is a risk management policy, how effective is it.*
12. **Organizational Support on Risk:** *The existence of clearly defined organizational structure at organization level in order to sustain the risk management process.*
13. **Robust Risk assessment:** *The existence of Robust Risk assessment such as the ISO31010.*
14. **Professional training on Risk:** *To find out if there is Professional training methods used to facilitate the knowledge improvement on risk.*

15. **Information on Risk:** *Previous information about risk, such as enough data on events history, thus the organization could learn from its own mistakes.*
16. **Risk management culture:** *is the system of values and behaviors present in an organization that shapes risk decisions of management and employees.*
17. **Inspection on Risk:** *To find out if there are any inspections plans implemented so that reductions of the inherent risks can be achieved, which are periodically revised.*
18. **Existence Warning Systems:** *The existence of any monitoring systems in the potential high risk areas that identify the changing of risk level.*
19. **Risk transfer:** *To find out If there is a policy that can be used as an instrument for risk transfer or sharing with other organizations (e.g. insurance companies).*
20. **Risk review:** *The process of risk review after implementation of the mitigation measures / controls for identified risk.*

1.6.2 Operational definitions for Respondents Profile

1. **Job position:** *The position of employees as either senior staff or junior staff.*
2. **Education:** *The education level ranges from High school, Diploma, Bachelor's Degree and Other (postgraduate diploma, masters or PhD)*
3. **Age:** *This is the age of the employees in the organization*
4. **Department:** *There are two departments involving here; Electoral Department and IT Department.*

1.6.3 Operational definitions for Respondents Profile

1. **Voter cheating by ink removal:** *If there is voting fraud by which the voters attempt to cheat removing the ink on their fingers.*
2. **Voter cheating by using different machines:** *If there is voting fraud by which the voters attempt to cheat using different machines at different times and different locations.*

3. **Errors due to lack of knowledge:** *In the case of the citizens committing mistakes due to their lack of knowledge on using the e-voting.*
4. **Hardware failure:** *The failure of voting equipment, computer machines and computer peripherals.*
5. **Hardware failure is worst risk:** *If the worst perceived risks comes from the hardware failure.*
6. **Paper work as an alternative of voting:** *In case of the total failure of the e-voting, if paper work can be used as an alternative method.*
7. **Power failure is worst risk:** *If the worst perceived risks comes from the power failure.*
8. **Software failure is worst risk:** *If the worst perceived risks comes from the software failure.*
9. **Software failure:** *The failure of software involving voting equipment, computer machines and computer peripherals.*
10. **Voting Process Faster:** *How fast is the voting process using e-voting.*

1.7 THESIS ORGANIZATION

This thesis consists of five chapters. Each chapter of the thesis covers the component topic that forms the structure of this research. The chapters are organized according to the role that each component plays in the structure.

Chapter 1 The current chapter gives an introduction to this research, including statement of the problem, objectives of the study, proposed methodology, significant of the study, organization of the dissertation and conclusion.

Chapter 2 presents a literature review of general theories related to Electronic voting and associated risks as well as theories that are specific to the implementation and adoption of e-voting initiatives. In considering these various theories of technology adoption, emphasis is placed on how the approaches relate to aspects of e-voting

Chapter 3 presents the method used as a quantitative approach one and the data collection starts with interview of employees working with election department and information technology department of MOI.

Chapter 4 focuses on the findings of the research. The descriptive analysis of the findings is presented accordingly. This findings include the demographic characteristics of the research sample, risk management culture and risk assessment of the old e-voting

system. The results from the AHP model helped the fundamental concepts of the new e-voting model. The new e-voting system challenges the risk issues of the old e-voting system.

Chapter 5 is the final chapter of the project and it presents the conclusions of e-voting risk analysis outcomes of the country of Oman. There are of four sections. The chapter begins with the research summary, followed by the contribution of the study, future research and recommendations.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Having explained in the previous chapter how e-voting technologies and voting processes can have risks on the electoral process and system which can have drastic effects on the broader concepts of e-governance and e-democracy, this chapter provides a literature review of general theories related to Electronic voting and associated risks as well as theories that are specific to the implementation and adoption of e-voting initiatives. In considering these various theories of technology adoption, emphasis is placed on how the approaches relate to aspects of e-voting

2.2 ELECTRONIC VOTING (E-VOTING) PARADIGMS

Electronic voting (e-voting) systems are characterized by the control of some procedure within the voting process; which is performed by computerized electronic means. In such systems the ballots are directly recorded electronically. According to Sako (2011), depending on the context, it may include voting systems that use electronic devices for reading paper ballots, such as punch cards and optically marked ballots. Generally speaking, depending on the technology used by the e-voting systems, they are typically classified into the following four e-voting paradigms: Mixnets (Peng (2011);Peng et al. (2011); Sebé et al., (2010); Commitments Brassard et al.(1988)), Homomorphic tallying Kiayias (2002); Pengetal(2004) and Blind signature-based (Fujioka et al., 1993;Ohkubo et al., 1999).

Analysis of scheme in Chaum (1981) only satisfies eligibility, privacy and individual verifiability properties as illustrated in Table 2.1. Hence the scheme is not accurate or robust. When a voter detects an inaccuracy (complaining voter), in order to protect privacy of the voter, redoing the election process is inevitable.

Table 2.1
Comparison of e-voting schemes

Scheme/property	**Eligibility**	**Privacy**	**Verifiable**	**Dispute-free**	**Accuracy**	**Fair**
Chaum (1981)	✓	Com	Ind	×	×	×
Chaum (1988)	✓	Com/Max	Ind	×	×	×
Boyd (1990)	✓	Com/Max	Ind	×	×	×
Sako& Killian (1995)	✓	Com	✓	×	✓	C
Chaum (2004)	✓	Com	Ind/CU	×	C	C
Cohen & Fischer (1985	✓	Com	✓	×	✓	×
Cohen & Yung (1986)	✓	Com	✓	×	✓	C
Benaloh (1987)	✓	Com	✓	×	✓	C
Iverson (1992	✓	Com	Ind	×	C	C
Sako& Killian (1994)	✓	Com	✓	×	✓	C
Cramer et al. (1996	✓	Com	✓	×	✓	C
Hirt&Sako(2000)	✓	Com	✓	×	✓	C
Baudron et al.(2001)	✓	Com	✓	×	✓	C
Lee & Kim (2002)	✓	Com	✓	×	✓	C
Okamoto(1997)	✓	Com	Ind	×	×	C
Golle et al.(2002)	✓	Com	Ind/CU	×	C	C
Lee et al.(2003)	✓	Com	✓	×	✓	C
Kiayias& Yung (2004)	✓	Com	✓	×	✓	C
Acquisti(2004)	✓	Com	Ind	×	C	C
Zhao et al.(2014)	✓	Com	Ind	×	X	C
Chen et al. (2014)	✓	Com	Ind	×	X	C
McCarthy et al. (2014)	✓	Com	Ind/CU	×	C	C
Su et al. (2014)	✓	Com	Ind	×	X	C

The keys for symbols in the table are :✓*Satisfied*; x, *not satisfied*; C, *conditionally satisfied*; Com, *computational privacy*; Max, *maximal privacy*; Ind, *individually verifiable*; CU, *conditionally universally verifiable.*

Fairness property is however, lost when there is a re-election, since partial tally would have been revealed previously and may affect the decisions of voters in the re-election. Table 2.1 is comparison of e-voting systems spanning for more than 3 decades.

Starting from 1981 with Chaum (1981) model until as recent as 2014 models developed by McCarthy et al. (2014), Su et al. (2014) etc. Another disadvantage of Chaum (1981) is that a collusion of all the mixes would breach privacy of the voter. This weakness is addressed by the schemes in Brassard (1988). The first technology of e-voting that was introduced was the Blind signatures. Chaum (1983)was the pioneer of the Blind signature technology. Such technology belongs to a class of digital signatures that allow signing data without revealing its contents. In the process of e-voting, "a ballot is blinded in order to achieve its confidentiality requirement. While according to Ibrahim et al. (2003) a voter is required to get the signature of a validator when he/she votes.

The subsequently, the next technology introduced was the Commitments. The Commitment schemes were formally defined by Brassard et al. (1988).When using the commitments, a protocol player (e.g., voter) chooses a value from a (finite) set and commits her choice (e.g., an electoral candidate). Such choice cannot be changed and must not be revealed or exposed. It is possible that the player, although, may choose to disclose the value (anonymously) at some later time. In an e-voting system, the most common commitment used are the Pedersen commitments (Pedersen, 1992), due to their ability to provide information-theoretic privacy or perfectly hiding the information. This is also known as the everlasting privacy Aumann (2002). Homomorphic cryptography e-voting system was introduced as a technology that can maintain the voter anonymity and the ballot privacy.

These are the e-voting schemes that makes use of the homomorphic cryptosystems (Cohen & Fischer, 1985; Paillier, 1999) to encrypt ballots so that when ciphered ballots are operated among them, their result is a cryptogram with the accumulated votes from all voters. It is believed that this scheme is very efficient and resourceful for the tally phase, since there are only few decrypting operations. These decrypting operations are necessary for the achievement of the elections' results while maintaining the voter anonymity and ballot privacy during the whole process. Another technology was introduced using mixed servers. This technology is called Mixnets.

According to (Chaum, 1981) this technology when applied in the e-voting system provides an anonymous control channel that does the shuffling the casted votes and prevents the correlation of their order. Such service is achieved by implementing a set of

mixing servers. The process starts when each server receives the votes, permutes their order, transforms the votes (typically re-encrypts or decrypts the votes) and finally, sends the votes to the next server. While the transformation is done at the in the re-encryption servers, which accomplishes the encryption of each vote.In contrast, in the decryption servers, the vote is encrypted as many times as the number of mixing servers. These layers are removed when votes go through the servers. In both cases, it is hard (not possible nowadays) to correlate any output with its input. Once the votes have crossed the last mixing server, these have been disassociated from their voters (Jardí-Cedó & Pujol-Ahulló, 2012).The implementation of fully robust and practical mixnets can lead to efficient tallying process when compared a tally based on homomorphisms as claimed by (Peng, 2009; Peng, Aditya, Boyd, Dawson, & Lee, 2005).

Some of these technologies include, as part of the protocol as a whole, the performance of tests to verify that the information given is unchanged (eg voter`s vote was cast and counted as intended), without revealing information. In order to achieve this goal zero-knowledge proofs (ZKPs) are used. They may differ in technology, according to the technique of encryption in use, while still providing completeness; as mentioned in Goldreich et al. (1987). It is based on the principle that if the test is true, an honest verifier will be convinced by an honest prover. Soundness is based on the principle that if the test is false, a cheating verifier will convince the honest prover only at a small probability. Zero-knowledge is based on the principle that if the test is true, a cheating verifier only learns this mere fact, nothing about its content.

A new modification was proposed by Radwin (1995); This paradigm where voters must go to the office of the voting authority office (which acts as the authentication authority) and then the voters ask for pseudonyms. Later, the voter will attach their blindly signed pseudonyms to the vote and will send it to the polling station through an anonymous channel. If some of the voters try to cheat by casting two or more votes, their identity could be disclosed. In this proposal, the vote is not blindly signed. Instead, a credential is needed which has been blindly signed by the authentication server. By means of this credential the voters can demonstrate that they appear in the electoral roll.

This approach increases the robustness of the protocol against attacks to the authentication server because the blind signature can be done before the election begins.

Subsequently, Mu & Varadharajan (1998) proposed an enhancement over the variant of Radwin (1995) in which the interaction between the authentication server and the voters are performed remotely. This new proposal of Mu & Varadharajan (1998) presents numerous security flaws as shown in (Chien, Jan, & Tseng, 2003; Lin, Hwang, & Chang, 2003; Yang, Lin, & Yang, 2004) which permitted fraudulent voters to cast several votes without being detected.

Furthermore, the anonymity of any voter could be exposed by a dishonest authentication server. Lin et al. (2003) and later Yang et al. (2004) suggested some improvements to the scheme; in which they claim to be secure. Hwang et al. (2005) indicated a weakness on the system proposed by Lin et al. (2003 in which an authentication server could determine the identity of the voter related to a given voting credential, and gave a new protocol to solve this issue. Yaser Baseri (2011) described some security flaws on the improvement proposed by Asadpour & Jalili (2009), and presented a new proposal.While Rodríguez-Henríquez et al. (2007) uncovered a vulnerability in the proposal by Hwang et al. (2005) which consequently also influenced the proposal by Yang et al. (2004) which permits, in some particular cases, the authentication server to prevent some voters from casting a vote.

The work of Rodríguez-Henríquez et al. (2007) also presented a new proposal that Asadpour & Jalili (2009) proved to be weak in the sense that a coalition of two deceitful voters would be able to vote several times. The above research indicated that there is always the possibly of attempting to cheat the e-voting system by the voters.

2.3 E-VOTING ADOPTION MODEL

E-voting adoption model is based on Schaupp & Carter (2005) who extended a previous model by Carter & Bélanger (2005). This framework aimed to explore the young citizen's usage of online voting system. College students were surveyed to try to determine what factors might influence their intention to use the electronic voting systems. Voter intentions evaluated despite existing security concerns. The results of this study indicate that user perceptions of compatibility, usefulness, and trust considerably impact the intentions of young citizens to use an e-voting system. If the user had perceived

that an e-voting system is compatible with their use of prior systems, such as e-commerce or e-government services, the user is more likely to adopt an e-voting system.

In addition, the voter's intent to use an e-voting service increases if the service is perceived to be useful. Evaluating what is the effect with respect to trust, a higher level of trust of the Internet is found to have a direct, positive effect on the intention of a voter to use an e-voting system. As a final point, for citizens to adopt e-voting, they must trust and believe that the government will take the necessary steps to ensure a fair and reliable voting process.

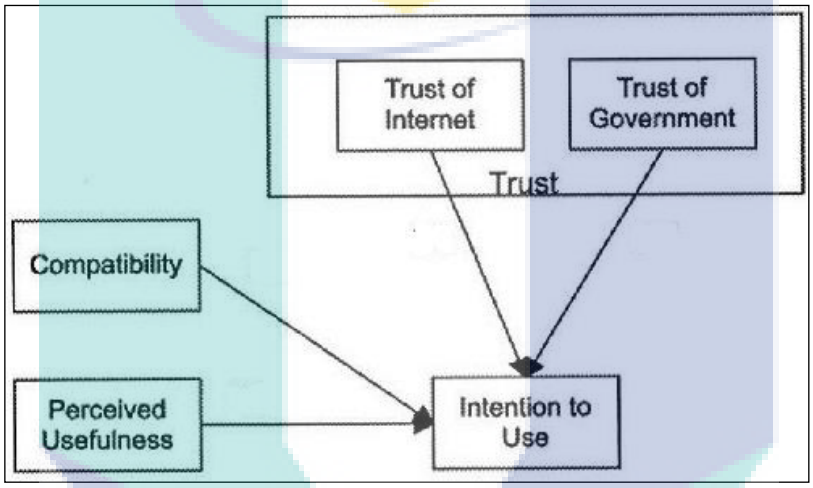


Figure 2.1. E-Voting Adoption Model

Source: Schaupp& Carter, 2005

Figure 2.1 shows the model of adoption of e-voting by Schaupp (2005). In the model of (Schaupp & Carter, 2005), the only important variables considered are the prior use of an e-commerce service and the prior use of an e-government service. The model demonstrates the use of innovative approaches to analyze and predict the intention of users to adopt e-government initiatives or e-voting systems. However, the other authors have expressed concerns about limitations of their work due to a variety of design and methodological factors.

2.4 DIRECT-RECODING ELECTRONIC VOTING MACHINE (DRE)

DRE, which stands for direct-recording electronic which requires voters to use a keyboard or touch screen to mark their votes on a computer terminal, directly connected to a stand-alone, polling-station-located computer Qadah (2007). The votes are immediately added to a running tally stored in the computer's storage system. The final DRE tally is then moved to a central location where it is added to the tallies obtained from other DRE machines. A comparison between DRE and paper-based voting systems is presented in Shamos (2004) claiming that DRE machines pose a number of security risks but that paper based records do no address them as well.

2.5 INTERNET VOTING (I-VOTING)

Although Internet voting (I-Voting) is a recent phenomenon, it traces its technological roots to 1960s, according to King & Williams (2004). The DRE systems were firstly used in a primary election in the United States. The DREs share many of the commonly linked advantages of computerized voting systems, such as fast and error-free counting of votes, consistent interface, and centralization of the voting process Kim & Nevo (2008). As might be expected, they also share many of the weaknesses of e-voting methods, including lack of an auditing trail, the possibility of a large-scale subversion or treason and the risk of failure of the entire system according to (Grove, 2004; D Jefferson & Rubin, 2004).

The advantage of Internet voting (I-voting) is that it has the potential to increase election turnout "attendance" by providing voters with a suitable voting method that does not require them to leave their homes or offices Nevo-Kim (2006). Even geographic distance is no longer a problem in participation in elections for example army personnel and their families (Jefferson et al. 2004), college students Schaupp-Carter (2005), and business people can apply their civic right and vote from anywhere around the world in spite of any time differences as mentioned in (Mohen & Glidden, 2001). The supporter of I-voting argue that it will boost election turnout since it presents voters with a suitable voting method, which allows them to "vote in their pajamas" Mohen (2001). The voting rates are expected to increase since the sick or disabled voters will find the method less physically demanding Nevo-Kim (2006). The cost of voting is minimized because voting

via the Internet can be done around the clock Mohen (2001), thus saving taxpayer's money. Nevertheless, with these advantages I-voting is not considered as a panacea (Nevo, 2006). There is no assurance that rate of voting will increase if I-voting is widely adopted according to Phillips & Spakovsky (2001). Additional to that, even if more people exercise their right to vote, there is no assurance that they will do so out of their free will and not by force Jefferson et al. (2004). Furthermore, there are considerable technical vulnerabilities involved in I-voting that expose the elections to the risk of treason by anti-democratic forces (Jefferson et al., 2004). Lastly, the voter anonymity may be endangered under this voting method (Eliasson, 2006).The opponents of I-voting dispute that giving the voters with an extra voting method is not guaranteed it will increase voting rates; at least not once the novelty of the process is gone Phillips (2001).

The challengers of the I-voting support their arguments by the fact that when American voters were given the option to vote early, or via absentee mail-in, turnout did not increase. While according to Schaupp (2005) as a matter of a fact the current voting rates are steadily heading downward. In addition to that criminals, terrorists, and others who gain from swinging elections may take advantage of the exposure of the technical systems that underlie I-voting by making malicious attacks. This is by is a threat to the foundations of democracy Mercuri (2004).

Therefore, opponents of I-voting claim that the unverified prospective for increased turnout is not sufficient enough to justify the risk of losing voters' trust in the democratic system Jefferson et al. (2004). From technical perspective it is very clear that I-voting is exposed to numerous sources of attacks as claimed by Lauer (2004). Among such technical issues are the viruses and worms, Trojan horses, spoofing, and (distributed) denial of service ((D)DoS). Denial of service is specifically designed to hurt the voting process in general while other attacks may be used to swing elections in favor of one candidate or another (e.g. Trojan horses or Spoofing) according to Jefferson et al.(2004). After lengthy analysis of comparing and contrasting the advantages and disadvantages of I-voting the government of Oman made the decision of not offering I-voting as method of voting. The decision is based on the conclusion that the risks associated with I-voting outweigh its benefits.

2.6 E-VOTING RISKS AND RISK ASSESSMENT

As claimed by Bishop & Wagner (2007) that e-voting has spread throughout the world without satisfactory awareness of reliability, security, or transparency. For example, in today's e-voting systems use of proprietary code and vendors have often asserted the privacy of this code when independent examinations of certified systems were requested. This confidentiality conflicts with the transparency necessary for public elections. Risk assessment for e-voting systems involves assigning a quantitative or qualitative value to the risk of a threat in a specific situation. Assigning a value to the risk of a threat allows the analyst to judiciously allocate relatively scarce resources, conduct sensitivity analysis, perform cost-benefit analyses, and compute residual risk.

As noted by Goldsmith (2011) the Council of Europe recommends that a risk assessment plan must be developed always for an electronic voting and counting technology projects. This is indeed an excellent practice for any project; however electoral projects in particular where timely delivery of voting services are so critical. The risk assessment plan should cover the following potential difficulties if or when they occur. Equipment is late or missing, equipment breaks down, Internet connection fails, software error, hardware failure, power failure, poor voter usability of the e-voting, polling station personnel do not arrive, natural disaster or other emergency etc (Goldsmith, 2011). Thus, the work presented in Kohno et al. (2004) discusses some relevant attacks that can be applied to e-voting infrastructures and also who could perform them. That information is summarized in Table 2.2. Risks of e-voting should be analyzed from different perspectives, starting from the general public level and proceeding to more technical problems. There are a wide variety of risks at each level; in this research will focus on the main and most important risks. Electronic voting systems (electronic voting) effectively reduce the cost of traditional approaches; however, they can also pose other types of challenges for the verifiability of elections. While according to Madise & Martens (2006) the following are the major risks of e-voting: *Incorrectness or untrustworthiness* of the voting results, which remain unnoticed at the time of elections (e.g. voters are illegitimately influenced, multiple votes from one person are counted, a wrong vote is counted and so on). *Breach of the voter's anonymity* (for example, a person's political preferences will be presented to the general public).

