# A MODEL FOR AN INFORMATION SECURITY RISK MANAGEMENT (ISRM) FRAMEWORK FOR SAUDI ARABIAN ORGANISATIONS

Naser Alshareef
*School of Information Systems – Curtin University, Perth, Western Australia*

**ABSTRACT**

Countries in the Gulf represent thriving, globally important commercial centres. They have embraced technology and modern management methods, often originating in the western countries. In adapting to quite different cultures these do not always operate as successfully. The adoption and practices of the Information Security Risk Management (ISRM) frameworks are an example. Although ISRM has become a standard in information security for much of the world, its uptake in the Gulf countries has been poor. This study tests the possibility that this may be due to cultural "biases" built into the operation and structure of the framework. Using a Design Science approach it aims to develop a modified ISRM framework that incorporates a cultural dimension. This will lead to an increased acceptance of ISRM in Gulf countries, and also to allowing it to be used in other non-western cultures. Centring on Saudi Arabia as a typical example of a Gulf culture, a qualitative approach will be adopted. Data will be collected through structured interviews with information security experts in Saudi Arabian organisations, system integrators and vendors. These will focus on cultural dimensions of parts of the ISRM framework and business responses that result. The modified framework developed through this method will be confirmed using focus groups.

**KEYWORDS**

Information Security Management, Cyber Security, Risk Management

## 1. INTRODUCTION

Managing information security risk is becoming more challenging. Countries around the world allocate a huge budget for their IT infrastructure and its security; however, without a proper security risk management they will be under high risk of cyber-attacks and data breaches regardless of how big the allocated budget is. There are many well established international approaches and methodologies adopted by organisations to help them to make appropriate decisions that mitigate their information security risk. The very widely adopted Information Security Risk Management (ISRM) framework represents a common approach. ISRM has much in common with other security approaches. However, it doesn't consider regional and cultural factors and assumes that all organisations operating large systems requiring sophisticated formation security measures work the same way.

In Gulf countries for example, identifying an organisation's assets as well as team members' lack of experience, while they are accepted as major factors of information security risk management, are culturally more sensitive in this country, and consequently much more difficult to decipher (AbuSaad et al., 2011). This and other difficulties have impacted the uptake of ISRM in businesses in this region, notwithstanding that such businesses are very enthusiastic about adopting modern practices, boast modern of infrastructure and technology, have well developed management expertise, and no shortage of capital to implement their initiatives.

Despite this there is a gap in scholarly and professional research into information security risk management in these countries, and in others in the Middle East with similar cultures. This applies too to Saudi Arabia, which is the focus of this proposed study. This research will develop the existing ISRM frameworks to introduce culture dimensions, in particular those that applying to Saudi Arabia and other Gulf Countries, with the aim of improving its uptake and success in those countries. An appreciation of culture in the ISRM framework will also improve its use for many other non-Western organisations and can possibly lead to changes even amongst core users.

## 2. BACKGROUND

Managing organisations' information security is very crucial and failure to do so may result in disclosure, disruption, modification, or destruction of critical information. This could lead to negative impacts on an organisation's finance, reputation and/or image (McCumber, 2004). The total cost to the global economy from cyberattack data breach is more than $400 billion a year.

With more than 29,000 breached records in 2014, Saudi Arabia and United Arab Emirates companies have a much higher average number of breached records compared to the global average of 23,078; more than 26.5% higher than the global average (Ponemon Institute, 2015). Unlike many other developed countries (Saudi Arabia is considered a developed country, though not a Western one), it has adopted e-services including e-government and e-commerce.

It is naturally becoming much more exposed to cyber-attack. In addition, the Saudi Arabia political conflicts with its neighbour countries including Israel and Iran have increased cyber espionage in the region, and Saudi Arabia is sensitive to this threat. In June 19, 2015 more than 500,000 cables and emails from the Saudi Foreign Ministry, including many "Top Secret" reports from the Saudi's General Intelligence Services have been breached after an attack by the so-called the "Yemeni Cyber Army" (Blake, 2015).

It is therefore clear that Saudi Arabia appears to be at more risk of security breaches, and have a higher impact per breach than the global average. Because of its and its neighbours' importance in global trade, commodities, finance and logistics, risks to these countries tangibly increase the overall global risk level.

### 2.1 Risk Management

Risk is defined as "the effect of uncertainty on objectives" that can be described as "the combination of the likelihood of an event and its consequence" (ISO/TR31004, 2013). It measures the potential condition or event an entity could be threatened by, including the negative impacts that would come along if the event occurs and the occurrence probability or likelihood of these occurring. Risk management is the process of risk identification, assessment, and reduction to an acceptable level (Stoneburner, 2002).