Table 2.2
Assessment of relevant attacks on e-voting systems

Attacks	Forgery Vote	Poll worker	Device developer
1. Vote multiple times	✓		
2. Access Admin functions	✓	✓	
3. Modify system configuration		✓	✓
4. Modify ballot		✓	✓
5. Cause votes to be miscounted		✓	✓
6. Impersonate tallying authority		✓	✓
7. Create, delete, and modify votes		✓	✓
8. Link voters with their votes		✓	✓
9. Tamper with audit logs		✓	✓
10. Insert backdoors to e-voting code			✓

Annulment of the elections; which causes interruption of the voting process (for example, due to a major security breach in e-voting). As suggested by (Madise & Martens.(2006) from these three risks, the first two are the most serious.

2.7 SECURITY REQUIREMENTS FOR E-VOTING

In order to be deployed widely, a voting scheme is expected to satisfy certain general security requirements determined by the application of Poovendran (2006) and also some system implementation specific requirements.

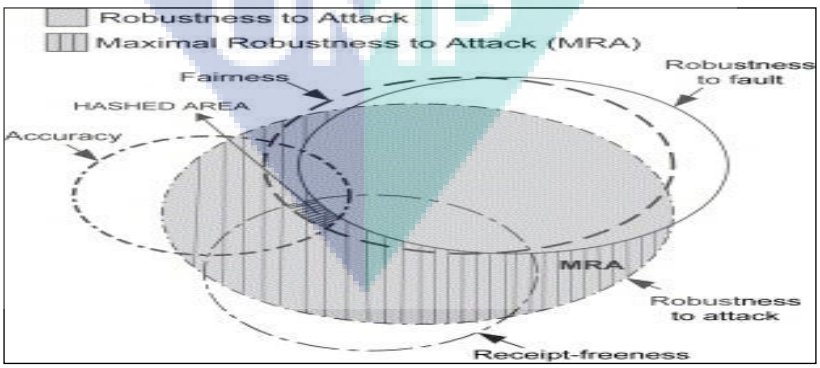


Figure 2.2. Security properties of voting scheme

Source : Sampigethaya & Poovendran, 2006

However, as shown in Figure 2.2 some of the requirements turn out to be conflicting, and tradeoffs often arise in system design. This now presents these

requirements by categorizing them as general security, adversary counter-attack, and system implementation requirements. To be considered secure against adversarial attacks a voting scheme must satisfy additional security requirements.

As shown in Figure 2.2 a Venn diagram showing the connections between several security properties of voting schemes. The intersecting regions establish the properties satisfied and are the planned spaces for voting schemes. For example, the indicated hashed area is the design space for a scheme that should satisfy accuracy, fairness, receipt-freeness and maximum robustness to attack; nevertheless it cannot assure robustness to fault property (Sampigethaya & Poovendran, 2006).

2.7.1 General Security Measurements

Before the deployment of the e-voting system, the voting scheme should satisfy certain general security requirements determined by the application. These security measures are proactive and they provide protection mechanism for any potential attacks that will weaken the system for malicious activities or expose it to dangerous risks. Therefore the e-voting system must provide an uncompromised and secure eligible voters, protect the privacy of the voter, verifiability of the vote, should be dispute-free, fair and accurate.

a) Eligibility

In any voting scheme, only valid voters who meet certain pre-determined criterion are eligible to vote. That means the voter meets the stipulated requirements as an upright citizen that can participate the election and cast his/her vote. According to Devi et al. (2014), an enhanced e-voting system provides an authenticated fingerprint of each eligible voter. The ability to verify voter's validity and a mechanism to ensure that each entity can cast permitted number of votes is a must for a voting scheme as noted by (Sampigethaya & Poovendran, 2006).

b) Verifiability

A voter should be able to verify if his/her vote was correctly recorded and accounted for in the final vote tally results. Mostly in the literature two types are found for this requirement. One is the *individual verifiability* proposed by Sako (1995) where only the voter can verify its vote in the tally. The second is *universal verifiability* also proposed by Sako (1995) where after the tally is published, anyone can verify that all valid votes were included, and the tally process was accurate. According to Sampigethaya & Poovendran (2006) the universal verifiability is more practical since assuming voters to verify their votes individually is not realistic. Verifiability constraint requires voter to be connected to vote, and therefore is in disagreement to privacy. Nevertheless, this prerequisite is very critical in gaining the trust of the voter in the voting system. While Namara et al.(2014) claims that verifiability requirements in an attempt to define requirements of e-voting systems in less formal language while retaining precision.Verifiability of a voter can be attacked, internal adversary attacks may compromise the system for example; as shown in Figure 2.3 let us assume person named voter scans her ballot in an optical-scanner-based (opscan) voting system.

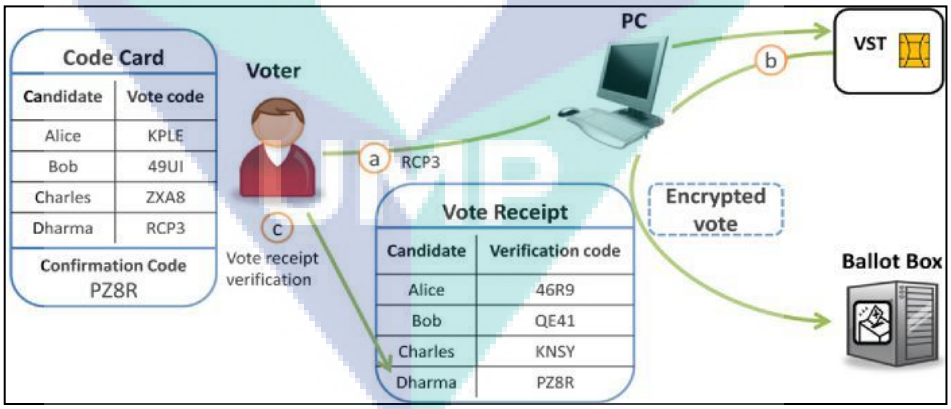


Figure 2.3. Verification overview

Source: Joaquim, Ferreira, & Ribeiro, 2013

Let us also consider that a poll worker is an adversary with enough access rights discards voter's scanned ballot without informing her. When the actions is completed if no proof of that scanning was provided to Voter, she or any other independent observer

could not be sure whether her electronic ballot has been eliminated or modified after her ballot casting as suggested by Joaquim et al. (2013).

In an attempt to solve these issues Joaquim et al. (2013) proposed new model called the EVIV(An end-to-end verifiable Internet voting). The architecture of EVIV is constituted by the Enrolment Service, the Election Registrar, the Ballot Box, the Bulletin Board, the Verification Service using the Voter Security Token (*VST)* and the vote client platform (*PC*). In this case the voter selects the candidate with the vote code and then, the VST creates the vote encryption and receipt and sends them to the Ballot Box through the PC. The voter gets and verifies the vote receipt by checking that the confirmation code on his/her code card is identical with the verification code of the candidate in the vote receipt. The description of EVIV system is illustrated in Figure 2.4. The process starts by presenting the system players which are the Electoral Commission, Voter, Trustees, and Independent Organizations.

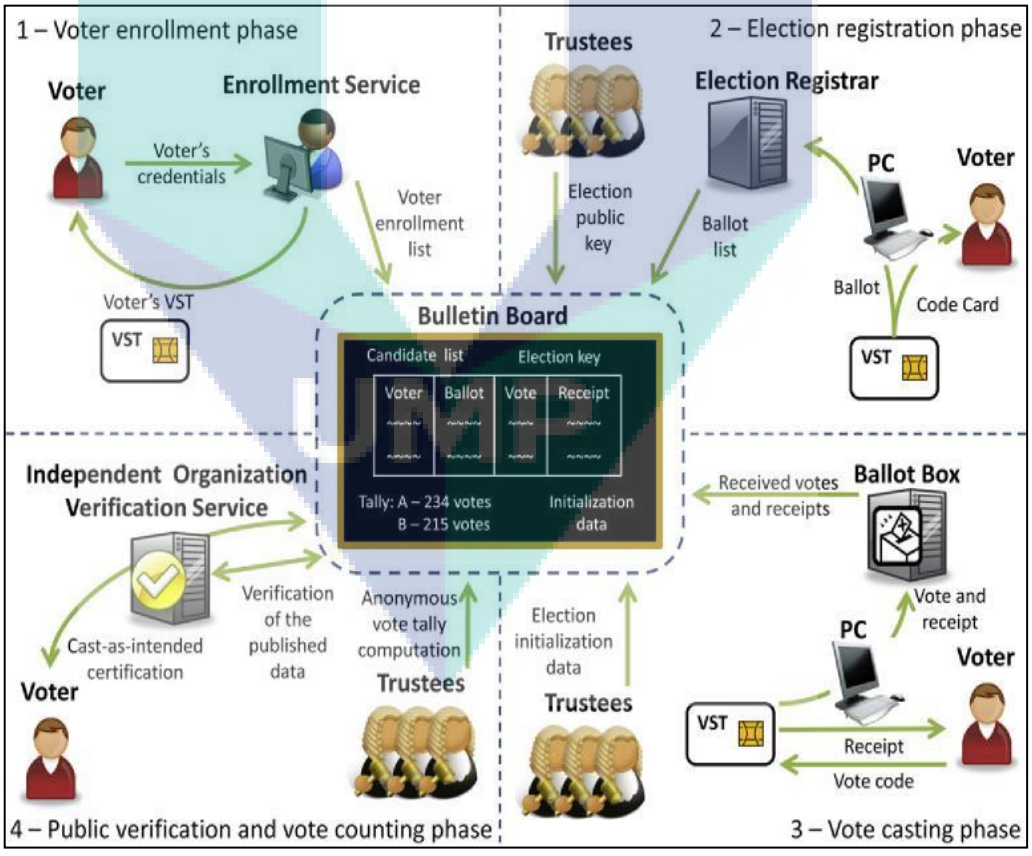


Figure 2.4. Overview of the EVIV vote protocol phases

Source: Joaquim et al., 2013

The phases are presented clockwise starting at the left upper corner with the voter enrolment phase. In this system, the verifiability of the voting system becomes essential for trustworthy elections. This ability is usually considered less than three dissimilar points of view, which leads to individual, universal and end-to-end types of verifications. Briefly speaking, individual verification allows voters to check that their individual ballots are correctly cast and counted. As claimed by Joaquim et al.(2013), universal verification allows voters, electoral and third parties to inspect that the elections' results correspond to cast ballots.

The aim is to ensure that the whole voting process is performed correctly, which, in turn, leads to trustworthy elections' results. In traditional voting systems, both verifications can be achieved by a set of procedures (i.e., manual operations addressed by elections officials, or also by independent entities and observers from candidates). The proposed EVIV system, a voter can check the ballot is correctly cast and counted in the final tally. The goal is to increase the voters' confidence in the elections' results. Note that this property was hardly supportable in traditional voting systems (Joaquim et al., 2013).

c) Privacy

According to Joaquim et al. (2013). In addition to verifiability issues, security holes in the technology used to implement an e-voting infrastructure may also jeopardize the voter anonymity. In a secret ballot, a vote must not identify a voter and any traceability between the voter and its vote must be removed. Maximal privacy is achieved by a voting scheme, if the privacy of a voter is breached only with a collusion of all remaining entities (voters and authorities). In periodic elections, long-term intractability or privacy may have to be provided to the voter. As noted as noted by Sampigethaya & Poovendran (2006), information-theoretically secure cryptographic schemes are used to satisfy this property.

d) Dispute-freeness

According to Sampigethaya & Poovendran (2006) dispute-freeness can simply be achieved through any voting scheme must provide a mechanism to resolve all disputes

in any stage. The notion of universal verifiability is similar but limited to the voting and tallying stages. Since all the stages of this scheme are publicly verifiable, disputes can be resolved by anyone. However; satisfying dispute-freeness can make design of schemes complicated (Sampigethaya & Poovendran, 2006).

e) Accuracy

According to Chen et al. (2014) all voting schemes must be error-free. The votes must be correctly recorded and tallied. All valid votes are counted correctly. A voter's vote cannot be altered, duplicated, or removed. Votes of invalid voters should not be counted in the tally (Chen et al., 2014). Universal verifiability property is directly related to accuracy (Sampigethaya & Poovendran, 2006).

f) Fairness

According to Mateu et al. (2014) since traditional paper-based voting systems are being severely judged after having found, in some cases, evidences of misbehaving parties. This made the confidence on the fairness of an election to decrease. Fairness can compromised both in paper based voting systems or e-voting system. Fairness must be achieved in order to conduct an impartial election; no one should be able to compute the partial tally as the election progresses. According to Chen et al. (2014) only eligible voters are permitted to vote and they can vote only once.

2.7.2 Counter-Attack Requirements

In addition to the general security features, it is still imperative that a voting scheme must be resilient to threats and attacks by an adversary. To guarantee resilience, the following requirements have to be met; in order to utilize after adversary counter-attack. An *adversary* is a malicious entity in the voting model, which attempts to manipulate the voting and/or tallying (Sampigethaya & Poovendran, 2006). An *external adversary* may actively try to coerce a voter or buy a voter, and may passively try to breach the privacy of voters.

An *internal adversary*, apart from breaching privacy, may try to modify or reveal the partial tally as well as corrupt the authority. The e-voting system must possess countermeasures mechanisms that can undertake if threats and attacks occur to the e-voting system during the election process. As claimed by Gjøsteen (2010), in practice, the two most significant security problems are compromised computers and coercion. According to Stenbro (2010), there is no cryptography can defend a voter from coercion while voting from home or some public location, however the system should have attributes that can hinder coercion. As noted in (Haenni & Koenig, 2013) for a counter-measure against coercion or forced-abstention attacks, the registrars have to issue a random number of posting tickets to each vote.

a) Robustness

This property refers to the strength of the system against attacks. The system should be able to face situations in which some voters or authorities are misbehaving so as to try to disrupt the process. A scheme has to be robust against active or passive attacks (corrupt authorities/voters) as well as faults. A voting scheme achieving maximum robustness in the presence of corrupt authorities requires an involvement of all authorities to disrupt the election. But this also necessitates all the authorities to participate in conducting the election. Any non-participating authority can also disrupt the election, leading to zero robustness to faults. Before the election begins, accrediting to Radwin (1995) scheme boosts the robustness of the protocols against attacks to the authentication server since the blind signature can be executed in a noncapital moment.

While according to Mateu et al.(2014)credential based e-voting is more robust than the classical blind signature-based approach. This is due to the voters can ask for their credentials before having decided their vote. In this way, credentials can be provided during a long time period before the day of the election so that there is time for recovering from ultimate attacks against the authentication server. moreover, as noted in Mateu et al.(2014) the use of a distributed polling station as well as increases robustness.

b) Receipt-Freeness

This is the ability that a voter should not be provided with a receipt with which it may be able to prove vote to any other entity. Receipt-freeness has the same notion of un-traceability or privacy. Many schemes offering receipt-freeness are known in the literature such as Benaloh & Tuinstra (1994); Hirt & Sako (2000); Okamoto (1998); Lee et al. (2004). There number of schemes achieves receipt-freeness by using deniable encryption, which allows a voter to produce a fake receipt to confuse the coercer as indicated in (Philip, Simon, & A, 2011; Zou, Li, & Su, 2014).

c) Coercion prevention

Coercion prevention or incoercibility is an important element for security measurements of e-voting after adversary attack. Coercion which is the action or practice of persuading someone to do something by using force or threats can be risk issue of e-voting system. Free democratic elections, voters should have the possibility to cast their votes in full privacy and without any external pressure. A prerequisite to achieve this in remote electronic voting is to prevent the system from providing a receipt, which allows voters to prove to somebody else how (or that) they voted. The absence of such voting receipts disallows voters from selling their votes and protects them from being coerced.

There are many schemes which are known in the literature such as Benaloh & Tuinstra (1994); Hirt & Sako (2000); Okamoto (1998); Lee et al. (2004), that offer receipt-freeness and can also prevent coercion. An adversary may undertake to coerce a voter and influence the manner in which a vote is cast. It is also possible that an adversary may also force a voter to withdraw from casting a vote, or may even represent a valid voter at *any* stage of the voting scheme, by obtaining the voter's private key.

As noted by Sampigethaya & Poovendran (2006) an incoercible voting scheme, will not allow such an adversary to coerce voters. A more formal and even stronger notion of coercion has been proposed by(Juels, Catalano, & Jakobsson, 2005). Their goal is to make remote electronic voting resistant against various forms of coercion. While privacy is defined in terms of an adversary that cannot interact with voters during the election process, it is assumed that a coercive adversary may interact with voters at any time.

Thus an election scheme is called private, if the adversary cannot guess somebody's vote (or the fact that there is no vote) better than an adversarial algorithm whose only input is the final tally, and the scheme is called coercion-resistant, if the adversary can be deceived into thinking thata coerced voter has behaved as instructed. Clearly, a scheme with this property prevents voters from selling their votes or from being coerced.

According to Juels et al. (2005), forcing a voter to vote for a particular candidate selection is only one of several types of coercive attacks. As noted by Joaquim et al. (2013), that, a system that allows a certain individual to link a vote with the voter opens the door to coercibility attacks (i.e., a voter might be coerced into voting for a particular candidate).

The following topics describe other coercive attacks applicable to remote electronic voting, which a coercion-resistant system must address. The **randomization attack**, voters are forced to vote for a random selection of candidates. The goal of this attack is to nullify with high probability the choice of the group of voters under attack, for example by selecting them from an area with a well-predictable election outcome. Note that for the success of this attack, the attacker (and perhaps even the voters) does not need to learn the actual candidate selection.

The **forced-abstention attack**, voters are forced to abstain from participating in the election, either by not casting a vote at all or by casting an invalid vote. With respect to its goal and effectiveness, this type of attack is closely related to a randomization attack, however much easier to achieve. By simply observing the public bulletin board in a scheme prone to this kind of attack, no direct interaction with the coerced voter is needed.

The **simulation attack**, voters are forced to hand over the legitimating to vote, for example by handing out the private voting credentials to the coercer, which can then impersonate (simulate) the coerced voters and hence vote on their behalf. For remote e-voting internet voting there is a scheme that is resistant against both the selling of votes and the coercion of voters. It is called JCJ-scheme which has been proposed by Juels, Catalano, and Jakobsson as claimed in (Juels et al., 2005). Figure 2.5 depicts the original

JCJ-scheme in which the filter initially eliminates votes with invalid proofs, the second filter eliminates duplicate votes, and the third filter eliminates fake votes by checking them against the electoral register.

The JCJ-scheme is the first remote electronic voting scheme that offers full coercion-resistance under minimal assumptions. The so-called "JCJ-scheme" uses an anonymous authentication mechanism to guarantee that the identities of the voters remain hidden during the whole voting and tallying process. The anonymous authentication mechanism requires that during the registration phase each voter receives a secret credential over an exploitable (un-tap-able) channel. According to Haenni & Koenig. (2013), the knowledge of the secret credential permits the voter to post a non encrypted vote anonymously to the public bulletin board, such that its inclusion in the final tally is guaranteed.

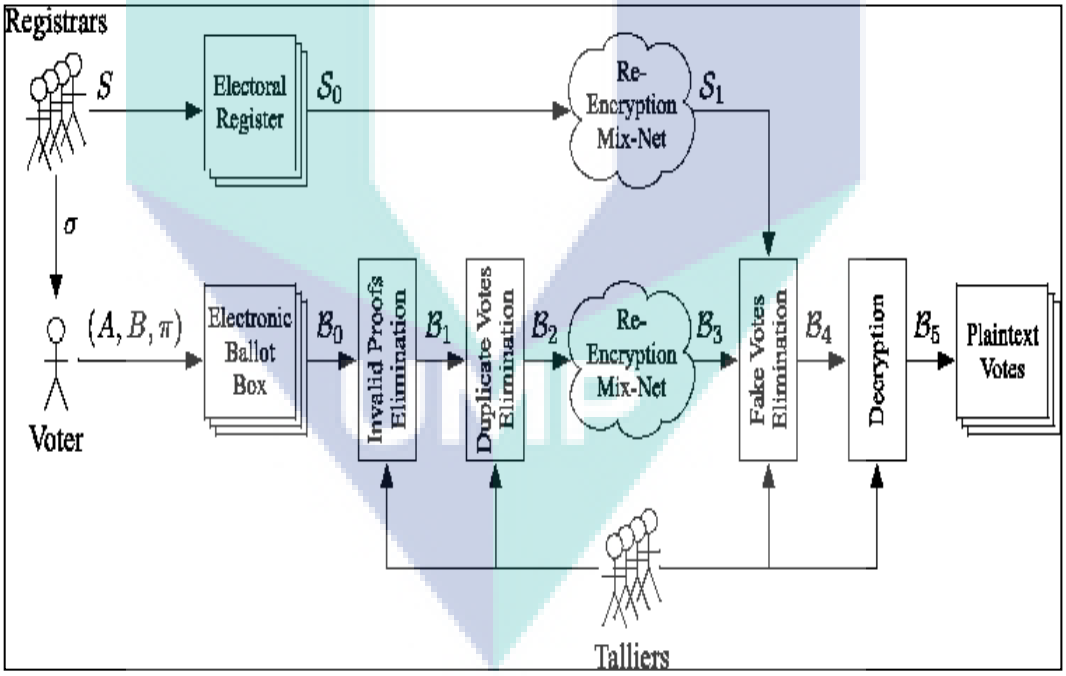


Figure 2.5. Overview of the JCJ-scheme

Furthermore, it is also possible to post invalid votes based on counterfeit credentials, but those will be filtered out later during the tallying phase. Given the fact that both types of board entries are indistinguishable, then it is always possible to lie as claimed by Haenni & Koenig. (2013).