### 2.2 Information Security Risk Management (ISRM)

Information security involves "protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction" to accomplish organisation's confidentiality, integrity, and availability of information. Information Security Management (ISM) is an information security process that:
**1)** identifies the organisation's IT environment and its criticality and prioritising its involvements to the organisation's business capabilities.
**2)** identifies all possible IT security risks, assesses, and finally mitigates them.
**3)** provides frequent improvement of the organisation's security risk position (Raggad, 2010).

A Crucial component of Information Security Management is risk management, which itself has become a formal component of ISM referred to as Information Security Risk Management (ISRM) and defined as "the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what countermeasures to take in reducing risk to an acceptable level, based on the value of the information resource to the organisation" (Raggad, 2010).

### 2.3 Current ISRM Approaches and Methodologies

ISRM is not a new research domain. Other mechanisms have been used for some time. As long ago as 1975, Annual Loss Expectancy (ALE) had been proposed by the US National Bureau of Standards for measuring IT risks. ALE was very basic and could not distinguish between high or low impact of events. After a series of workshops in the 1980s by the US National Bureau of Standards, ALE evolved into an iterative process for information security risk management with the following steps: requirements identifications, threats analysis, risk measurement, acceptance test, protection and implementation. The following ISRM methodologies are the most adopted and widely in use today.

### 2.3.1 NIST 800-39

National Institute of Standards and Technology NIST a part of the United State Department of Commerce has developed information security framework for the federal government and its contractors. The idea is to enhance information security and improve risk management processes (Ross et al., 2011). NIST 800-39 includes four main components: framing risks, assessing risks, responding to risks, and monitoring risks (Fenz et al., 2014).

### 2.3.2 OCTAVE

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) was developed by CERT Coordination Centre (Vorster and Labuschagne, 2005). It is an ISRM framework that provides organisations with processes to understand, assess and address their information security risks from their internal perspective. It is a methodology that identifies, prioritises and manages information security risks.

### 2.3.3 ISO/IEC 27005

This International Standard provides guidelines for information security risk management. It supports “the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach”. It can be adopted by all types of organisations including commercial enterprises, government agencies, etc. (ISO/IEC27005, 2011). ISO/IEC 27005 divides information security risk management into three main phases: risk assessment, risk treatment and risk acceptance.

### 2.3.4 CRAMM

The reason behind the development of “Central Computer and Telecommunications Agency” Risk Analysis Management & Methodology (CRAMM) was the need for a subjective and vulnerability driven information security risk management methodology. CRAMM focuses primarily on technical security aspects and the main phases are identification and evaluation of assets, assessment of threat and vulnerability, and selection and recommendation of countermeasure. One of the CRAMM main issues that it has been developed focusing on large (Fenz et al., 2014).

## 2.4 Information Security in Saudi Arabia

The latest Kaspersky report (2014) categorises Saudi Arabia as “High Risk” with 53% infected personal computers and 36% of connected users facing cyberattacks. Cyber threats are also large. For example, Saudi Aramco, the world’s largest oil producer, had a catastrophic cyberattack in 2012. Its computer network was struck by a very aggressive virus, Shamoon, which damages as many as 30,000 computers, deleting all hard drive data. It took about two weeks to recover and cost the company millions of Dollars to rectify (Bronk and Tikk-Ringas, 2013). Most of Saudi Arabian organisations focus on information security technologies rather than the human aspect to protect information assets from any vulnerability that could lead to possible data breach or attacks (Alzamil, 2012), which represents improper ISRM implementation. The total ICT spend in Saudi Arabia in 2015 could reach $36.95 Billion according to International Data Corporation's newly released predictions (McBride, 2015). That means the country spends an adequate amount of money on its IT security and infrastructure; however, managing IT is not a success.

## 2.5 Information Security Culture in Saudi Arabia

Studies by (Alarifi et al., 2012) show there is a far higher level of creating very simple passwords in Saudi Arabia 45% compared to South Africa, which is only 9.1%. As well, 35.8% people share their passwords with others in Saudi Arabia compared to 0% in South Africa. In addition, 65.7% Saudis have never changed their passwords compared to only 27.3% in South Africa.  Poor IT planning, lack of expertise, and low levels of management support as well as cultural and social barriers are the major information security problems in Saudi Arabia (Alnatheer, 2012). Employee behaviour has a big impact on information security in organisations. It has been disclosed that 80% of security failures were the result of weak employee’s security behaviour. It has been supported by other studies in which most of information security threats are initiated by irresponsible employees who do not follow information security policies and procedures of their organisations. “Cultural concept can help different segments of the organisation to concern about the information security within the organisation” (Lim et al., 2009). Social and cultural characteristics of Arab and Muslim countries are different from the West countries. Professional aspects and deals with IT acceptance (of which ISRM is a component) are affected by social and cultural characteristics (Al-Gahtani, 2004).