In conclusion, as suggested by Joaquim et al. (2013), the ideal e-voting schemes should consider these issues in order to provide proper verifiability, ensure voter anonymity and reduce the costs in comparison with the traditional voting approaches.

2.8 HISTORICAL PERSPECTIVE ON E-VOTING ISSUES

In this section we issues faced by countries with e-voting projects. Here we discuss the problems faced by the USA and Estonia for using e-voting system.

2.8.1 The Case of USA

According to a report from Electoral Knowledge Network (2014), the polling places of e-voting have affected the 2004 presidential election. Since there were widespread reports of voting terminal failures, and growing concern about the security of these machines that raised debates over how to ensure the integrity of the presidential elections. An important part of this discussion has focused on whether to equip direct recording electronic (DRE) voting terminals with a voter-verifiable paper audit trail (VVPAT). Seven states have directives or laws requiring VVPAT, and 14 others have introduced similar legislation. Federal legislators considered reforms that would mandate a VVPAT for DREs(ACE Electoral Network 2014).A wide debate about the practicability and feasibility of remote e-voting has evolved after the Secure Electronic Registration and Voting Experiment (SERVE) designed for expatriates participation in the US presidential elections of November 2004, was stopped in spring 2004 based upon a report of four members of a review group financed by the Department of Defense. Experiment (SERVE), that allowed citizens and their families who were living overseas to use their personal computers (PCs) to register and vote electronically via the Internet in the 2004 general election (FVAP 2004; Stewart 2011; Joaquim et al. 2013).

It was finally recommended shutting down the development of SERVE immediately because they considered the Internet and the PC as insufficiently secure to cast a vote. The SERVE system was planned for deployment in the 2004 primary and general elections, and would have allowed the voters overseas and military personnel to

vote entirely electronically via the Internet, from anywhere in the world. SERVE was canceled in response to specific security concerns (Stewart, 2011). Security risks was identified by Jefferson et al. (2004) the SERVE project that included a lack of audit trails, privacy issues, and the potential for large-scale vote manipulations.

2.8.2 The Case of Estonia

Based on a report from the Estonia E-voting Organization (2014), before the European Parliamentary elections on May 25, 2014, an international team has acknowledged major risks in the security of Estonia's Internet voting system as shown in Halderman et al. (2014). The team also recommended its urgent withdrawal from the e-voting system. Estonia is the only country in the world that relies on Internet voting in an important way for nationwide elections. This e-voting system has been used for Estonia's national parliamentary elections, municipal elections and is planned to be used for the upcoming European Parliamentary elections.

The Estonia E-voting Organization has claimed that reasearch in recent polls; between 20 percent and 25 percent of voters cast their ballots online. But the nation's Internet voting system cannot guarantee fair elections because of fundamental security weaknesses and poor operational procedures, security and Internet voting researchers have found(EEO, 2104; Madise & Vinkel, 2014). The analysis performed by the team members revealed that sophisticated attackers could easily compromise the integrity of the country's Internet voting system and influence an election's outcome, quite possibly without a trace.

The researchers recommend that the system should immediately be discontinued. These observations – and subsequent security analysis and laboratory testing – revealed a series of problems: Operational security is lax and inconsistent. Transparency measures are insufficient to prove an honest count as indicated in (Halderman et al., 2014). And the software design is highly vulnerable to attack from local criminals or foreign powers.

As shown in Halderman et al. (2014) everything appears normal, but the final count produces a dishonest result. While some of the problems can be corrected in the short term through changes to the system, others stem from fundamental weaknesses that

cannot be fixed. With the growing risk of state-level cyber attacks, the team unanimously recommends discontinuing Internet voting until there are fundamental advances in computer security Halderman et al. (2014).

2.9 ANALYTICAL HIERARCHY PROCESS(AHP)

The Analytical Hierarchy Process (AHP) and survey method was used in this research. In this section only AHP was discussed since the survey method is considered not necessarily significant in the literature review.AHP has been largely applied to macro complex and real problem, and the most addressed decision themes are product and process design and, managing the supply chain. As shown in Subramanian & Ramanathan (2012), most of AHP application are case study oriented and only a few papers aimed at contributing to AHP modeling before applying to practical problems. The review of the researchers has found that significant research gap exists in the application of AHP in the areas of forecasting, layout of facilities and managing stock(Subramanian & Ramanathan, 2012).

The application of AHP in risk management projects is considered modest since there is extensive research indicated strong applications of AHP in risk management. Samvedi et al. (2013) proposed a supply chain risk index, which captures the level of risk faced by a supply chain in a given situation. Their work indicates an effort towards quantifying the risks in a supply chain and then consolidating the values into a comprehensive risk index. As concluded by Samvedi et al. (2013) in their technique for order preference by similarity to the ideal solution (TOPSIS) a robust risk management method which integrates fuzzy analytical hierarchy process (AHP).Using AHP on risk assessment on various projects such energy managements and of solar-thermal power plant projects, design and selection of public policies, and on construction projects as indicated in (Aminbakhsh, Gunduz, & Sonmez, 2013; Aragonés-Beltrán, Chaparro-González, Pastor-Ferrando, & Pla-Rubio, 2014; Moreno-Jiménez, Pérez-Espés, & Velázquez, 2014). Aragonés-Beltrán et al. (2014) work reviewed the current state of the art of solar-thermal power plant projects, and then proposed a decision models based on the AHP. As concluded by Aragonés-Beltrán et al. (2014), the managing Board can reject unfeasible projects before investing heavily in them. Aminbakhsh et al. (2013) proposed

a safety risk assessment framework is presented based on the theory of cost of safety (COS) model and the analytic hierarchy process (AHP).

The main contribution of the proposed framework is that it presents a robust method for prioritization of safety risks in construction projects to create a rational budget and to set realistic goals without compromising safety (Aminbakhsh et al., 2013). It is very clear that literature on AHP applications in e-voting is very limited and modest. The closest AHP application in e-voting is the research of Moreno-Jiménez et al.(2014) proposing a methodology for the design and selection of public policies based on the cognitive democratic model known as e-Cognocracy.

AHP is employed in resolving two issues of e-Cognocracy as mentioned in (Moreno-Jiménez et al., 2014) one is checking the robustness of the model, do the conclusions remain stable when the hierarchy of the problem is slightly modified and second considering the stability of the solutions when confronted with small changes in the judgments of e-Cognocracy. Therefore, there exists a significant research gap on the applications of AHP in e-voting and in general for all e-government services.

2.10 SUMMARY

In the country of Oman, e-voting (electronic voting) is implemented and used for elections. While I-voting (Internet voting) is not yet implemented. After lengthy analysis of comparing and contrasting the advantages and disadvantages of I-voting the government of Oman made the decision of not offering I-voting as method for voting due to the conclusion that the risks associated with I-voting outweigh its benefits. E-voting effectively reduces the cost of traditional approaches; however, they can also pose other types of challenges for the verifiability of election as shown in Kohno et al. (2004). Madise & Martens (2006) heighted major risks of e-voting: Incorrectness or untrustworthiness, Breach of the voter's anonymity, and Annulment of the elections.

Despite these additional challenges and problems, the trend is clear and firm toward using electronic voting means E-Voting.CC and Competence Center for Electronic Voting and Participation (2009), in particular, not only electronic tally, but also electronic vote casting as mentioned in (Esteve, 2008; Williams et al., 2006). However; state of the art research claims weaknesses of e-voting methods, includes lack

of an auditing trail, the possibility of a large-scale subversion or treason and the risk of failure of the entire system according to (Grove, 2004; D Jefferson & Rubin, 2004). Nevertheless; there are other researchers who have done more studies using computer technologies to improve elections Kohno et al., (2004), Neff, (2001), Trechsel (2005). The issues of transparency, security, accessibility and usability of e-voting have been considerably improved and people achieved a sense of reliance on the e-voting system.

The next chapter presents a research design that builds on the literature reviews of this chapter and a case study on the Voter Registration Application System in the country of Oman, which is based on an integrated network of information system. Quantitative approaches were employed based on questionnaires and AHP model.

CHAPTER 3

METHODOLOGY

3.1 INTRODUCTION

This chapter presents the methods that are going to be adopted to conduct this research. The research is initially designed to be a case study on the Voter Registration Application System in Oman, which is based on an integrated network of information systems. In this research a quantitative approach is employed as the research method. Data collection starts with interview of employees working with election department and information technology department of MOI. The old e-voting system was also observed. It is then followed by three questionnaires sessions (in Appendix B) that were created for data collection. Decision model based on Analytical Hierarchy Process (AHP) is also designed to assist the identification of the main weaknesses of the e-voting system.

3.2 RESEARCH DESIGN

The research design is the logical sequence that connects the empirical data produced by research to the study's initial research questions and ultimately to its conclusions (Fellows, 2015). One of the principal purposes of the research design is to help avoid the situation in which the collected data does not address the initial research question (Fellows, 2015). Much research in the social sciences and management spheres involves asking and obtaining answers to questions through conducting surveys of people by using questionnaires, interviews and case studies (Fellows and Liu, 2015).

The aim of this research is to develop a model for e-voting risk assessment for the ministry of interior of Oman. This will be achieved through the use of statistical data analysis and AHP decision making model that will reduce and manage electoral risks. To achieve this aim, collecting data for AHP and statistical model is needed to formulate the model. In order to achieve this purpose, one interview session was conducted and three set of questionnaires (refer to Appendix B) were distributed. Figure 3.1 illustrates the research design flow chart.

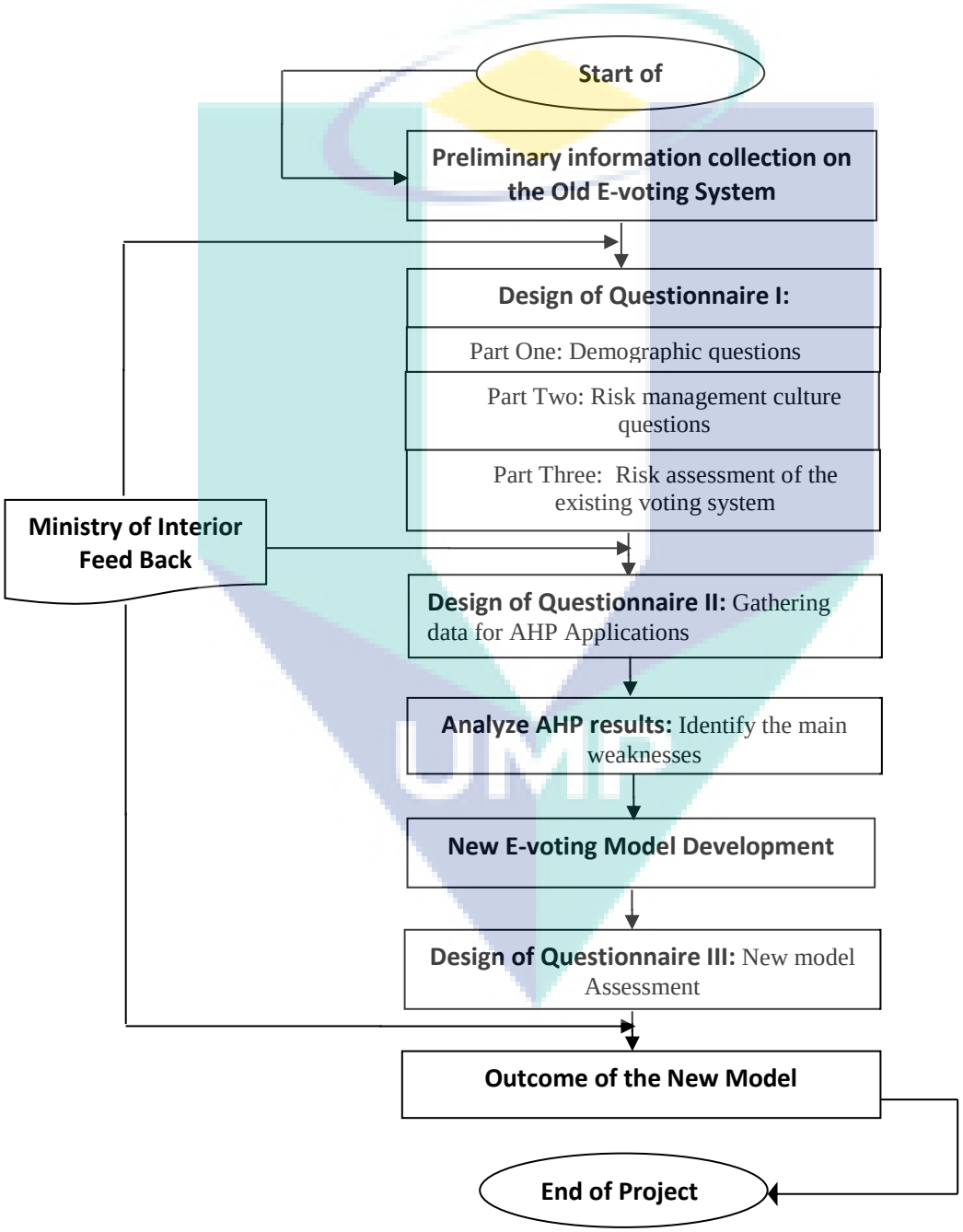


Figure 3.1. Research Design

3.3 INSTRUMENT DEVELOPMENT

After developing a thorough understanding of the research, the next step is to generate statements/questions for the questionnaire. In this step, content (from literature/theoretical framework) is transformed into statements/questions refer to European regional development project on Hungry and Romania (www.mrisk.ro/irm). The targeted respondents are the IT staff working at Ministry of Interior (MOI) and at the department of electoral management. The sample size for the study was 100 employees. This decision was made by using an online sample Size Calculator package software access via this website (www.surveysystem.com). Using Confidence Interval of ±5 and the target population of 300, the sample size was found to be 100.

3.3.1 Questionnaire I: Assessing Risk Management Culture

The researchers have chosen survey questionnaire method since it has advantages over some other types of surveys in that they are cheap, do not require as much effort from the questioner as verbal or telephone surveys, and often have standardized answers that make it simple to compile data. The survey questionnaire (Appendix B) is divided into three sections: socio-demographics questions, risk management culture questions and risk assessment of the existing voting system. Here questionnaire I is designed to answer objective one (1); which is to evaluate the risk management culture on e-voting at the Ministry of Interior by analyzing the risks of the old e-voting system through statistical analysis.

Part One: Demographic questions

Demographic variables are used to depict the characteristics of the people surveyed in the sample. We established in the previous paragraphs that you should only ask those socio-demographics that matter to your research project. Asking the right demographic questions will allow you to discover meaningful and actionable insights to assist you in making better business decisions. Below we discuss the asked socio-demographics:

Job position: To collect information necessary to establish the employee's occupational level.

Work field: Information relating to the practical work conducted by the employee.

Age: It has been shown in various scientific disciplines that opinions on a vast number of topics differ between different age groups.

Education: There are clear differences in opinion between respondents with a different educational level. Moreover, educational level – generally asked as 'the highest level of education completed' – is also quite often used as a proxy for income. It includes such education level as High school, Diploma, Bachelor Degree and Other.

Part Two: Risk management culture questions

In this part we raise questions pertaining to risk management culture. The respondent will be asked how frequently each statement fits the risk and risk management being described. Each factor is measured through the use of a Likert scale, consisting of 5 categories. The data from these questions can be used as a diagnostic tool that can help any organization gauge the effectiveness of its enterprise-wide risk management culture, a key foundation of sustainable risk management and compliance programs. Here the existence of risk assessment regarding election in the electoral and IT department of Ministry of Interior (MOI) examined. Due to their powerful impact on the e-voting system, the following are the main points of the questionnaire to consider: Familiarity of employee on the ISO 31000 and ISO 31010 standards on risk management, Organizational support on risk management, Risk assessment, Professional training on risk management, Information pertaining to risk, Inspections on risks, Warning systems, Risk transfer, Risk review and Limitations of the system, if there is any, as can be seen in Kohno (2004).

Part Three: Risk assessment of the existing voting system

In this part of the questionnaire we assess the risk of the Old E-voting system. Risk assessment is used as the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat or hazard. The employees are asked if they ever encounter risk for example: Hardware failure when voting was in process.

Software failure when voting was in process, Power (electricity) failure, Cheating by using different machines so he/she can vote twice, Encounter voter cheating by ink removal, Errors from voter due to lack of knowledge and Risk of voting process getting slower. These items can be seen in the questionnaire of the risk analysis of the old e-voting system on page 102.

3.3.2 Questionnaire II for Applying AHP

In this part we raise questions pertaining to AHP method. This questionnaire will finally present the weights for the risk management in e-voting. It is anticipated at least three of the following factors will be used: Operator authentication, Reliability, Delectability, Availability of system, Immunity to attack, Integrity of votes, Traceability, Recoverability, Fault tolerance and Isolation. Questionnaire II was designed to answer objective three (3); which is to apply AHP model that can determine the most risky elements in the old e-voting system and the respondents were experts and general managers, directions and head of sections of the MOI.

3.3.3 Questionnaire III for assessing new e-voting system

In this questionnaire we assess the risk of the New E-voting system. Risk assessment is used as the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat or hazard. Here questionnaire III is designed to answer for objective three (3); which is to develop a new e-voting system using citizen ID that reduces the electoral risks. And objective four (4) also; which concerns the evaluation of the strength and weaknesses of the new e-voting system through statistical analysis. The employees were asked if they ever encounter risk for example: Hardware failure when voting was in process. Software failure when voting was in process, Power (electricity) failure, Cheating by using different machines so he/she can vote twice, Encounter voter cheating by ink removal, Errors from voter due to lack of knowledge and Risk of voting process getting slower.

3.4 THE APPLICATION OF AHP IN ASSESSING E-VOTING

The analytic hierarchy process (AHP) is a structured technique for organizing and analyzing complex decisions. It is structured multi-attribute decision method that was developed by Thomas L. Saaty in the 1970s and has been extensively studied and refined since then Saaty (1990). Since 1980s the research in AHP still continues according to some recent reviews (Ho, Xu, & Dey, 2010; Vaidya & Kumar, 2006; Zahedi, 1986). Since AHP is an Eigen value approach to the pair-wise comparisons. It also provides a methodology to calibrate the numeric scale for the measurement of quantitative as well as qualitative performances. The scale ranges from 1/9 for *'least valued than'*, to 1 for *'equal'*, and to 9 for *'absolutely more important than'* covering the entire spectrum of the comparison (Vaidya , 2006).

3.5 DATA COLLECTION METHOD

Statistical methods can be used to summarize or describe a collection of data; this is called descriptive statistics. This is useful in research, when communicating the results of experiments. In this research the statistical analysis was conducted to answer six research questions. The tool used in this research is known as SPSS which stands for Statistical Package for Social Sciences (SPSS) program. SPSS is a computer program used for statistical analysis

3.5.1 Data Collection From Questionnaire

Data for this study were obtained by means of two sets of questionnaires given to IT staff working at Ministry of Interior (MOI) and department of electoral management. Using Confidence Interval of ±5 and the target population of 300, the sample size was found to be 100. And out of the 100 questionnaires that were distributed, 82 responded. There were 42 respondents from the IT department of MIO and 40 employees responded from the electoral department. The questionnaire checklist was separated into three sections: Demographic information of the respondents, Risk management culture, and Risk assessment of the existing voting system.

3.5.2 Data Collection From AHP Survey Questionnaire

The analytical hierarchy process (AHP), a hierarchically layered structure, was developed for decision making (Saaty, 2003). It is presented a questionnaire that was specially designed questionnaire for AHP. It is then distributed to ten (10) experts from the Ministry of Interior. Experts include the General Managers of ministry and election affairs, strategic planning director, directors of IT and elections departments, heads of sections (software, hardware, network, information and media etc).

3.6 DATA ANALYSIS

In this research we have used SPSS version 16.0 to perform exploratory data analysis and descriptive statistics. All survey items were tabulated and mean values and ranks were computed for judged risk assessment questions. All data were studied as a whole concerning e-voting risk management.

3.6.1 Descriptive Analysis

The techniques were used in SPSS to create histograms, frequency distributions, calculate the standard measures of central tendency (mean, median, and mode), calculate the standard measures of dispersion (range, semi-inter quartile range, and standard deviation / variance), and calculate measures of kurtosis and skewness. This method has been used for this study in demographic profile that is consists of gender, age, working experiences, qualification, occupation and states. In additional this method has been used to analyze risk management culture and risk of existing system.

3.6.2 Steps of Applying AHP

AHP can help decision makers to: examine a complex problem with a number of possible solutions, evaluate and prioritize alternatives, and organize the information and judgments used in decision making. The analytic hierarchy process allows the relative independent judgments made by people to be used in a more formalized decision making process.AHP derives scales of values from pair wise comparisons in conjunction with ratings and is suitable for multi objective, multi criterion, and multi-actor decisions with

any number of alternatives(Aminbakhsh, Gunduz, & Sonmez, 2013). AHP involves assessing scales rather than measures; hence, it is capable of modeling situations that lack measures (e.g., modeling risk and uncertainty). AHP is comprised of three main principles: decomposition level of the structure, comparison of judgments, and hierarchical decomposition level (or synthesis) of priorities. Decomposing a decision problem into its constituent parts facilitates building hierarchies of criteria to determine the importance of each criterion. Some key and basic steps involved in AHP methodology are described in Table 3.1 as shown below.

Table3.1
Steps of AHP method

Number of Steps	Description
Step one	State the problem.
Step Two	Broaden the objectives of the problem or consider all actors, objectives and its outcome.
Step Three	Identify the criteria that influence the behavior.
Step Four	Structure the problem in a hierarchy of different levels constituting goal, criteria, sub-criteria and alternatives.
Step Five	Compare each element in the corresponding level and calibrate them on the numerical scale. This requires *n(n - 1)/2* comparisons, where n is the number of elements with the considerations that diagonal elements are equal or '1' and the other elements will simply be the reciprocals of the earlier comparisons.
Step Six	Perform calculations to find the maximum Eigen value, consistency index CI, consistency ratio CR, and normalized values for each criteria/alternative.
Step Seven	If the maximum Eigen value, CI, and CR are satisfactory then decision is taken based on the normalized values; else the procedure is repeated till these values lie in a desired range.

AHP helps to incorporate a group consensus. Generally this consists of a questionnaire for comparison of each element and geometric mean to arrive at a final solution. In AHP computing the vector of criteria weights is very essential step. The weighting is mainly determined by the decision makers, who conduct the pair wise comparisons, if there are n evaluation criteria, the decision-makers have to conduct ***C(n,2)=n(n-1)/2*** pair wise comparisons(Liu, 2009). In order to compute the weights for

the different criteria, the AHP starts creating a *pair-wise comparison matrix* A. The matrix A is a $m \times m$ real matrix, where m is the number of evaluation criteria considered. Each entry a_{jk} of the matrix **A**represents[1] the importance of the *j*th criterion relative to the *k*th criterion. If $a_{jk} > 1$, then the *j*th criterion is more important than the *k*th criterion, while if $a_{jk} < 1$, then the *j*th criterion is less important than the *k*th criterion. If two criteria have the same importance, then the entry a_{jk} is 1. The entries a_{jk} and a_{kj} satisfy the following constraint:

$$(a_{jk})x(a_{kj}) = 1$$

Obviously, $a_{jj} = 1$ for all j. The relative importance between two criteria is measured according to a numerical scale from 1 to 9, as shown in Table 3.2, where it is assumed that the *j*th criterion is equally or more important than the *k*th criterion (Saaty, 1980).The phrases in the "Interpretation" column of Table 3.2 are only suggestive, and may be used to translate the decision maker's qualitative evaluations of the relative importance between two criteria into numbers. Table 3.2 shows the evaluation hierarchy structure. Then the evaluation measurement of ratio scale is employed to conduct pair wise comparison to clarity the relative importance of each attribute.

Table3.2
Relative Scores

***Value of** ajk*	***Interpretation***
1	*j*and*k*are equally important
3	*j*is slightly more important than *k*
5	*j*is more important than *k*
7	*j*is strongly more important than *k*
9	*j*is absolutely more important than *k*

It is also possible to assign intermediate values which do not correspond to a precise interpretation. The values in the matrix **A** are by construction pair-wise consistent. On the other hand, the ratings may in general show slight inconsistencies. However; these do not cause serious difficulties for the AHP.

3.7 SUMMARY

This chapter presented the methodology that was adopted in odrer conducted a very successful research. The research is initially designed to be a case study on the Voter Registration Application System in Oman, which is based on an integrated network of information systems. In this research a quantitative approach is employed as the research method. Data collection starts with interview of employees working with election department and information technology department of MOI. At MOI, the existing old e-voting system was also observed. It is then followed by three questionnaires sessions (in Appendix B) that are introduced to collect data. Questionnaires have benefits over some other types of surveys in such that they are cheap, do not need as much effort from the questioner as verbal or telephone surveys, and often have standardized answers that make it simple to compile data Decision model based on Analytical Hierarchy Process (AHP) is also designed to assist the identification of the main weaknesses of the e-voting system.

CHAPTER 4

DATA ANALYSIS AND FINDINGS

4.1 INTRODUCTION

The findings of the research are reported in this chapter. The descriptive analysis of the findings is presented accordingly. This findings include the demographic characteristics of the research sample, risk management culture and risk assessment of the old e-voting system. The results from the old e-voting system point out the weakness and vulnerability of the system and the possibility of experiencing high risk problems. Based on that, ten (10) experts were given questionnaire for AHP model. The experts provided their judgment on the highest possible risks perceived from the old e-voting system. Therefore an AHP model is built. The results from the AHP model helped the fundamental concepts of the new e-voting model. The new e-voting system challenges the risk issues of the old e-voting system.

4.2 RELIABILITY TEST

It is a primary objective of the recommendation that "e-voting shall be as reliable and secure as elections and referendums which do not involve the use of electronic means" and it thus appears to the Commission that the recommendation is a useful benchmark by which to evaluate the proposed migration from paper to electronic voting methods in Oman. The Recommendation incorporates guidance on how to design, implement, operate and supervise e-voting systems to ensure that they are as reliable and secure as traditional paper-based methods.

Due to limited space other items were omitted. However; it has shown the similar reliability test of above 0.70. Cronbach's alpha ranges from 0 to 1.00, with values close to 1.00 indicating high consistency. It is desirable to have a reliability coefficient of 0.70 or higher. As shown in table 4.1, the results show that Cronbach's Alpha is 0.739. The alpha coefficient for the nineteen (19) items is 0.739, suggesting that the items have relatively high internal consistency. This shows that the data is reliable (Santos, 1999).

Table 4.1
Reliability Statistics

Reliability test using Cronbach's Alpha	
Cronbach's Alpha	.737
Number of Items	19

And Table 4.2 shows detailed variables with its corresponding reliability tests. Reporting errors with reliability measures while most individuals utilizing Likert-type scales will report overall scale and subscale internal consistency reliability estimates in the analysis of the data, many will analyze individual scale items.

Table 4.2
Reliability Item-Total Statistics

	Factors	Scale Mean	Scale Variance	Total Correlation	Cranach's Alpha
1.	Risk management awareness	52.5610	55.089	.207	.735
2.	Importance of Risk assessment	51.9024	55.052	.240	.732
3.	Risk Assessment Capacity	52.4512	55.386	.284	.729
4.	Training on risk	53.2927	52.407	.371	.721
5.	Interest to learn about risk management	52.1585	51.913	.427	.716
6.	Familiar with ISO31000 and ISO31010	53.7073	50.975	.380	.719
7.	Risk well understood In the department	52.9146	52.277	.433	.716
8.	Perception of employees of Risk	52.9268	53.254	.317	.725
9.	Encouragement of risk identification	52.5976	53.626	.330	.725
10.	Communicating issues related with risk	52.4146	53.258	.393	.720
11.	Risk management effectiveness	51.8415	54.925	.254	.730
12.	Organizational Support on Risk	52.7439	54.736	.176	.739
13.	Robust Risk assessment	53.7073	53.987	.353	.723
14.	Professional training on Risk	53.8171	53.781	.381	.721
15.	Information on Risk	53.0122	53.049	.287	.729
16.	Inspection on Risk	53.4878	53.685	.306	.726
17.	Existence Warning Systems	53.3293	50.446	.433	.714
18.	Risk transfer	54.1098	56.741	.082	.745
19.	Risk review	53.4878	55.660	.217	.733

Here reliability test is used by employing The Cronbach's alpha coefficient of internal consistency. One of the most popular reliability statistics in use today is Cronbach's alpha (Santos, 1999). Cronbach's alpha is a measure of internal consistency, that is, how closely related a set of items are as a group. It is considered to be a measure of scale reliability. It is generally used as a measure of internal consistency or reliability of a psychometric instrument. Furthermore, and although the recommendation is broadly based in terms of the democratic principles underpinning elections that are conducted by electronic means, its specific objective of ensuring the reliability and security of such elections corresponds very closely with the Commission's mandate in relation to the secrecy and accuracy of the chosen system.

4.3 RESPONDENTS PROFILE

The sample distribution is discussed through the findings of four demographic elements: Job position**,** Education, Age, and Department. From the 100 questionnaires distributed to the respondents, 82 completed surveys were collected, which yielded a response rate of 82%. These variables are used to identify the respondents' background, which included the elements of Job position, Department, Age and Education.

4.3.1 Job Position

Table 4.3 showed that the distribution of the respondents by occupation levels were 18% for senior staff and 82% for junior staff. This distribution showed that there were significantly less senior staff respondents compared to non-senior staff and the difference was 17.8 %.

Table 4.3
Frequencies of Job position Variables (N=82)

Position	Frequency	Percentage (%)
1. Senior staff	15	18%
2. Junior staff	67	82%
	82	**100**

4.3.2 Educational Level

Educational levels ranged from High school to Bachelor's Degree. This clarifies differences in opinion between respondents with a different educational level. From Table 4.4, the distribution of the respondents by education level was as follows; 21 respondents (26 %) were High school holders, 26 respondents (32 %) were Diploma holders, 30 respondents (37 %) were Bachelor's Degree, 5 respondents (6 %) were holding other degrees such Master or Postgraduate diploma.

Table 4.4
Frequencies of Educational Level Variables (N=82)

Educational Level	Frequency	Percentage (%)
1.High school	21	26%
2.Diploma	26	32%
3.Bachelor's Degree	30	37%
4.Other	5	6%
	82	**100**

4.3.3 Department

Table 4.5 shows the distribution of the respondents by Department. Number of employee responded to the questionnaire from the Electoral department were 42 %, while the number of respondents from the IT department were 58 %.

Table 4.5
Frequencies of Department Variables (N=82)

Department of work	Frequency	Percentage (%)
1. Electoral Department	40	48.8%
2. IT Department	42	51.2%
	82	**100%**

This distribution showed that there were more IT department respondents compared to Electoral department. The difference was 8 %.

4.3.4 Age

The age of the respondents is being analyzed and the distributions of age among respondents are shown in Table 4.6. Based on the Table 4.4, there were 29 respondents (32.2 %) who were under the category of age between 20 and 29.

Table 4.6
Frequencies of Age Level Variables (N=82)

Age	Frequency	Percentage (%)
1. 20-29	33	40%
2. 30-39	27	33%
3. 40-49	20	24%
4. 50 and Above	2	2%
	82	**100**

Twenty one (21) respondents (23.3 %); who were under the category of age range between 30 and 39. Twenty (20) respondents (22.2 %) who were under the category of age between 40 and 49 and lastly, there are 20 respondents (22.2 %) who were under the category of 50 and above.

4.4 ANALYSIS OF THE OLD E-VOTING PROCESS

In this section, collection of important information pertaining to the old e-voting system was performed with purpose of investigating weaknesses. Employees from both the information technology department and election department of the Ministry of Interior (MOI) have been interviewed. Also numerous observations were carried out against old system.

4.4.1 Interviews and Observations

Interviews were conducted with employees working with election department and information technology department of MOI. This interview was informal and based on questions and discussions. Ten questions with seven of them open ended and three closed questions were asked. Respondents also commented on their perspective of the system and issues relating with existing E-voting system.

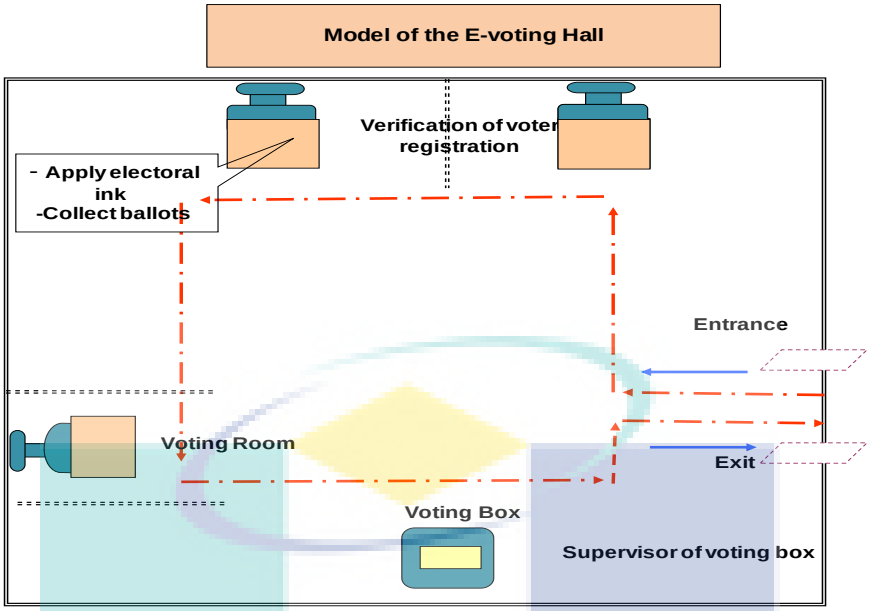


Figure 4.1. Old system voting hall model

Observation on the old e-voting process indicated it has a number of weaknesses and strengths. The Figure 4.1illustrates the voting hall model and the follow of process. The voter enters the building and starts the process of verification if the voter is registered voter or not. Then the voters get ink applied in their fingers. Voters collect the ballots and head for the voting room.

4.4.2 Interview Results on the Analysis of the Old E-Voting Process

Here among the people interviewed were the director of the election department, director of IT department director and the deputy director of the IT department in the MOI. There are some advantages in this old system. Such advantages include the possibility to use passport of the voters, those who does not have a valid resident card. The time taking for authorizing the voters are less compare to normal elections, so it is possible to eliminate large queue formation in front of voting centers.

The voting software and databases are running locally in a disconnected environment. So any kind of hacking, failure of network or server issues can eliminate and can ensure smooth running of elections. Always keeps one back up for every local server, so it is decrease the down time in the case of failures. Nevertheless, the

disadvantages are many in the old system. Such issues include, whenever any voters that has a resident card, come with passport instead of his valid resident card, the person could not vote because the passport number is not always be recorded in case that person is holding a valid ID card.

It is difficult to track a person, is used other registered voters identity card for voting purpose. The electoral ink was used to identify the voted person, the voter's feel very uncomfortable for marking the electoral inking on the finger, some of the voters refuses to mark the electoral ink also. The non-elected candidates are trying to complaint about the system, like the fraud voting is possible in case that the people could erase the election ink on their nail, and choose second voting center to vote. And finally the backup servers or PC's increase the cost almost double of actual amount.

In summary there are both some advantages and disadvantages. However; the disadvantages outweigh the advantages for example a voter might erase the election ink and try to vote again, while some candidates are claiming that fraud voting is possible since the ink can be erased. A citizen might attempt to vote more than once from different machines. Other important issues include difficulty in tracking citizens; some voters are not comfortable with the election ink. Therefore, from this interview and observation it was then learned the need to make a full scale analysis involving questionnaire data collection.

4.5 ASSESSMENT OF RISK MANAGEMENT CULTURE

This section provides answer for objective one; which was to evaluate the risk management culture on e-voting at the Omani Ministry of Interior. Risk management culture refers to the way organizations think and act about reducing risk. It is a proactive, institution-wide program where policies, procedures, processes and technology are used to measure, monitor and manage risk (Cooper, Speh, & Downey, 2014). The goal of creating a risk management culture is to create a situation where staff and managers instinctively look for risks of e-voting and consider their impacts when making effective operational decisions. Table 4.7 illustrate the results of the risk management culture questionnaire. In this section we will consider discussing the top three factors and the lowest three factors. Since these factors are posing the highest critical risks.

Table 4.7
Overall ranking of the factors of risk management culture

Descriptive Statistics						
	Risk Factors	**N**	**Min.**	**Max.**	**Mean**	**Std. Deviation**
1)	Risk management effectiveness	82	1.00	5.00	4.0732	.87179
2)	Importance of Risk assessment	82	2.00	5.00	4.0122	.88183
3)	Interest to learn about risk management	80	1.00	5.00	3.7625	.99675
4)	Communicating issues related with risk	82	1.00	5.00	3.5000	.86424
5)	Risk Assessment Capacity	82	2.00	5.00	3.4691	.72606
6)	Risk management awareness	82	2.00	5.00	3.3537	.96061
7)	Encouragement of risk identification	80	1.00	5.00	3.3462	.93735
8)	Organization Support on Risk	82	1.00	5.00	3.1707	1.13099
9)	Risk well understood In the department	82	1.00	5.00	3.0000	.92962
10)	Perception of employees of Risk	82	1.00	5.00	2.9747	1.02500
11)	Information on Risk	80	1.00	5.00	2.9012	1.12478
12)	Training on risk	82	1.00	5.00	2.6296	1.03010
13)	Existence Warning Systems	82	1.00	5.00	2.6125	1.16373
14)	Risk review	82	1.00	5.00	2.4268	.81696
15)	Inspection on Risk	80	1.00	5.00	2.4250	.97792
16)	Familiar with ISO31000 and ISO31010	82	1.00	5.00	2.2278	1.21897
17)	Professional training on Risk	82	1.00	5.00	2.2073	.82758
18)	Risk transfer	82	1.00	4.00	2.0976	.81057

The results supported the mechanism of coping with challenge of creating consistent and workable processes for managing operational risks, the MOI need to adopt a "risk management culture" that emphasizes at all levels the importance of managing risk as part of each person's daily activities. Comparing with table 4.2, one of the factors was left (Risk review); since it is understood it won't have effect on the risk management culture.

(1) Risk management effectiveness; is the highest factor that employees believe importance of having effective risk management as shown in Table 4.8. Forty seven (48) responded with category 4 of the Likert scale (Yes, Certainly) and 24 with category 5 of Likert (Yes, Very much). In total 87.8 % of the respondents, believe that it is very important to have an effective risk management.

Table 4.8
Risk management effectiveness

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	2	2.4	2.4	2.4
	Not Much	4	4.9	4.9	7.3
	Maybe	4	4.9	4.9	12.2
	Yes, Certainly	48	58.5	58.5	70.7
	Yes, Very much	24	29.3	29.3	100.0
	Total	82	100.0	100.0	

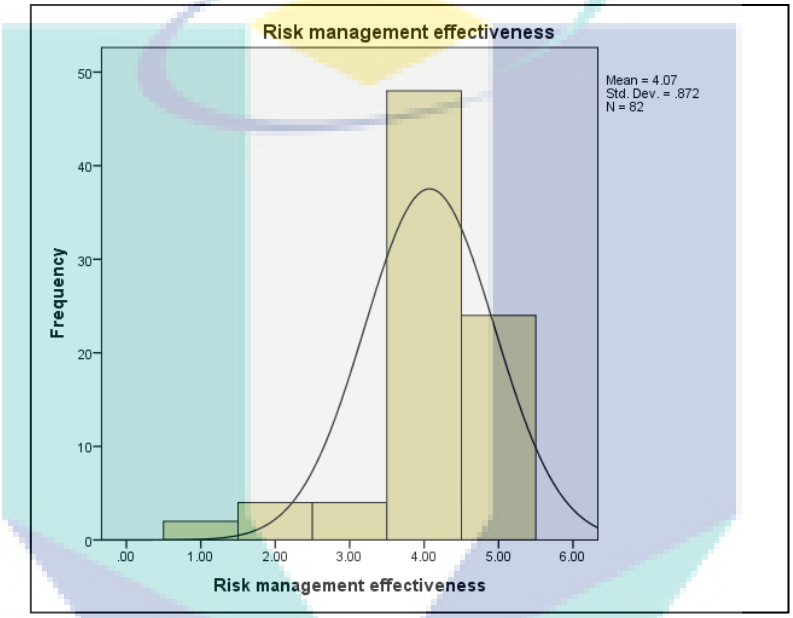


Figure 4.2. Risk management effectiveness

The histogram in Figure 4.2 above shows the depiction of the risk management effectiveness and it is very clear to identify it as the most important element in risk management culture. The respondents believe that an effective risk management is very important in the aftermath of risk that occurs to the e-voting system or the election process. The top three factors are considered importance because of their impact on the respondents.

(2) Importance of Risk assessment; The objective here is to know the importance of risk assessment process for removing or reduce the level of its risk by adding precautions or control measures, as necessary. This is the second most important factor for risk management culture. Table 4.9 shows information on importance of risk assessment.

Table 4.9
Importance of risk assessment

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not Much	9	11.0	11.0	11.0
	Maybe	4	4.9	4.9	15.9
	Yes, Certainly	46	56.1	56.1	72.0
	Yes, Very much	23	28.0	28.0	100.0
	Total	82	100.0	100.0	

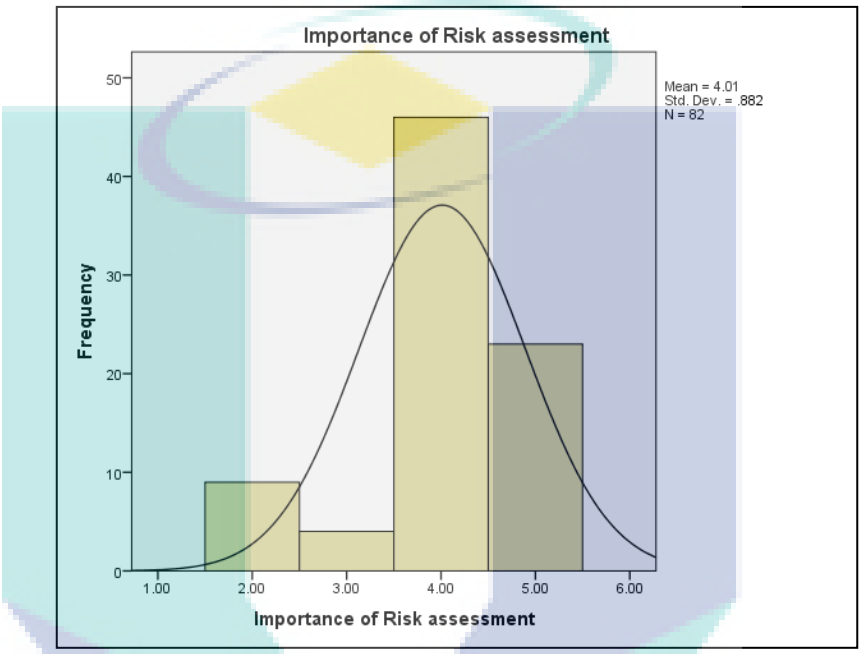


Figure 4.3. Importance of risk assessment

The number of respondents who judged it is certainly important to assess risk were 48 individuals while 23 respondents believe it is very important to assess risk. Overall 84.1 % of respondents believe risk assessment is an important element. The histogram in Figure 4.3 above shows the depiction of the importance of risk management and it is obvious from the histogram it is one of the most important factors.