### 2.6 Evaluating ISRM Adoption in Saudi Arabian Organisations

Global distribution of ISO/IEC 27001 certificates in 2013 survey (2014) shows that out of 22,293 ISO 27001 certified companies around the world, there are only 59 Saudi Arabian certified companies. ISRM has a very poor uptake in this country. AbuSaad et al. (2011) have studied 8 out of 13 ISO 27001 certified Saudi Arabian organisations. They concluded that during the ISRM implementation phase, identifying the organisation's assets and team’s lack of experience are the major obstacles. Another study by AbuMusa (2009) revealed that more than 60 percent of respondents stated that managing information systems are not audited in Saudi Arabian organisations.

Perhaps in line with the poor adoption of ISRM in Saudi Arabia there is little evidence of relevant research in the context of that country or indeed of other Gulf countries. This study will add to the knowledge base and as scaffolding for further research and practice with regard to regional cultures. It will also make a contribution in comparative studies between western and Middle Eastern countries and deliver a better understanding of the mechanisms at work in both areas. It will develop the existing ISRM frameworks for Saudi Arabia organisations to allow them to contribute to improved risk management of information security. Also, it will evaluate current ISRM adoptability in Saudi Arabian organisations and will reveal ISRM critical success and failure factors in Saudi Arabian organisations.

## 3. RESEARCH METHOD AND RESEARCH QUESTIONS

A design Science approach is proposed in this study. Venable (2006) states that Design Science Research (DSR) provides “constructs, models, methods, instantiations, and better theories”. According to Hevner et al. (2004), design science research points serious and unresolved problems in innovative or unique ways or resolved problems in more efficient or effective ways. This research lends itself well to a Design Science Research “DSR” methodology in developing a localized, culturally sensitive and applicable ISRM framework.

Specifically, the following research questions are addressed:

1. What are the key success and failure factors of effective ISRM implementation in the Saudi Arabian context?
2. What are the critical cultural, social and technological factors that must be considered for developing ISRM framework for Saudi Arabian organisations?
3. How could Saudi Arabian enterprise organisations improve their information security risk management using the newly adopted and developed ISRM framework?

This research will be divided into five phases to accomplish its objectives as follows:

**Phase 1 -** Problem Formulation and Identification:

Stage One: Literature Review

Stage Two: Gathering Data using semi-structured interviews. This research will involve semi-structured interviews as primary source of data in order to evaluate the current state of ISRM in Saudi Arabia and understand the information security problems and challenges faces organisations. This stage will be divided into two parts:

1) Interviewing Saudi Arabian organisation CIO’s, IT managers, security engineers and security analyst to identify the problem and evaluate ISRM current state in participants organisations

2) Interviewing IT vendors and systems integrator and software’s developer companies in Saudi Arabia to triangulate findings and identify gaps

**Phase 2 -** Data Analysis **-** Theory Building: The data collected from the semi-structured interviews and the literature will be analysed to identify critical ISRM factors necessary for Saudi Arabian organisations in order to build the theory and identify gaps.

**Phase 3 -** Developing New Framework – Purposeful Artefact Design: This phase will manage and control the problems identified in the previous phase. A new integrated coherent ISRM framework for Saudi Arabian organisations will be develop based on previously developed international ISRM frameworks

**Phase 4 -** Focus Groups **-** Purposeful Artefact Evaluation: In Design Science Research, evaluation is considered as a key activity (Hevner et al. 2004). The new ISRM framework will be reviewed and evaluated by focus groups and used to further refine the new framework. A set of three focus groups from different Saudi Arabian companies will be going over the new ISRM framework and provide their feedback and comments. Each focus group will be five to seven participants including CIO's, IT managers, security engineers and security analyst. The Methodology for Evaluation in Design Science (MEDS) will be adopted in this phase to evaluate the new ISRM framework

**Phase 5 -** Enhancing and Confirming New Framework **-** Purposeful Artefact Design: The feedback and results provided by focus groups will be further enhance and finalize the newly developed ISRM framework for Saudi Arabian enterprise organisations.