(3) Interest to learn about risk management is the third highest factor. As shown in table 4.10, the number of employees who believe they are interested to learn about risk and how to manage are 47 individuals. While 15 individuals believe it is very important for them to learn about risk management.

Table 4.10
Interest to learn about risk management

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	2	2.4	2.4	2.4
	Not Much	11	13.4	13.4	15.9
	Maybe	7	8.5	8.5	24.4
	Yes, Certainly	47	57.3	57.3	81.7
	Yes, Very much	15	18.3	18.3	100.0
	Total	82	100.0	100.0	

Overall 75.6% of the employees believe it is important for them to learn risk management. Since there is no well documented risk assessment plan, there is a need for training and seminars regarding risk management.

Figure 4.4. Interest to learn about risk management

The histogram in Figure 4.4 above shows the depiction of rating of Interest to learn about risk management from the respondents. Based on the graphical representation it can be seen as one of the most important elements of risk management culture. The above paragraphs have been discussed with highest three factors related with the risks involving the e-voting system. In this section the opposite of the previous discussion will be carried out. The lowest three factors are important also and the ministry should address.

(4) Risk transfer: As shown in Table 4.11 and figure 4.5; that the existence and knowledge of risk transfer is almost negligible.

Table 4.11
Risk transfer

Response		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	41	50.0	50.0	50.0
	Not Much	24	29.3	29.3	79.3
	Maybe	10	12.2	12.2	91.5
	Yes, Certainly	6	7.3	7.3	98.8
	Yes, Very much	1	1.2	1.2	100.0
	Total	82	100.0	100.0	

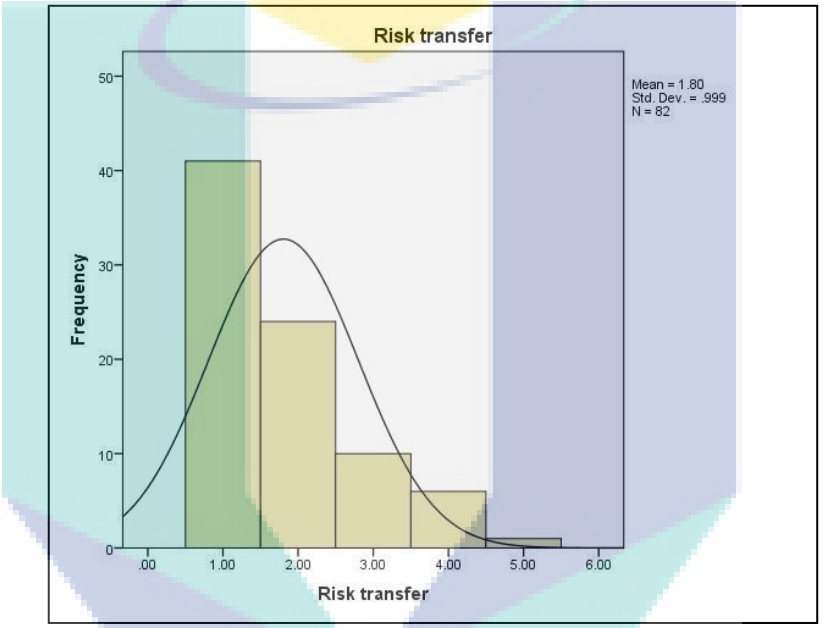


Figure 4.5. Risk Transfer

It can be concluded that there is no risk transfer among the employees and departments of MOI. The number of respondents who claimed that there is no risk transfer is 79.3 % or 65 employees out of the 82 respondents believe there is no risk transfer at all.

(5) Professional training on Risk: Table 4.12 shows that professional training on risk for the employees is very rare or it never happened. Therefore, at the MOI there is so significant training on risk or it does not exist at all. This shows the lack of interactive learning and the latest thinking, standards, theory and best practice in risk management.

Table 4.12
Professional training on Risk

Response		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	16	19.5	19.5	19.5
	Not Much	49	59.8	59.8	79.3
	Maybe	10	12.2	12.2	91.5
	Yes, Certainly	7	8.5	8.5	100.0
	Total	82	100.0	100.0	

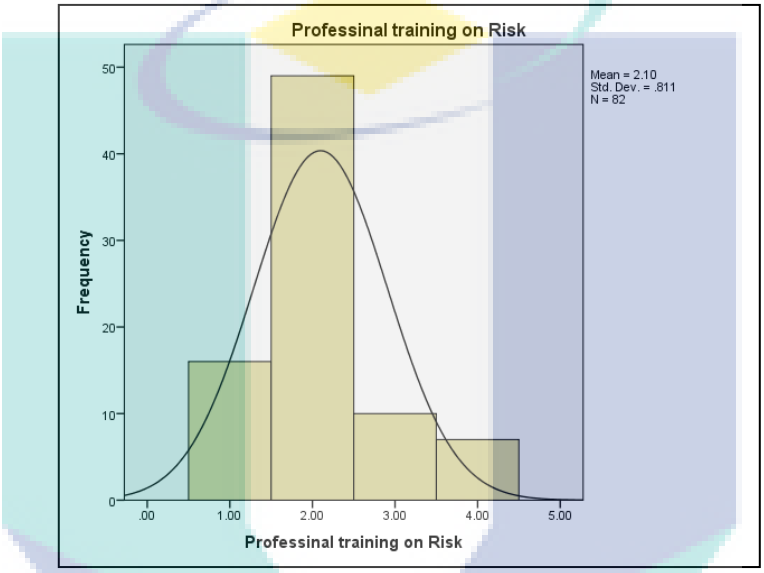


Figure 4.6. Professional Training on Risk

The numbers of respondents who claimed that there is no professional training on risk 79.3 % or 65 employees out of the 82 respondents believe there is not that much training or no training on risk was ever made. Figure 4.6 shows the histogram of Professional training on Risk. It is obvious that training on the risk management is essential for creating the systematic process of understanding; evaluating and addressing these risks to maximize the chances of objectives being achieved and ensuring the MOI staff can sustain a risk free elections process.

(6) Familiar with ISO31000 and ISO31010: Table 4.13 shows the statistics of number of respondents who are familiar with ISO31000 and ISO31010. Sixty one (61) individuals or 74.4 % of the respondents believe there is little about ISO31000 and ISO31010 or they have never learned anything relating with ISO31000 and ISO31010.

Table 4.13
Familiar with ISO31000 and ISO31010

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	25	30.5	30.5	30.5
	Not Much	36	43.9	43.9	74.4
	Maybe	6	7.3	7.3	81.7
	Yes, Certainly	9	11.0	11.0	92.7
	Yes, Very much	6	7.3	7.3	100.0
	Total	82	100.0	100.0	

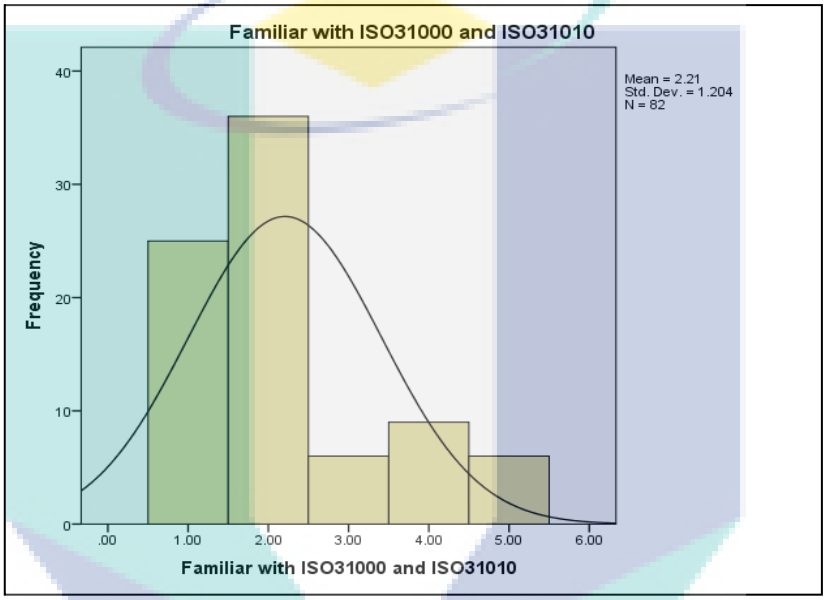


Figure 4.7. Familiar with ISO31000 and ISO31010

Figure 4.7above shows the histogram of Professional training on Risk. If the employees work seamlessly considers risk, then a healthy risk management culture exists. This means responsibility and accountability are at the forefront, and every employee has been trained and understands risks. Risks are identified, monitored, and managed in a consistent and coordinated way.

4.6 ASSESSMENT OF THE EXISTING VOTING SYSTEM

In this section we conduct analysis of the questionnaire data from the Risk Management Assessment of the existing (old) e-voting system. Here objective two (2); which was to assess the risks of the old e-voting system through statistical analysis is

answered. Table 4.14 illustrate the results of the risk assessment questionnaire. The most risky three factors involving in the voting process as shown in table 4.9, the top two elements and the last one were chosen.

Table 4.14
Overall ranking of the factors of risk assessment

Descriptive Statistics

	Risk Factors	N	Min.	Max.	Mean	Std. Deviation
1)	Voter cheating by ink removal	82	3.00	5.00	4.4512	.59114
2)	Voter cheating by using different machines	82	3.00	5.00	4.4268	.58858
3)	Errors due to lack of knowledge	82	1.00	5.00	3.5488	.93164
4)	Hardware failure	82	1.00	5.00	3.3902	1.40331
5)	Hardware failure is worst risk	82	1.00	5.00	2.6709	1.02706
6)	Paper work as an alternative of voting	82	1.00	4.00	2.6585	1.20922
7)	Power failure is worst risk	82	1.00	4.00	2.4024	.90075
8)	Software failure is worst risk	82	1.00	5.00	2.1220	1.32768
9)	Software failure	82	1.00	4.00	1.5926	.68092
10)	Voting Process Faster	82	1.00	3.00	1.1098	.35158

There are some advantages, such advantages include the possibility that citizens can use passport for validation, for those who do not have a valid resident card. It is also possible to eliminate large queue formation in front of voting centers. The other advantages is that the voting software and databases are running locally in a disconnected environment; making it impossible to hack. Nevertheless, the disadvantages are many in the old system. The disadvantages include difficulty to track a person, the voters feel very uncomfortable for marking the electoral inking on their fingers etc, In this section; employees were asked if they ever encounter risk for example: Hardware failure when voting was in process. Software failure when voting was in process, Power (electricity) failure, Cheating by using different machines so he/she can vote twice, Encounter voter cheating by ink removal, Errors from voter due to lack of knowledge and Risk of voting process getting slower.

(1) Voter cheating by ink removal; as shown in Table 4.15 and Figure 4.8 depict the highest risk factor for the old e-voting system is the possibility of voter cheating by in removal. Seventy eight (78) of the respondents; that are 95.1 % of the respondents believe that it is certainly or very much possible that voters can cheat by ink removal.

Table 4.15
Voter cheating by ink removal

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Maybe	4	4.9	4.9	4.9
	Yes, Certainly	37	45.1	45.1	50.0
	Yes, Very much	41	50.0	50.0	100.0
	Total	82	100.0	100.0	

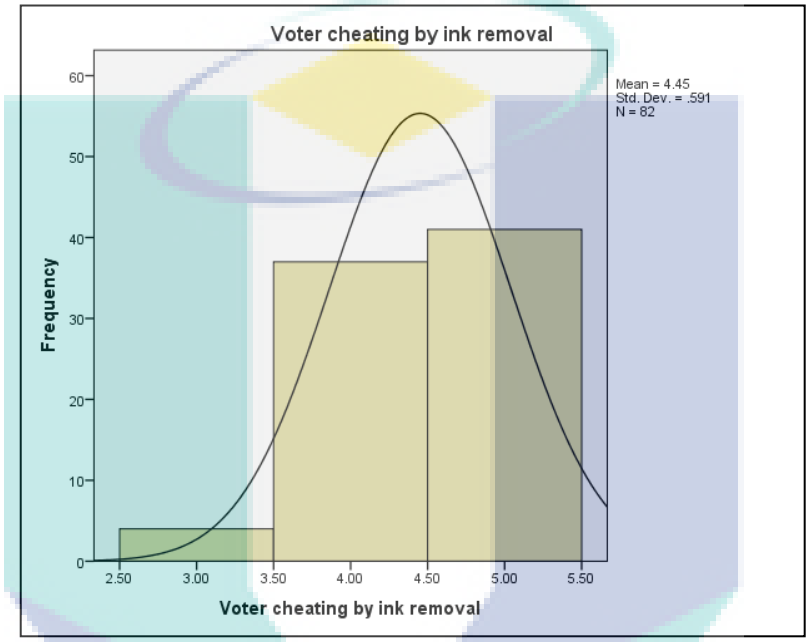


Figure 4.8. Voter cheating by ink removal

It is suspected that in fingerprint security systems for example, indelible ink used for voting may not be foolproof. At brain storming sessions which were held in the MOI, some of the employees pointed out that it is possible if an individual wants to cheat the vote that it might create innovative ways of removing the indelible ink; for example greasing the fingers before the ink was applied. This shows that some individuals might have intention to cheat.

(2) Voter cheating by using different machines; is the second highest risk factor. As Table 4.16 and Figure 4.9 depict seventy eight (77) of the respondents or 94 % of the respondents believe that it is certainly or very much possible that voters can cheat by using different machines.

Table 4.16

Voter cheating by using different machines

	Response	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Maybe	4	4.9	4.9	4.9
	Yes, Certainly	39	47.6	47.6	52.4
	Yes, Very much	39	47.6	47.6	100.0
	Total	82	100.0	100.0	

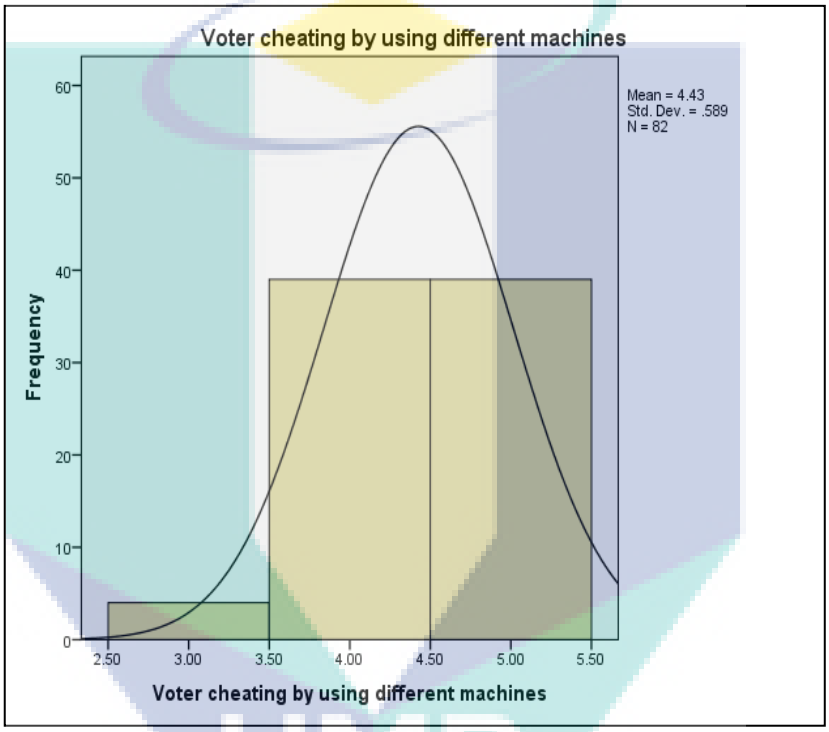


Figure 4.9. Voter cheating by using different machines

It is possible that a voter my try to vote multiple times using different machines. Although the possibility of doing that is very small but still it is possible to breach the system. This dishonest attempt can be prevented. Most of respondents believe that a voter can attempt to cheat by using different machine.

(3) The voting process is not fast. The respondents indicate that the voting process is slow. As Table 4.17 and Figure 4.10 depict the third highest risk factor for the old e-voting system is that the voting process is not fast enough. Majority of the respondents, seventy four (74) of them; which is 90% of the results have shown that the old e-voting was not fast. The respondents indicated that the machines can be slow and

time consuming. This can create negative feelings of the voter. Only one (1) individual or just 1.2 % of the respondents claimed it was may be fast. This can be the reason of technical problems inexpertly handled by polling officials.

Table 4.17
Voting Process Faster

Response		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not at all	74	90.2	90.2	90.2
	Not Much	7	8.5	8.5	98.8
	Maybe	1	1.2	1.2	100.0
	Total	82	100.0	100.0	

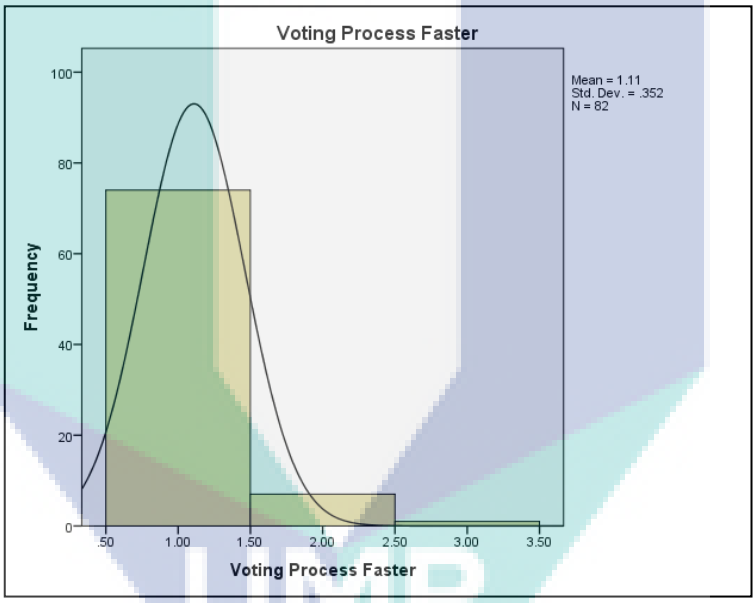


Figure 4.10. Voting Process Faster

Nevertheless, the results of the old e-voting system risk analysis indicate three issues are the most risky factors are: Voter cheating by ink removal, Voter cheating by using different machines and slow voting process based on the mean rankings as shown figure 4.7.

4.7 RESULTS OF AHP ANALYSIS

Here objective three (3) is analyzed for developing AHP model using Microsoft Excel as the software tool. This AHP model will carry-out decisions on the identification

of the most risky areas of e-voting security. Here the considered risk elements are shown in Table 4.18.

Table 4.18
Security risks of e-voting system

	SECURITY (S)	100 %
S1	Operator authentication	11%
S2	Reliability	15%
S3	Isolation	8%
S4	Availability of system	14%
S5	Immunity to attack	17%
S6	Integrity of votes	9%
S7	Traceability	5%
S8	Recoverability	8%
S9	Fault tolerance	9%

These are in fact considered as the most common factor of security risks of e-voting system. These variables have been constructed from the literature as indicated in Cunha et al. (2006). This research focused relevant security, transparency, usability and accessibility and their sub-criterion for an e-voting system used for the Portuguese parliament general elections, and then established an auditing procedure based on AHP

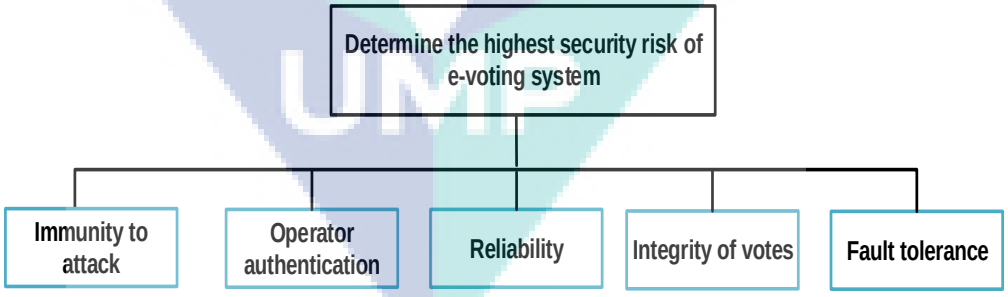


Figure 4.11. Chosen variables of security

Here only five (5) variables have been chosen to use for the AHP analysis as shown in Figure 4.11. These variables are based on the data from questionnaire for AHP by which 10 experts at the MOI were given to judge the highest and lowest security risks of e-voting system. Three steps was used to create the complete AHP model using Ms excel and steps are as follow: step one pair wise comparison, step two for normalization

and step three consistency analyses. The following excel tables show the detailed process of the AHP modeling. Table 4.19 below show the pair-wise comparison of the selected risk factors of the e-voting system. The criteria in the row are being compared to the criteria in the column.

Table 4.19
Pair-wise Comparison

	Reliability	Operator authentication	Immunity to attack	Integrity of votes	Fault tolerance
Reliability	1.00	3.00	3.00	5.00	7.00
Operator authentication	0.33	1.00	0.33	3.00	5.00
Immunity to attack	0.33	3.00	1.00	3.00	3.00
Integrity of votes	0.20	0.33	0.33	1.00	3.00
Fault tolerance	0.14	0.20	0.33	0.33	1.00
SUM	2.01	7.53	5.00	12.33	19.00

Table 4.20 below shows the normalization or the standardized matrix of the selected risk factors of the e-voting system. This step is to normalize the matrix by totaling the numbers in each column.

Table 4.20
Standardized Matrix

	Reliability	Operator authentication	Immunity to attack	Integrity of votes	Fault tolerance
Reliability	0.50	0.40	0.60	0.41	0.37
Operator authentication	0.17	0.13	0.07	0.24	0.26
Immunity to attack	0.17	0.40	0.20	0.24	0.16
Integrity of votes	0.10	0.04	0.07	0.08	0.16
Fault tolerance	0.07	0.03	0.07	0.03	0.05
SUM	1.0	1.0	1.0	1.0	1.0

Each entry in the column is then divided by the column sum to yield its normalized score. The sum of each column is one, then the eigenvector values are found; which are normalized priority weights of each attribute. These weights are the values that are the most consistent with the pair-wise comparison values. Table 4.21 shows the eigenvector

values or priority vector. It is very clear that much importance should be given to Reliability, Immunity to attack and Operator authentication.

Table 4.21
Results of the analysis

Risks	Weight
Reliability	45%
Operator authentication	17%
Immunity to attack	23%
Integrity of votes	9%
Fault tolerance	5%
Total	100%

Table 2.22 illustrates the computation of lambda max (λmax) and Table 4.23 computes the consistency of the AHP method and the standard rule states the following condition: If CR <= .10, consistency is acceptable. To compute consistency ratio (CR): CR = CI / RI. The appropriate Consistency index is called Random Consistency Index (RI).

Table 4.22
Computing λmax.

Risks	SUM	SUM/Weight
Reliability	2.45	5.40
Operator authentication	0.92	5.26
Immunity to attack	1.31	5.62
Integrity of votes	0.46	5.15
Fault tolerance	0.25	5.23
Lambda Max(λmax) ==========>5.33		

The RI is shown in table 4.23 The RI = random index (CI of randomly generated pair-wise comparison matrix). The value of RI is based on *n.* A true Consistency Ratio is calculated by dividing the Consistency Index for the set of judgments by the Index for the corresponding random matrix. According to (Saaty, 2003); It is suggested that if that ratio exceeds 0.1 the set of judgments may be too inconsistent to be reliable. However; in practice, CRs of more than 0.1 sometimes have to be accepted.

Table 4.23
Random Consistency Index

Computing Random Consistency Index										
Number of Variables (n)	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

$$CI = (\lambda max - n) / (n-1) = (5.33-5)/(5-1) = 0.0825.$$

Compute consistency ratio (CR) $= 0.0825/1.12 = 0.068$. Since the consistency ration is 0.068 and it is less than 0.10. Then the AHP model is acceptable.

4.8 NEW E-VOTING SYSTEM DEVELOPMENT

In this section objective four (4) is answered. To resolve the issues of the old e-voting system that it has been mentioned in section 4.4.2 based on that we have developed a new e-voting model which is based on the E-Authentication Activation Application (EAAA) technique in an attempt to resolve all of the risks of the old e-voting system.

4.8.1 E- Authentication Activation Application (EAAA)

The fundamental solution to the old system problems is to implementing the e-Authentication project, which uses the existing National ID Card to authenticate citizens for voting in the national elections. The solution shall allow all citizens to come to election points and get authenticated through their National ID Card before proceeding to the vote. The solution shall be hosted within the current National ID System, taking advantage of the electronic authentication of the cards while enhancing these capabilities with functions specific to the election process, ensuring election rights and introducing vote timestamp storage in the cards.

Figure 4.12 below, illustrates the process of carrying out ID card activation. The above three ways of activating the ID card ensures that the Omani Citizens prepare for the upcoming election which will be based on E-voting system.

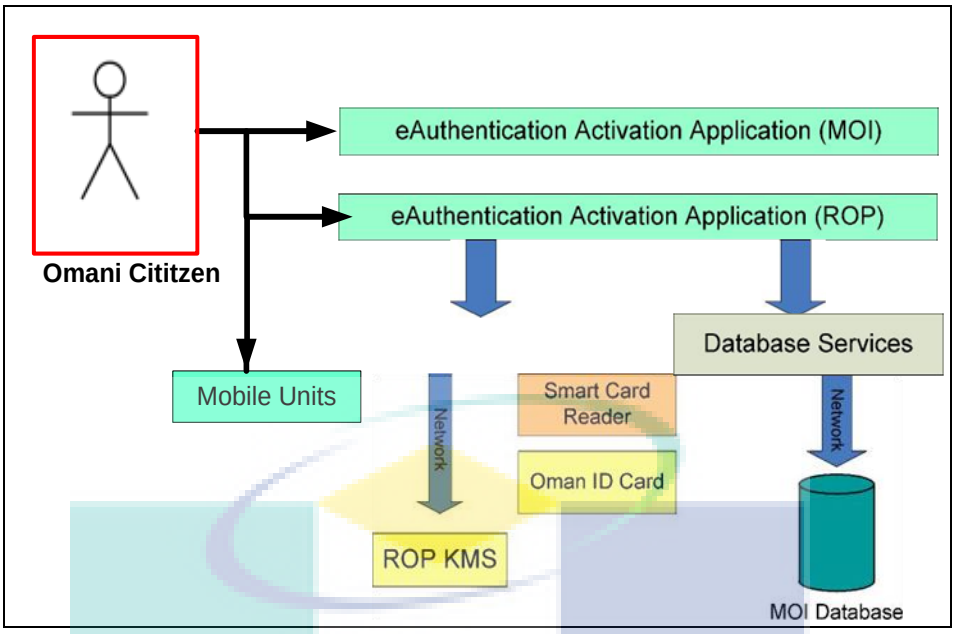


Figure 4.12. E-authentication of citizens

The Omani citizens can visit the Royal Omani Police headquarters to activate their Identity card. They can also visit the MOI and then activate their ID cards. Another way the Omani citizens can active their ID card is through the use of Mobile Units; these units can move from one state to another and from city to city.

The E-Authentication Application is responsible for the validation and authentication of voters updating the Citizen card on the electoral day. Update Database data on the electoral day. The minimum hardware Components required running the E-AA Application is: - Pre-Configured PC, Card Reader Device (Use any of the card readers), Biometric device (For fingerprint Identification), Dongle (For Biometric device security) and Citizen Card (Valid Oman Citizen Card).

To Authenticate Voter the application performs all the validation checks successfully andthe fingerprint Match dialog will be displayed. The voter has to get authenticated with their fingerprints, as shown above in Figure 4.13.

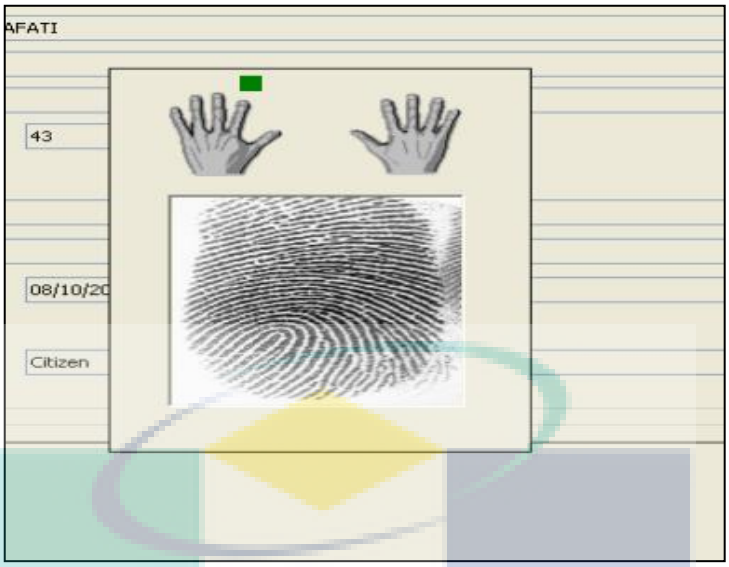


Figure 4.13. A sample of the voter authenticated with fingerprints

There are two user roles in the application; Operators and Supervisors. The Operators let the voter insert the ID card; so that the system can automaticcally read the ID card data. Then the operator will Authenticate the voter including using fingerprint biometrics, and finally give the voters back their ID card and allow them for voting. While the Supervisors (in addition to Operators), ensures that the voting system is setup and organized according to the guidelines. This will help to prevent major human errors in the voting process.

4.9 ASSESSMENT OF THE NEW E-VOTING SYSTEM

In this section we conduct analysis of the questionnaire data from the Risk Management Assessment of the existing new e-voting system as part of objective four (4). The questionnaire was filled by the MIO and election department employee. Table 4.25 illustrates the results of the risk assessment questionnaire.

Table 4.25
Overall ranking of risk assessment factors of the new e-voting

	Risk Factors	N	Min.	Max.	Mean	Std. Deviation
1)	Process faster than before	82	4.00	5.00	4.5488	.50068
2)	Paper work as an alternative of voting	82	3.00	5.00	4.4756	.54942
3)	Errors due to lack of knowledge	82	1.00	5.00	4.2561	.62482
4)	Hardware Failure	82	3.00	5.00	3.9390	.80657
5)	Software Failure	82	2.00	5.00	3.9024	.67786
6)	Hardware Failure is the work risk	82	1.00	4.00	2.7927	.81252
7)	Power Failure is the worst risk	82	1.00	5.00	2.5976	.90075
8)	Software Failure is the work risk	82	1.00	3.00	1.7805	.81687
9)	Voter cheating by using different machines	82	1.00	2.00	1.0244	.15521

Comparing with Table 4.14 illustrates the results of the risk assessment of the old e-voting system, it is very clear that the new e-voting system performs superior to the old one. The risks which were apparent from the old e-voting system are absolutely eliminated in the new e-voting system. The factors caused severe risks on the old e-voting system are not an issue in this new e-voting system. During this step the key risk assessments include system elements, such as hardware, software, systems, data and information, personnel actions, and the mission of the voting system, are reviewed. Based on Table 4.25, the following elements of risk will be analyzed: Voting Process faster than before, Paper work as an alternative of voting, Voter cheating by using different machines and Errors due to lack of knowledge. As indicated in chapter three, the employees are asked if they ever encounter risk for example: Hardware failure when voting was in process. Software failure when voting was in process, Power (electricity) failure, Cheating by using different machines so he/she can vote twice, Encounter voter cheating by ink removal, Errors from voter due to lack of knowledge and Risk of voting process getting slower.

(1) The voting process is much faster than before. The respondents indicate that the voting process is much faster in the new e-voting system. Table 4.26 shows that all the 82 individuals responded positively that the new e-voting system is fast enough. That is 100%, responded system faster than before.

Table 4.26
Process faster than before

	Risk Factors	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes,Certainly	37	45.1	45.1	45.1
	Yes,Very much	45	54.9	54.9	100.0
	Total	82	100.0	100.0	

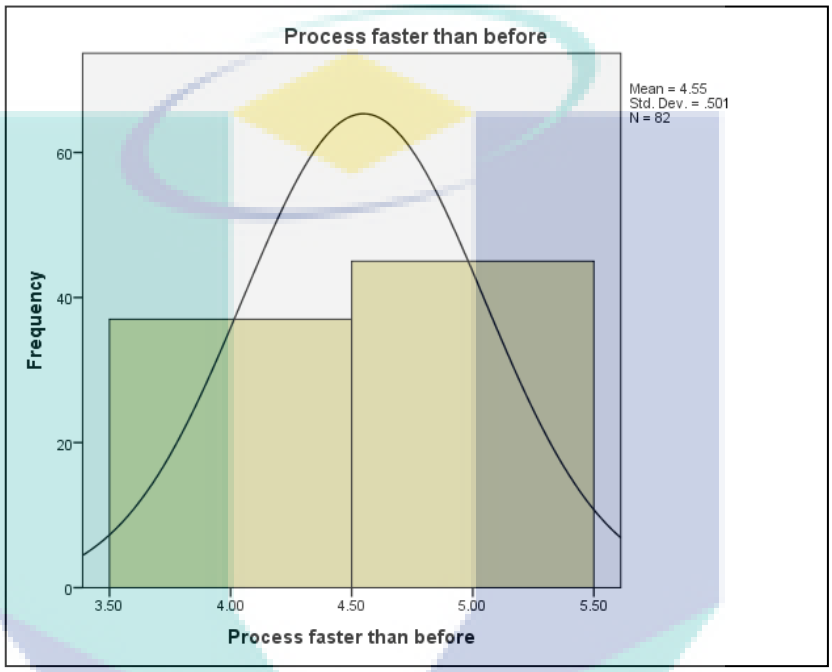


Figure 4.17. Voting process is faster than before

Figure 4.17 shows the graphical representation of the respondent's data. By comparing with the results of the old –voting system from section 4.5 it is very clear that the new e-voting is far more superior. Table 4.17 and Figure 4.10; which depicted the third highest risk factor for the old e-voting system; which was voting process is not fast enough. The issue of slow process is totally eliminated now with new e-voting system.

(2) Paper work as an alternative of voting; the respondents were asked if there is any failure to the e-voting system, will the use of paperwork as an as an alternative of voting be a good option.

Table 4.27
Paper work as an alternative of voting

Risk Factors		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Maybe	2	2.4	2.4	2.4
	Yes, Certainly	39	47.6	47.6	50.0
	Yes, Very much	41	50.0	50.0	100.0
Total		82	100.0	100.0	

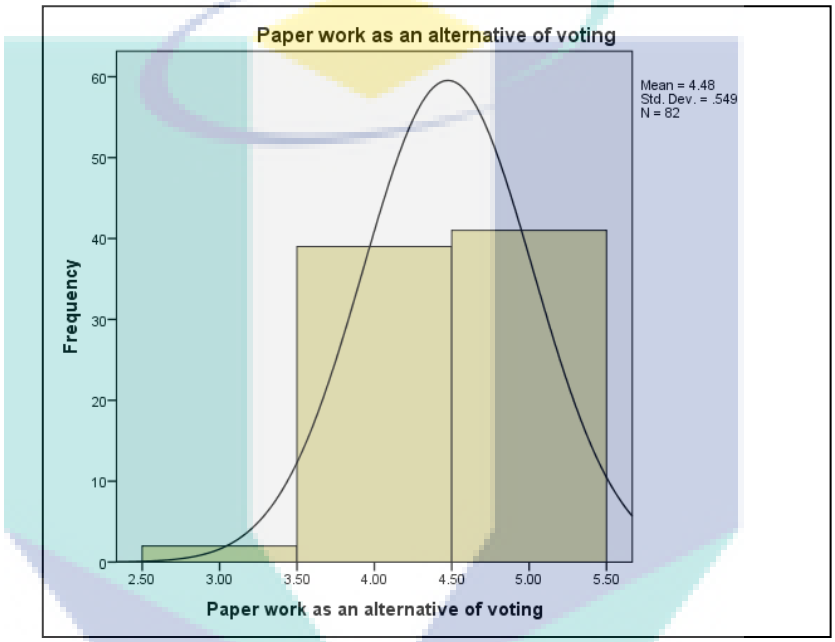


Figure 4.18. Paper work as an alternative of voting.

Based on Table 4.27 and figure 4.18, the number of respondents who agreed that paper work is good alternative is 80 individuals; which correspond to 97.6% of the employees. Only two (2) employees said may be it is better option. Therefore, paperwork will always be used a backup method if unforeseen issues happen to the e-voting system.

(3) Voter cheating by using different machines; this was the second highest risk factor for the old e-voting system. However; it is almost not existent issues with the new e-voting system. By comparing it with Table 4.16 on section 4.5, we can see that table 4.28 and figure 4.19, it depicts eighty (82) of the respondents, which is 100%, claimed that they did not encounter any cheating by using different machines.

Table 4.28
Voter cheating by using different machines

Risk Factors		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all	80	97.6	97.6	97.6
	Not Much	2	2.4	2.4	100.0
	Total	82	100.0	100.0	

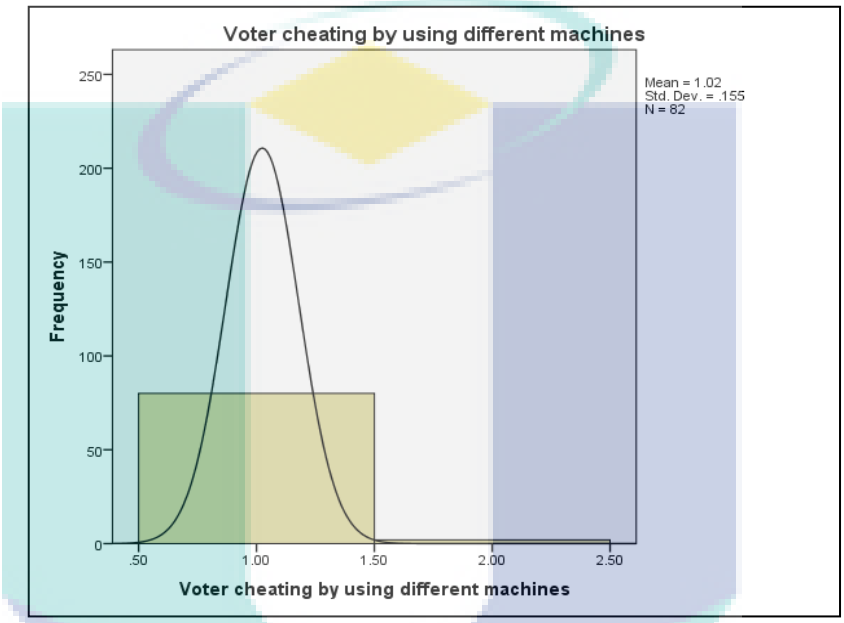


Figure 4.19. Voter cheating by using different machines

The reason being with the card reader devices; which reads the chip of the citizen ID card and the biometric device for finger print identification makes impossible for the citizen to cheat by voting more than once by using different machines.

(4) Errors due to lack of knowledge; this can me the only risky issue for the new e-voting system. Based on Table 4.29 and Figure 4.17 it can be seen that seventy nine (79) or 96. 3 % of the employees believe that errors will arise due to the Omani citizens` lack of knowledge of how to vote correctly with the e-voting.

Table 4.29
Errors due to lack of knowledge

	Risk Factors	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not at all	1	1.2	1.2	1.2
	Maybe	2	2.4	2.4	3.7
	Yes, Certainly	53	64.6	64.6	68.3
	Yes, Very much	26	31.7	31.7	100.0
	Total	82	100.0	100.0	

Therefore, extensive public awareness and training on how to complete e-voting should be given to the Omani citizens.

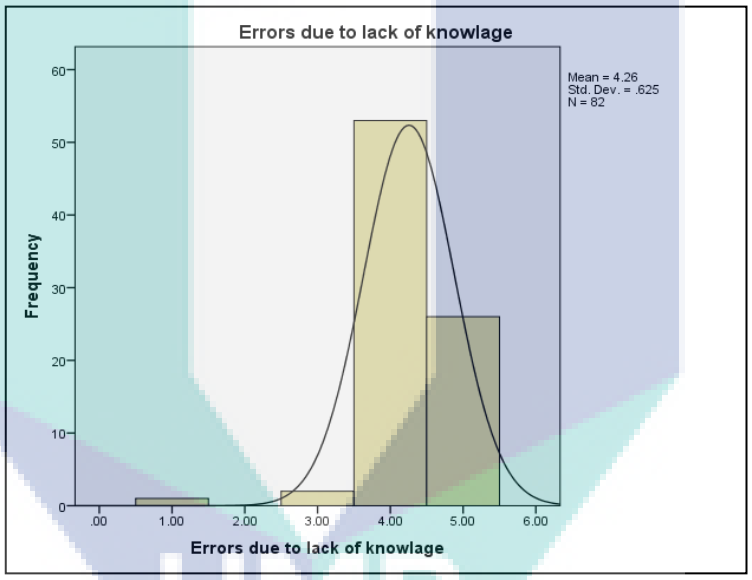


Figure 4.20. Errors due to lack of knowledge

This issue is particularly more severe, old citizens, women, people living remote areas and young people. Therefore, the e-voting as a new technology is very important step forward to development of the nation, but if large proportion of the citizens did not understand how to use this technology, then it is an issue that should be addressed. The table 4.30 below and figure 4.21 show the comparisons between the number of recorded citizens who casted their votes in 2009 and 2013. Population increase implies increase of voting turnout. There has been steady increase of the pollution in each state.

Table 4.30
Comparisons of the number of the voters between 2009 and 2013

No	The region	Number of Voters in 2009	Number of Voters in 2013
1	Muscat	21808	23666
2	Al Batinah	68353	77193
3	Musandam	4514	5388
4	Al Buraimi	4002	4760
5	Al Dhahirah	10350	12014
6	Al Dakhiliyah	18342	24202
7	Al Sharqiyah	41630	52906
8	Al Wusta	4371	5714
9	Dhofar	23341	25794
	Total	196711	231637

The number of registered voters was in 2009 was 196,711 while in this 2013 it was 231, 1637. There is 18% increase of the number of citizens voting from 2009 to 2013. This might indicate the positive impact of new e-voting has on the Omani population.