## 4. RESEARCH OUTCOME

There is little evidence of ISRM research in a Saudi Arabian context and development of this framework will add to the knowledge base for further research and practice, and in an extension of knowledge in ISRM in Saudi Arabia, and due to its cultural, commercial and economic similarities to other countries in the Arabian Gulf region, serve as a base for comparative studies between western countries and Middle Eastern countries. This research will develop the existing ISRM frameworks for Saudi Arabia organisations that will improve risk management of information security. Also, it will evaluate current ISRM adoptability in Saudi Arabian organisations and will reveal ISRM critical success and failure factors in Saudi Arabian organizations. Review of literatures and one-to-one interviews will be the primary raw data to build the new ISRM framework based on current ISRM frameworks where focus groups will ensure the framework practicality.

## 5. CONCLUSION

In conclusion, this research will provide improved ISRM framework implementation and effectiveness in enterprise organisations in Saudi Arabia, with further relevance to other Gulf countries. Also, it will increase the knowledge base of ISRM in Saudi Arabia to assist organisations in Saudi Arabia to adopt ISRM and implement it more effectively and mitigate information security risk to acceptable levels.

## REFERENCES

Abusaad, B., Saeed, F., Alghathbar, K. & Khan, B. Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned. Australian Information Security Management Conference, 5th -7th December, 2011 2011. secau Security Research Centre, Edith Cowan University, Perth, Western Australia.

Al-Gahtani, S. 2004. Computer Technology Acceptance Success Factors in Saudi Arabia: An Exploratory Study. *Journal of Global Information Technology Management*, 7**,** 5-29.

Alarifi, A., Tootell, H. & Hyland, P. A study of information security awareness and practices in Saudi Arabia. Communications and Information Technology (ICCIT), 2012 International Conference on, 26-28 June 2012 2012. 6-12.

Alnatheer, M. A. 2012. *Understanding and measuring information security culture in developing countries: case of Saudi Arabia.* Queensland University of Technology.

Alzamil, Z. A. 2012. Information Security Awareness at Saudi Arabians' Organizations: An Information Technology Employee's Perspective. *International Journal of Information Security and Privacy,* 6**,** 38-55.

Blake, E. 2015. *Iran and Saudi Arabia Heading Toward A Cyber War* [Online]. Available: http://www.ibtimes.com/iran-saudi-arabia-heading-toward-cyber-war-1989789 [Accessed 30 November 2015].

Bronk, C. & Tikk-Ringas, E. 2013. The Cyber Attack on Saudi Aramco. *Survival,* 55**,** 81-96.

Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. 2014. Current challenges in information security risk management. *Information Management & Computer Security,* 22**,** 410.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. *MIS Quarterly,* 28**,** 75-105.

ISO/IEC27005 2011. Information technology — Security techniques — Information security risk management. Switzerland: International Standards Organization (ISO).

ISO/TR31004 2013. Risk management — Guidance for the implementation of ISO 31000. Switzerland: International Standards Organization (ISO).

Lim, J. S., Chang, S., Maynard, S. & Ahmad, A. Exploring the relationship between organizational culture and information security culture. Australian Information Security Management Conference, 2009. 12.

Mcbride, S. 2015. *Saudi ICT spend to near $37bn in 2015: IDC* [Online]. ITP. Available: http://www.itp.net/601452-saudi-ict-spend-to-near-37bn-in-2015-idc [Accessed 20/8/2015 2015].

Mccumber, J. 2004. *Assessing and Managing Security Risk in IT Systems*, Auerbach Publications.

Ponemon Institute 2015. 2015 Cost of Data Breach Study: Arabian Region. Traverse City, Michigan USA.

Raggad, B. G. 2010. *Information security management: concepts and practice*, CRC Press.

Ross, R., Bodeau, D., Williams, P., Stoneburner, G., Rodrigo, S., Quigg, K., Fabius, J., Gouldmann, P., Sames, C., Dempsey, K., Johnson, A. & Enloe, C. 2011. NIST 800-39 Managing Information Security Risk. *Nist special publication,* 800.

Stoneburner, G. G., Alice; Feringa, Alexis 2002. *Risk Management Guide for Information Technology Systems* [Online]. National Institute of Standards and Technology. Available: csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [Accessed 29 April 2015 2015].

Venable, J. 2006. The role of theory and theorising in design science research. *Proceedings of the First International Conference on Design Science Research in Information Systems and Technology in Alan Hevner and Samir Chatterjee.* Claremont, CA, USA.

Vorster, A. & Labuschagne, L. 2005. A framework for comparing different information security risk analysis methodologies. *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries.* White River, South Africa: South African Institute for Computer Scientists and Information Technologists.