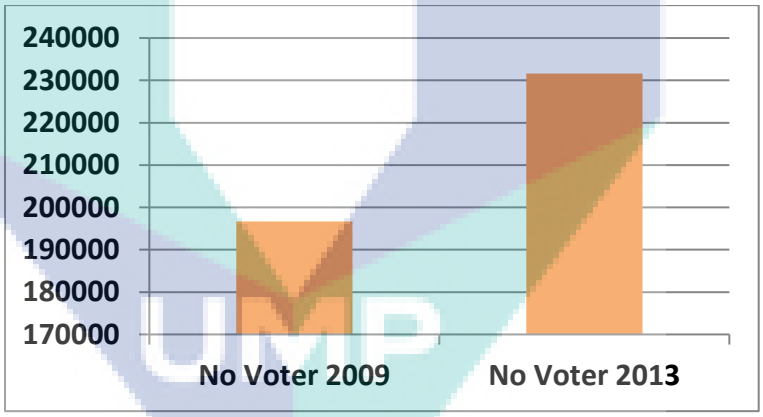


Figure 4.21. Comparison of 2009 and 2013 voters.

It can be easily seen on graphical representations the high turnout of the votes in the year 2013 when compared to 2009. Another factor of increase of the turnout is linked to the new e-voting system for its use of both citizen card and passport for easy of flexibility on registration.

4.9.1 Advantages of the New E-Voting System

The new system completely eliminated the manual entry for authentication of voters. The voting data along with the voted timestamp is stored in the database along with the resident card. The voter is not able to present the card in any other voting centers, because his card is already updated the status as voted in the election. The data updates on the card, is completely eliminated marking of electoral ink on voters finger. The Black list feature ensures that, the voter can use one and only one resident card for voting purpose. Some time individuals can have more than one resident card, but he could use only one active card and all other cards will be black listed from voting. The black list will give more control to the authorities even block unwanted voters from voting procedure. The big queue is almost completely eliminated with EAAA system. The time consumption almost reduced 1/3 of the previous system. The new system is 100 % fool free and no fraud voting is possible in any of the case.

4.10 SUMMARY

In summary, this chapter started with data analysis of the sample distribution through the findings of four demographic elements: Occupational, Education, Age, and Department. Next a survey was conducted on risk assessment of the old e-voting system. After data analysis we have concluded four most risky factors involving in the voting were: Slow voting process, voter cheating by ink removal, voter cheating by using different machines and errors due to lack of knowledge. Next AHP method was used to develop a model for decision analysis on risks which are more important than others so that remedy can be found. The AHP method used is supported by literature as shown in Moreno-Jiménez et al.(2014). Finally one factor is seen as an issue for the new e-voting system, and it is the errors citizens commit due to lack of knowledge. Discussions on the recommendations, contribution and future research will be conducted the following chapter (Chapter 5).

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 INTRODUCTION

This is the final chapter of the project and it presents the conclusions of e-voting risk analysis outcomes of the country of Oman. There are four sections. The chapter begins with the research summary, followed by the contribution of the study, future research and recommendations. This empirical study has explored and investigated a variety of factors that influence potential risks of the e-voting system for parliamentary elections of Oman. These factors determined from questionnaire data on risk management culture and risk assessment of the e-voting system. A new e-voting model was created with the help of the results from an AHP model developed to cater for the need to address the most risky areas of the system. This chapter concludes with a summary of the study.

5.2 RESEARCH SUMMARY

The voting machine's greatest asset is protection against voting fraud or human error. However, critics claim that it intimidates some citizens, that some machines are subject to breakdown, and that fraud is not completely eliminated. Computerized voting machines that use punch cards are also susceptible to voter error, as they lack the means to prevent a person from voting for two candidates for the same office, and can fail to register a vote clearly. Since e-voting systems (e.g DRE) have many advantages of computerized voting systems (Kim & Nevo, 2008), but still there are weaknesses of e-

voting methods, includes lack of an auditing trail, the possibility of a large-scale subversion or treason and the risk of failure of the entire system according to (Grove, 2004; D Jefferson & Rubin, 2004).

Based on the results obtained from investigation and analysis from Chapter 4, it is concluded that the objectives were achieved through the use of data analytics and AHP model:

1. The evaluation the risk management culture on e-voting at the Ministry of Interior has been successfully achieved.
2. The assessment the risks of the old e-voting system through statistical analysis was accomplished.
3. The application AHP modeling technique that can determine the most risky elements in the old e-voting system was completed and results achieved.
4. The valuation of the risks of the new e-voting system was completed.

The notions of risk management, the elections process in Oman, the research scope and the problem statement was clearly explained in chapter 5. Risk Management is becoming a key factor within organizations since it can minimize the probability and impact risks. This research project concerns the risk management of electronic voting (e-voting) which is phenomenon from electronic government (e-government). Using questionnaires, the risks relating with e-voting system will be examined. Some of the risks already found include OS Crash, Hard-Disk Failure, Database Crash, and Power Failure. E-voting systems (e.g DRE) have many advantages of computerized voting systems, such as fast and error-free counting of votes, consistent interface, and centralization of the voting process Kim & Nevo (2008).

However; state of the art research claims weaknesses of e-voting methods, includes lack of an auditing trail, the possibility of a large-scale subversion or treason and the risk of failure of the entire system according to (Grove, 2004; D Jefferson & Rubin, 2004). In this research using questionnaire as the research instrument because the questionnaires have benefits over some other types of surveys in such that they are cheap, do not need as much effort from the questioner as verbal or telephone surveys, and often have standardized answers that make it simple to compile data. This Questionnaires will

be used both voting citizens of Oman and the staff of ministry of interior. From there on outlined nine steps of risk assessment will be carried out.

Next data analysis was performed on the sample distribution through the findings of four demographic elements: Occupational, Education, Age, and Work-field. Data pertaining to the old e-voting system was collected from questionnaire. Subsequently we have conducted survey on risk assessment of the old e-voting system. After data analysis we have concluded four most risky factors involving in the voting were: Slow voting process, voter cheating by ink removal, voter cheating by using different machines and errors due to lack of knowledge. Next AHP method was used to develop a model for decision analysis on risks which are more important than others so that remedy can be found.

5.3 RECOMMENDATIONS

In this section recommendation are suggested to the Ministry of Interior, Oman; which has implemented projects to authenticate voters for the elections like Shura Council, Municipal Election of the country. The findings of the research have indicated that the most important weakness of the new system is Errors due to lack of knowledge; this can me the only risky issue for the new e-voting system. This is the errors citizens commit due to lack of knowledge. Therefore, it is recommended to carry out extensive public awareness and training on how to complete e-voting should be given to the Omani citizens. This issue is particularly more severe, old citizens, women, people living remote areas and young people.

5.3.1 E- Authentication Activation

In 2013 Shura election the ministry implemented a system “Election Day” to authenticate the voters for participating in the elections. Each center having 4 Computer systems with local database in it and the voting starts morning 7 to evening 5. Table 5.1 shows the Steps of Voting Process. The department of IT makes required amount computers (approx 1500) along with Election Day application with local database in it. A week before the dispatching of the prepared system starts.

Table 5.1
Steps of Voting Process

STEP 1:
✓ Once entered the card then specially designed SDK can read the card Or
✓ Enter the passport number through the application GUI.
STEP 2:
✓ Check this card is a valid Oman ID or not. The valid Oman card only will continue for next operations otherwise its halt.
STEP 3:
✓ Read the Name, Citizen ID and Photograph of the voter from the card. Or
✓ Fetch details (Name, Citizen ID and Photograph) against the passport number of the voter.
STEP 4:
✓ The retrieved data will cross check with the database and found the voter is registered or not.
✓ If registered proceeding to next step, otherwise the application will give message that not registered and halt the process
STEP 5:
✓ The Citizen Id number will crosscheck against the black list, if the voter found in the black list or already voted in embassy, he cannot proceed and the process will halt. Otherwise proceed to next step
STEP 6:
✓ Each voting centers have different kind of setups for voting wilayats. The database will crosscheck the voting Wilayat and the voting center wilayts if it same he can proceed for next step.
✓ If the voter needs to vote a different Wilayats, the application will shows concerned message and halt the process.
✓ If all the above checking passed, the voters status change in the database to voted from not voted, and record the voter attendance.
STEP 7:
✓ If all the above checking passed, the voter can proceed for applying voting stain in his fore finger.
STEP 8:
✓ Collects the ballots and poll the vote.
STEP 9:
✓ Put the polled ballot in to the box and leave the voting center.

The voters authenticating happens against the local database and records their votes in database. The Ballets for all the Wilayat will be kept and given as per the voters recorded in their willayats in database. Comparatively less number of voters is embassies and committees. So manual counting with the presence of top officials like Ambassador also happened on the same day itself. The counted votes are keeping in a separate table with high secured authentication. And the Counted ballets are also kept securely for further crosschecking if necessary. The task of preparing computers for Election Day is very important task. Above Table 5.1 shows the Steps of Voting Process and Figure 4.14

depicts the flowchart diagram of Elections and Application Process. The latest committee, embassy voted and new black list are also be included the database with the specially designed supporting software. The technical persons will do this work with the presence of senior responsible officer. Another round of final checking will also take place and just make all the systems ready for Election Day. Each Wilayat have separate counting centers. At the end of election all the ballot paper box get sealed and moved to counting centers along with the sealed system.

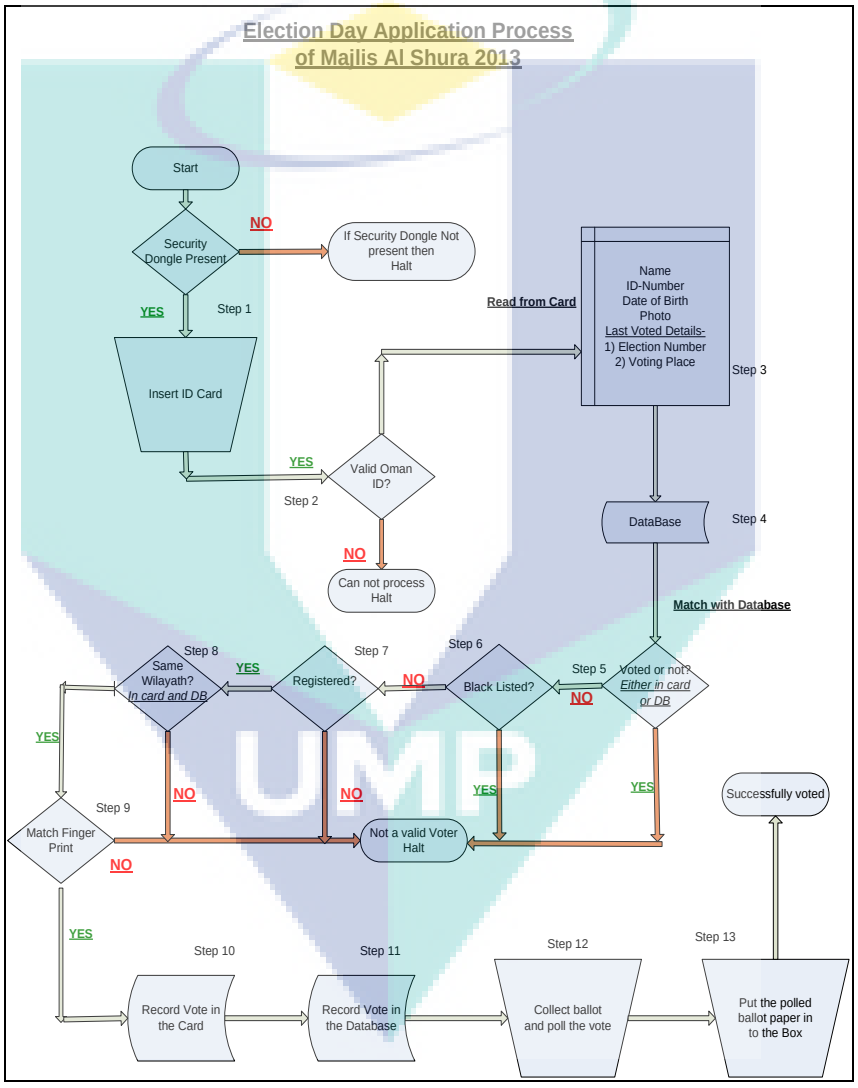


Figure 5.1. Elections and Application Process.

The ballots papers are counted by the machines, which are able to read embossed mark and printed barcode. These fast machines can finish the counting and gives the result immediately. Through the counting machine, the output can be connected to big

television screens and display to the public. So the public can know the progress of the counting. The final result of the each Wilayat will be faxed to the ministry election office, so the authorities are able to announce the final results on the same day. The statistical reports also are announced couple of days after result published.

5.3.2 Security Related Advantage of Technical IT Design

It is possible to use passport of the voters, those who does not have a valid resident card. The time taking for authorizing the voters is short so it is possible to eliminate large queue formation in front of voting centers.

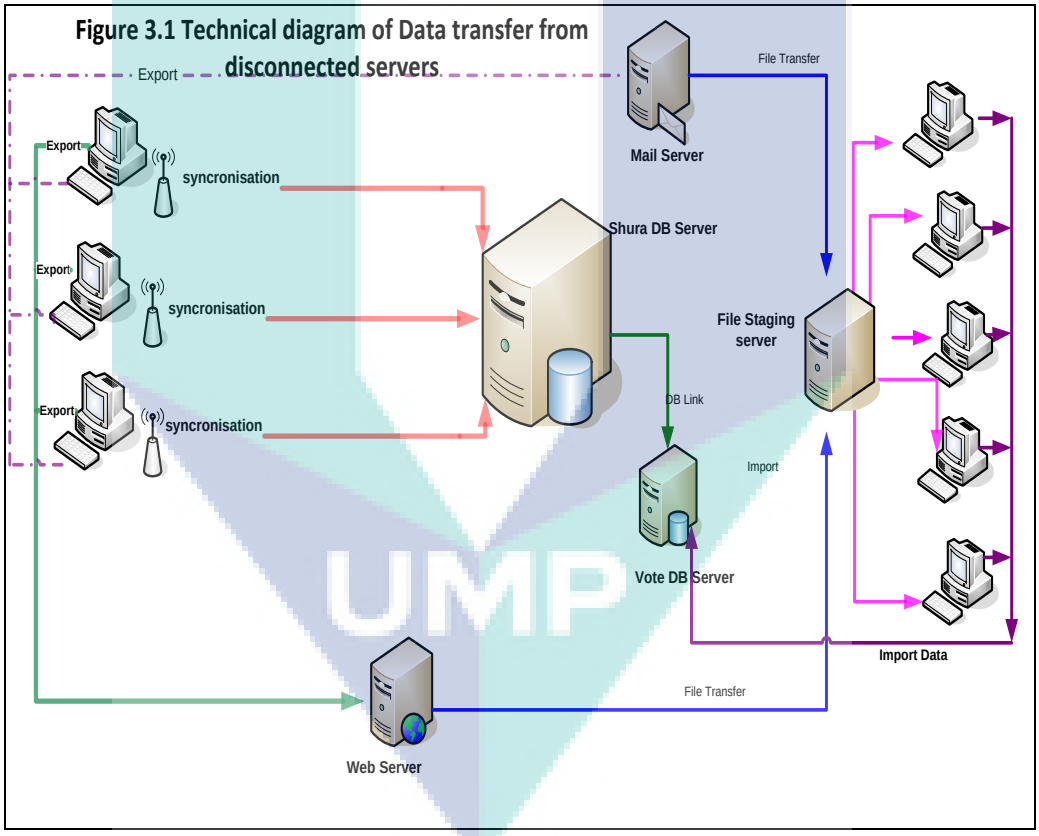


Figure 5.2. Data transfer from disconnected servers

The voting software and databases are running locally in a disconnected environment as shown in Figure 5.2. So any kind of hacking, failure of network or server issues can eliminate and can ensure smooth running of elections. Always keeps one back up for every local server, so it is decrease the down time in the case of failures.

5.3.3 Risk Mitigation Techniques

It is important to mitigate and resolve risks involving for the e-voting system. The following sections document the nine-step risk assessment methodology, in accordance with developed MOI risk management guide for E-voting system, for the country of Oman`s certification and accreditation guidelines.

Step 1: Characterize the Electoral System Voting System

During this step the key risk assessments include system elements, such as hardware, software, system interfaces, data and information, personnel actions, and the mission of the voting system, are reviewed. The application boundaries establish system bounds. System bounds establish the scope of the risk assessment. Clearly defined security boundaries of the system are established and approved by the Government of Oman. Within the established security boundaries, security domains are determined based on system functionality and purpose.

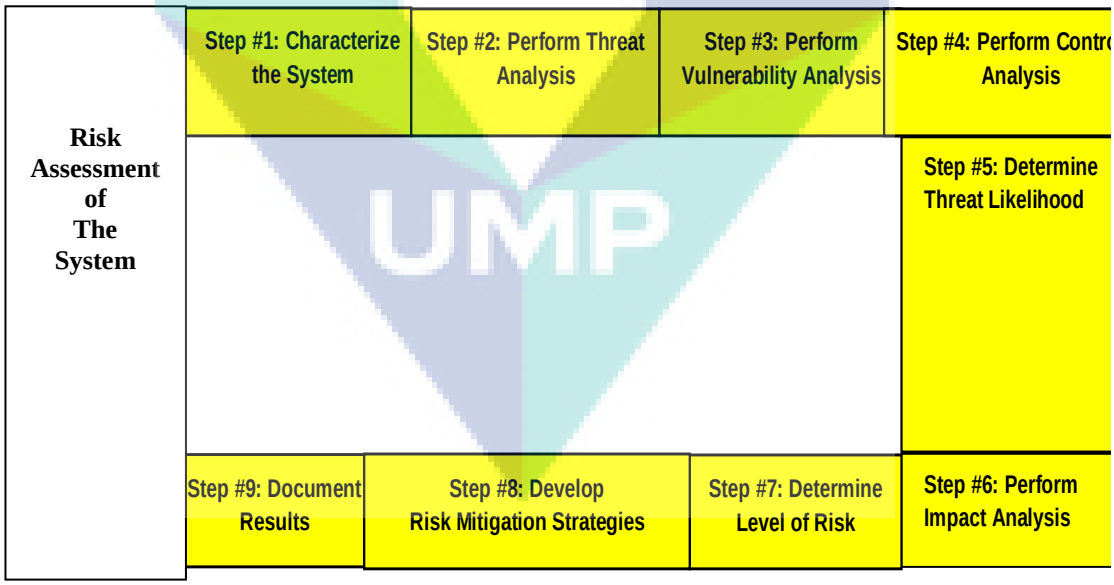


Figure 4.16. Steps of risk mitigation

The system's function is determined and essential elements are identified during this step. Network diagrams and architectural drawings were provided to the risk assessment team. Applicable security policies and requirements, in addition to any

existing policies, procedures, or standards that affect Electoral System security must be determined during this process. Results of previous risk assessments, audits, and certifications, and application related documentation are collected and reviewed.

Step 2: Perform Threat Identification

Step 2 consists of determining the threats posed to the Electoral System voting system. Key elements, such as previous attacks on the Electoral System and data from IT security-related organizations, will be examined for applicability to the electoral system. Identify Threat Sources. Human threats to the Electoral System voting system will be identified and documented.

Step 3: Perform Vulnerability Identification

In Step 3, the vulnerabilities of the system will be examined and identified. Results from prior audits, tests, inspections, and an examination of the current state of the Electoral System voting system are used to determine existing weaknesses as described below. A comprehensive review of the security configurations, standards, procedures, and degree of compliance of both technical and non-technical requirements will determine areas where the Electoral System voting system is vulnerable.

Step 4: Perform Controls Analysis

This step examines the security controls and mechanisms for the Electoral System voting system as currently implemented. Controls analysis involves examining the system security requirements and the security controls employed by the system. The management, operational, and technical controls are examined to determine the degree of compliance with established security requirements and the degree of protection to data confidentiality, integrity, and availability.

Step 5: Determine Threat Likelihood

This step is based on the results of the threat identified in Step 2, and includes the examination of the threat against vulnerability to arrive at a likelihood rating of High, Medium, or Low. Likelihood Specific Vulnerability will be exercised by Particular

Threat. The threat sources identified in Step 2 are examined against the nature of the threat and the security controls in place to counter the threat. In the case of the human threat, motivation and capabilities are taken into account as well.

Step 6: Perform Impact Analysis

Step 6 is used to determine the probable result of a successful exploitation of a vulnerability or weakness by a threat. This risk assessment is used to determine impact on the Electoral System voting system if vulnerabilities are successfully exploited. The process used to evaluate the impact of a successful exploitation of a given vulnerability is very critical.

Step 7: Determine Level of Risk

Step 7 provides a total risk rating for vulnerabilities by combining the results of the Impact Analysis established in step 6 with Likelihood of Threat established in step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place is applied to a risk-level matrix to determine the resultant risk-level

Step 8: Develop Risk Mitigation Strategies

Step 8 seeks to provide solutions to the risks identified and quantified in the previous step. Develop Risk Mitigation Strategies that Are Effective, Practical, Have Reasonable Cost and Ease of Implementation. Countermeasures or risk-mitigation strategies are developed. When several strategies are apparent, they are categorized from most effective, least cost, and easiest implementation.

Step 9: Document Results

The objective of step 9 is to Combine Steps 1 through 8 to produce a Final Risk Assessment Report. The results of steps 1 through 8 are combined into a comprehensive report.

5.4 CONTRIBUTION OF THE STUDY

This research has contributed importance to the country of Oman by solving the fundamental problems of the old e-voting system by implementing the e-Authentication project, which uses the existing National ID Card to authenticate citizens for voting in the national elections. All the risks which were apparent from the old e-voting system are absolutely eliminated in the new e-voting system; which was implemented in 2013. The process faster than before, Paper work as an alternative of voting, Voter cheating by using different machines is eliminated. Voter cheating by ink removal; which was rated as the highest risk factor for the old e-voting system is now eliminated to zero since there is electoral ink used. Another achievement is the factor of that the new e-voting system, and it is the errors citizens commit due to lack of knowledge.

Therefore, extensive public awareness and training on how to complete e-voting should be given to the Omani citizens. This issue is particularly more severe, old citizens, women, people living remote areas and young people. The results of this research which are presented along with statistical comparison provide evidence for the efficacy of the approach.

5.5 LIMITATIONS OF STUDY

As an exploratory study, this research builds on the foundation for future research involving the risks of e-voting system of the general voting public for parliamentary election of Oman. There are several important limitations that are observed in this exploratory stage.

First, the chosen population is limited IT staff working at Ministry of Interior (MOI) and department of electoral management in Oman. In spite of expanding the population of respondents to include employees working in different regions, still the average age of those surveyed were approximately thirty to thirty nine (30-39) years old, which is less than the average age of the overall voting public in this country.

Since the turnout of younger voters is typically low compared to the general population, this limitation due to the chosen sample population needs to be addressed in

future work. Although the data collected from this sample of IT staff working at Ministry of Interior (MOI) and department of electoral management in Oman are considered to be at least somewhat typical of data that would be obtained from an overall general population, the set of demographics of the chosen for the staff is clearly different from that of the general voting population. Since the majority of voters in most elections are no well-educated employees, other factors such as level of education, online experience, and work experience would vary significantly from the employee population used in this study.

In addition to the limited population from a demographic standpoint, the sample size is not as large as originally desired. With respect to the data analysis, several limitations are also observed.

However, as an exploratory study these limitations and results can be useful to develop new hypotheses and to refine the e-voting conceptual model to achieve more generalized results in the future.

5.6 FUTURE RESEARCH AND RECOMMENDATIONS

Based on the results of this investigation, it is recommended further research that will lead to the development of procedures of securing the Internet voting (I-voting). However, for this current time it is not advice to implement I-voting systems because of main issues with the verification, security, usability etc, challenges as the voting system becomes more computationally complex. Case studies on several countries have shown and further testified this issues some countries, such as Estonia ; which is now withdrawing from E-voting because an international team of researchers has acknowledged major risks in the security of Estonia's Internet voting system as shown in Halderman et al. (2014).

The future studies aim to provide support for the proper design and implementation of future Internet voting systems by helping to identify factors and characteristics that may determine the extent to which online voting systems are successfully implemented. In support of this objective, the study introduces an Internet voting conceptual model that builds on recent e-government models and extends these models to consider online voting

at multiple levels of government, including overall, local, state, and federal levels. The Internet voting conceptual model includes a range of factors and related characteristics that can motivate citizens to participate in the use of Internet or online voting systems.

REFERENCES

Aminbakhsh, S., Gunduz, M. and Sonmez R. (2013). Safety risk assessment using analytic hierarchy process (AHP) during planning and budgeting of construction projects. *Journal of Safety Research, 46(8),* 99–105.

Aragonés-Beltrán, P., Chaparro-González, F., Pastor-Ferrando, J.P. and Pla-Rubio, A. (2014). An AHP (Analytic Hierarchy Process)/ANP (Analytic Network Process)-based multi-criteria decision approach for the selection of solar-thermal power plant investment projects. *Energy*, *66(7),* 222–238.

Asadpour, M., and Jalili, R. (2009). Double Voting Problem of Some Anonymous E-Voting Schemes. *J. Inf. Sci. Eng.*, *25*(3), 895–906.

Aumann, Y. and Rabin, M. O. (2002). Everlasting security in the bounded storage model. *IEEE Transactions on Information Theory*, *48*(6), 1668–1680.

Benaloh, J. andTuinstra, D. (1994). Receipt-free secret-ballot elections (extended abstract). *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing - STOC 1994*, pp. 544–553.

Bishop, M. and Wagner, D. (2007). Risks of e-voting. *Communications of the ACM*, *50*(11), 120–128.

Brassard, G., Chaum, D. and Crépeau, C. (1988). Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, *37*(2), 156–189.

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, *15*(13), 130–139.

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology*, 8(4) 177–182.

Chen, C., Chen, Y., Jan, J. and Chen, C. (2014). A Secure Anonymous E-Voting System based on Discrete Logarithm Problem. *Appl. Math*, *8*(5), 2571–2578.

Chien, H., Jan, J. and Tseng, Y. (2003). Cryptanalysis on Mu–Varadharajan's e-voting schemes. *Applied Mathematics and Computation*, *2*(39), 525–530.

Cohen, J. and Fischer, M. (1985). A robust and verifiable cryptographically secure election scheme. *FOCS*. Retrieved from http://cs-www.cs.yale.edu/~fischer/pubs/tr416.pdf

Cunha, J. F., Leitão, M. J., Faria, J. P., Monteiro, M. P. and Carravilla, M. A. (2006). Auditing e-Voting Pilot Processes and Systems at the Elections for the European Parliament and for the Portuguese Parliament. In *Seconfd Internationl Conference on Electronic Voting* (pp. 145–155).

Devi, G., Anusha, K. and Rajyalakshmi, G. (2014). An Enhanced e-Voting System in Cloud Using Fingerprint Authentication. *Advanced in Computer Science and Its Applications, Springer B*, 1219–1224.

Esteve, J. (2008). The Certification of E-Voting Mechanisms: Fighting against Opacity. 7th *Proceedings of the Electronic Voting 2008*, pp.102-112.

Estoniae-votingorganization. (2104). Researchers Identify Security Risks in Estonia's Online Voting System. Retrieved August 19, 2014, from http://www.eecs.umich.edu/eecs/about/articles/2014/Estonia_evoting_risks.html

Fellows, R.F. and Liu, A.M.M.(2015). *Research Methods for Construction*, John Wiley & Sons

Gjøsteen, K. (2010). Analysis of an internet voting protocol.

Goldreich, O., Micali, S. and Wigderson, A. (1987). How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design.

Goldsmith, B. (2011). *Electronic Voting and Counting Technologies: A Guide to Conducting Feasibility Studies*. Washington DC: International Foundation for Electoral Systems (IFES). Retrieved from http://www.ifes.org/~/media/Files/Publications/Books/2011/Electronic_Voting_and_Counting_Tech_Goldsmith.pdf

Grove, J. (2004). ACM statement on voting systems. *Communications of the ACM, 47*(10), 69–70.

Haenni, R. and Koenig, R. E. (2013). A generic approach to prevent board flooding attacks in coercion-resistant electronic voting schemes. *Computers & Security*, *33*, 59–69.

Halderman, J. A., Hursti, H., Kitkat, J., MacAlpine, M., Finkenauer, T. and Springall, D. (2014). *Analysis of the Estonian Internet Voting System.*

Hirt, M. and Sako, K. (2000). Efficient receipt-free voting based on homomorphic encryption. *Advances in Cryptology—EUROCRYPT 2000*.

Hwang, S. Y., Wen, H. A. and Hwang, T. (2005). On the security enhancement for anonymous secure e-voting over computer network. *Computer Standards and Interfaces*, *27*(2), 163–168.

Ibrahim, S., Kamat, M., Salleh, M. and Aziz, S. R. A. (2003). Secure E-voting with blind signature. *Proceedings of 4th National Conference of Telecommunication Technology, 2003. NCTT 2003*, pp. 193–197.

Jardí-Cedó, R. and Pujol-Ahulló, J. (2012). Study on poll-site voting and verification systems. *Computers & Security 31*(8), 989–1010.

Jefferson, D. and Rubin, A. (2004). Analyzing internet voting security. *Communications of theACM, 47*(10), 59.

Jefferson, D., Rubin, A. D., Simons, B. and Wagner, D. (2004). Analyzing internet voting security. *Communications of the ACM*.

Joaquim, R., Ferreira, P. and Ribeiro, C. (2013). EVIV: An end-to-end verifiable Internet voting system. *Computers & Security*.

Juels, A., Catalano, D. and Jakobsson, M. (2005). Coercion-resistant electronic elections. *Towards Trustworthy Elections*, 37–63.

Kim, H. M. and Nevo, S. (2008). Development and application of a framework for evaluating multi-mode voting risks. *Internet Research*, *18*(1), 121–135.

King, M. (2004). Implementing voting systems: the Georgia method. *Communications of the ACM*.

Knowledge-Network, A. E. (2014). Countries with e-voting projects. Retrieved August 19, 2014, from http://aceproject.org/ace-en/focus/e-voting/countries

Kohno, T., Stubblefield, a., Rubin, a. D. and Wallach, D. S. (2004). Analysis of an electronic voting system. Proceedings of *IEEE Symposium on Security and Privacy,2004*, 27–40.

Lee, B., Boyd, C., Dawson, E. and Kim, K. (2004). Providing receipt-freeness in mixnet-based voting protocols. *Information Security and cryptography*, *15*(2), 115–125.

Lin, I. C., Hwang, M. S. and Chang, C. C. (2003). Security enhancement for anonymous secure e-voting over a network. *Computer Standards and Interfaces*, *25*(2), 131–139.

Madise, Ü. and Martens, T. (2006). E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. *Electronic Voting*, *86*(2), 120–120.

Madise, Ü. and Vinkel, P. (2014). Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections. Proceedings of *Relugalating E-technologies in European Union* 2014, pp. 53–72.

Mateu, V., Sebé, F. and Valls, M. (2014). Constructing credential-based E-voting systems from offline E-coin protocols. *Journal of Network and Computer Applications*, *42(10)*, 39–44.

Mohen, J. and Glidden, J. (2001). The case for internet voting. *Communications of the ACM*, *44*(1), 72.

Moreno-Jiménez, J. M., Pérez-Espés, C. and Velázquez, M. (2014). e-Cognocracy and the design of public policies. *Government Information Quarterly*, *31*(1), 185–194.

Mu, Y. andVaradharajan, V. (1998). Anonymous secure e-voting over a network. *In Computer Security Applications Conference*, (14), 293–299.

Namara, D. Mac, Gibson, J. and Oakley, K. (2014). Just Like Paper-a baseline for classifying e-voting usability. *International Conference on E-Democracy and Open Government*, 1–12.

Okamoto, T. (1998). Receipt-free electronic voting schemes for large scale elections. *Security Protocols*.

Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. *Advances in cryptology—EUROCRYPT'99*.

Pedersen, T. (1992). Non-interactive and information-theoretic secure verifiable secret sharing. *Advances in Cryptology—CRYPTO'91*.

Peng, K. (2009). A hybrid e-voting scheme. *Information Security Practice and Experience*.

Philip, A. A., Simon, S. A. and A, A. O. (2011). A Receipt-free Multi-Authority E-Voting System. *International Journal of Computer Applications*, *30*(6), 15–23.

Phillips, D. and Spakovsky, H. Von. (2001). Gauging the risks of internet elections. *Communications of the ACM*.

Qadah, G. and Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation. *Computer Standards & Interfaces*.

Radwin, M. (1995). An untraceable, universally verifiable voting scheme. *Seminar in Cryptology*, *2(1)*, 121–130.

Rodríguez-Henríquez, F., Ortiz-Arroyo, D. and García-Zamora, C. (2007). Yet another improvement over the Mu-Varadharajan e-voting protocol. *Computer Standards and Interfaces*, 29(4), 471-480.

Sako, kazue and Joe, K. (1995). Receipt-free mix-type voting scheme : a practical solution to the implementation of a voting booth.. *Advances in Cryptology*, *92(1)*, 393–403.

Sako, K. (2011). Electronic Voting Schemes. *Encyclopedia of Cryptography and Security*, *18(3)*, 391–393.

Sampigethaya, K. and Poovendran, R. (2006). A framework and taxonomy for comparison of electronic voting schemes. *Computers & Security*, *25*(2), 137–153.

Samvedi, A., Jain, V. and Chan, F. T. S. (2013). Quantifying risks in a supply chain through integration of fuzzy AHP and fuzzy TOPSIS. *International Journal of Production Research*, *51*(8), 2433–2442.

Santos, J. R. A. (1999). Cronbach's Alpha: A Tool for Assessing the Reliability of Scales. *Journal of Extension*, *37*(2), 1–5.

Schaupp, L. C. and Carter, L. (2005). E-voting: from apathy to adoption. *Journal of Enterprise Information Management*, *18*(5), 586–601.

Shamos, M. (2004). Paper v. electronic voting records-an assessment. *Proceedings of the 14th ACM Conference on Computers, Freedom and Privacy. 2004,* ,pp. 126–125.

Stenbro, M. (2010). *A Survey of Modern Electronic Voting Technologies*. Norwegian University of Science and Technology. Retrieved from http://www.diva-portal.org/smash/get/diva2:353047/FULLTEXT01.pdf

Stewart, C. (2011). Voting Technologies. *Annual Review of Political Science*., 14(1), 353-378.

Subramanian, N. and Ramanathan, R. (2012). A review of applications of Analytic Hierarchy Process in operations management. *International Journal of Production Economics*, *138*(2), 215–241.

Williams, R., Bertsch, B., Dale, B., Wiele, T. Van Der, Iwaarden, J. Van, Smith, M. and Visser, R. (2006). Quality and risk management: what are the key issues? *The TQM Magazine*, *18*(1), 67–86.

Yang, C., Lin, C. and Yang, H. (2004). Improved anonymous secure e-voting over a network. *Information and Security*, *15*(2), 181–198.

Yaser Baseri, M. P. J. M. (2011). Double Voter Perceptible Blind Signature Based Electronic Voting Protocol. In *IACR Cryptology 25 (3)*, 895–906.

Zou, X., Li, H. and Su, Y. (2014). Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties. In *INFOCOM, 2014 Proceedings IEEE* , pp. 136–144.

APPENDIX A

Questionnaire

Electoral Risk Assessment Questionnaire for IT department, Ministry of Interior

Position			
Work field			
Age			
Academic Qualification	High school: ____Diploma: _____ Bachelor Degree: _____Other: _____		
Phone		Fax	
E-mail			

Risk management culture

Instructions: You are provided with following options to state your answers for each question below. Please tick only one option for your answer.

Please select one option	Not at all	Not much	Maybe	Yes, certainly	Yes, very much
1. Have you heard about risk management?	○	○	○	○	○
2. Do you believe that a risk assessment regarding election is useful for the IT department of Ministry of Interior (MOI)?	○	○	○	○	○
3. Is there capacity to perform a risk assessment in the IT department?	○	○	○	○	○
4. Are there a recognized training methods to facilitate the improvement of general Knowledge on risk?	○	○	○	○	○
5. Are you looking for a training course in the field of risk management?	○	○	○	○	○
6. Are you familiar with ISO 31000 and ISO 31010 standards on risk management?	○	○	○	○	○
7. Is it understood in your department that risk is an integrant part of your business?	○	○	○	○	○
8. Do the employees have a common perception on what risk means for the department?	○	○	○	○	○
9. Does the management encourage the reporting of events in order to identify the risks?	○	○	○	○	○
10. Is there effective way to communicate the risk to the employees or stakeholders (internal and external)?	○	○	○	○	○

11. Is it understood that the risk management effectiveness critically depends on data collection, analysis and dissemination of relevant data?	○	○	○	○	○
Please select one option	Not at all	Not much	Maybe	Yes, certainly	Yes, very much
12. Organizational support. Is there a clearly defined organizational structure in order to sustain the risk management process?	○	○	○	○	○
13. Risk assessment. Is there any system and/or operational procedures that manage the processes of risk identification, measurement, ranking, treatment, monitoring and recording the risks which can affect the achievement of your organization's objectives?	○	○	○	○	○
14. Professional training. Is there any training method used to facilitate the knowledge improvement on risk?	○	○	○	○	○
15. Information. Is there enough data on events history, thus the organization could learn from its own mistakes?	○	○	○	○	○
16. Inspections. Is there an implemented inspection plans to reduce the inherent risks, which are periodically revised?	○	○	○	○	○
17. Warning systems. Do you have monitoring systems in the potential high risk areas that identify the changing of risk level? Can these systems be identified suitable manner?	○	○	○	○	○
18. Risk transfer. How important is the use instruments for risk transfer or sharing with other organizations (e.g. insurance companies)?	○	○	○	○	○
19. Risk review. How effective is the risk review process, after implementation of the mitigation measures / controls for identified risk?	○	○	○	○	○

Risk analysis of the old e-voting system

Instructions: You are provided with following options to state your answers for each question below. Please tick only one option for your answer.

Please select one option	Not at all	Not much	Maybe	Yes, certainly	Yes, very much
1. Did you ever encounter hardware failure when voting was in process?	○	○	○	○	○
2. Did you ever encounter software failure when voting was in process?	○	○	○	○	○
3. Is software failure posing the worst risk?	○	○	○	○	○
4. Is Hardware failure posing the worst risk?	○	○	○	○	○
5. Is Power failure posing the worst risk?	○	○	○	○	○
6. Paper work as an alternative of voting when the equipment fail is a good choice?	○	○	○	○	○
7. Did you encounter voter cheating by ink removal?	○	○	○	○	○
8. Did you encounter voter cheating by using different machines so he/she can vote twice?	○	○	○	○	○
9. Are there errors from voter due to lack of knowledge?	○	○	○	○	○
10. Is voting process faster than before?	○	○	○	○	○

Risk analysis of the new e-voting system

Instructions: You are provided with following options to state your answers for each question below. Please tick only one option for your answer.

Please select one option	Not at all	Not much	Maybe	Yes, certainly	Yes, very much
1. Did you ever encounter hardware failure when voting was in process?	○	○	○	○	○
2. Did you ever encounter software failure when voting was in process?	○	○	○	○	○
3. Is software failure posing the worst risk?	○	○	○	○	○
4. Is Hardware failure posing the worst risk?	○	○	○	○	○
5. Is Power failure posing the worst risk?	○	○	○	○	○
6. Paper work as an alternative of voting when he equipment fail is good choice?	○	○	○	○	○
7. Did you encounter voter cheating by using different machines so he/she can vote twice?	○	○	○	○	○
8. Are there errors from voter due to lack of knowledge?	○	○	○	○	○
9. Is voting process faster than before?	○	○	○	○	○

Electoral Risk Assessment Questionnaire for Ministry of Interior to evaluate weights of AHP

Position			
Work field			
Age			
Academic Qualification	High school: ____Diploma: _____ Bachelor Degree: _____Other: _____		
Phone		Fax	
E-mail			

Instructions: You are provided with following is the security criterion and it has nine (9) sub criteria.

Criterion One: SECURITY (S)		
The Sub- Criteria		
S1: Operator authentication	YES	NO
1. Do you authenticate the operator?	○	○
2. Is authentication of the operator important?	○	○
3. Is the security breached without Operator authentication?	○	○
4. Is Operator authentication most important element in security?	○	○
S2: Reliability	YES	NO
1. Do you assess reliability?	○	○
2. Is reliability very important?	○	○
3. Is reliability the most important element of security?	○	○
4. Is reliability the least important element of security?	○	○

S3: Availability of system	YES	NO
1. Do you think the Availability of system is achieved?	○	○
2. Is Availability of system important?	○	○
3. Is Availability of system the most important element of security?	○	○
4. Is Availability of system the least important element of security?	○	○
S4: Immunity to attack	YES	NO
1. Do you assess the Immunity to attack of the system?	○	○
2. Is Immunity to attack important?	○	○
3. Is Immunity to attack the most important element of security?	○	○
4. Is Immunity to attack the least important element of security?	○	○
S5: Integrity of votes	YES	NO
1. Do you think the integrity of votes is achieved?	○	○
2. Is integrity of votes important?	○	○
3. Is integrity of votes the most important element of security?	○	○
4. Is integrity of votes the least important element of security?	○	○
S6: Traceability	YES	NO
1. Do you assess the traceability of the system?	○	○
2. Is traceability important?	○	○
3. Is traceability the most important element of security?	○	○
4. Is traceability the least important element of security?	○	○

S7: Recoverability	YES	NO
1. Do you think the recoverability is achieved?	○	○
2. Is recoverability important?	○	○
3. Is recoverability the most important element of security?	○	○
4. Is recoverability the least important element of security?	○	○
S8: Fault tolerance	**YES**	**NO**
1. Do you believe fault tolerance is achieved in the system?	○	○
2. Is fault tolerance important?	○	○
3. Is fault tolerance the most important element of security?	○	○
4. Is fault tolerance the least important element of security?	○	○
S9: Isolation	**YES**	**NO**
1. Can the system be isolated?	○	○
2. Is isolation important?	○	○
3. Is isolation the most important element of security?	○	○
4. Is isolation the least important element of security?	○	○

LIST OF PUBLICATIONS

Alamry, F. & Jack kie, C., 2015a. Assessment of E-Voting Risks Using AHP Method for the Omani Government. *Information Security and Computer Fraud*, 23(2), pp.50–64.

Alamry, F. & Jack kie, C., 2015b. Publication - E-Voting Risk and Risk Management Evaluation using Analytical Hierarchy Process: The Case of Oman. *International Journal of Electronics Communication and Computer Engineering*, 6(4), pp.453–459.

Elrasheed Ismail Sultan, Noraziah A, Faisal Alamri, Nawsher Khan and Tutut Herawan. Article: Optimized Load Balancing based Task Scheduling in Cloud Environment. *IJCA Proceedings on Majan College International Conference* MIC(1):35-38, December 2014.

Elrasheed Ismail Sultan, Faisal Alamri, Kunna Mohamed, Noraziah. A, Ahmed N Abdalla and Gamal Awad. Article: Security based Risk Management based on Multi-Objectives Model using QPSO. *IJCA Proceedings on Majan College International Conference* MIC(1):39-42, December 2014.