CHAPTER 8

CONCLUSION

This chapter summarizes the whole thesis and provides conclusion, recommendation and future research directions.

8.1. Conclusion

Enterprises are continually challenged to increase the breadth and depth of their information security governance and security controls, often having to align to their business objectives. This forces the continual management and maintenance of security technologies, frequently requiring enterprises to master specific methods of software design and infrastructure configuration.

Through interview and discussion, it was possible to arrive at a consensus that a strategically balanced approach is required to achieve IT governance that integrates people, process and technology.

A conceptual model of IT-GRC for optimizing enterprise information security was developed and proposed as a balanced solution, underpinning the theoretical philosophies that influence the transition of information security from a technical perspective to information security governance. Thus governance can be achieved by fostering a security culture that leads to an optimized enterprise information security system in modern complex business environments. An innovative enterprise-wide security governance model providing a flexible decentralized decision making perspective with accountability and focusing on security objectives and strategies is devised.

This conceptual model included ERM as a unifying platform to integrate governance strategy, security polices and certification & evaluation for compliance to achieve
organizational transparency. This model provides opportunities to explore and exploit emerging threats and vulnerabilities and dynamically change security strategies in response to external environments. The findings from the questionnaire show that majority of information security practitioners in Oman are aware of COSO framework but unfortunately COSO is presumed as complex due to excessive grouping of risks and also fails to provide direction from an implementation perspective. To address this problem, risk was classified into three categories such as business risks, technical risks and regulatory risks. Based on these categories, a conceptual maturity model was developed which defines four different approaches such as due-diligence, probabilistic risk analysis, scenario-based approach and system analysis approach for managing enterprise risk.

In order to optimize information security, the IT infrastructure which acts as an enabler to business, needs to be optimized. To accomplish this, server virtualization strategy using bare-metal architecture was practically implemented to dynamically manage resource allocation. This implementation was successfully tested to help enterprises to overcome the typical concerns of modern data centre and provide many benefits such as high availability, scalability, cost reduction, minimizing floor space and enhanced security.

Research findings in these public sector enterprises which were used as a case study showed that there is lack of analytics and reporting system on the use of information assets and its security implications across the enterprise. This revealed that a robust IT governance framework was missing to deliver measurable value to the business while improving the productivity. Although COBIT provides direction to IT governance, it rarely defines the implementation details. Hence a framework was developed after evaluating the four domains of COBIT and selecting the most critical control
objectives and implemented IT governance within a short span of time and with limited resources. The implementation was done by mapping the selected control objectives with various best practices such as Prince2, ITIL and ISO 27002 for effective ITG implementation.

The findings of the interviews show that most of the information security assessors are not experts in virtualization since they do not understand the technical intricacies to ascertain if a specific design and configuration is secure. Also many of them confessed that they struggled with virtualization as no formal frameworks for auditing in virtual environments are prescribed. The notion of effective auditing in virtual environment was discussed and taxonomy of risks inherent in virtual environments and relevant control objectives was provided. The finding of this research shows that a formal framework for successful auditing in virtual environment is necessary and was devised.

A novel approach using methodical models is devised to optimize IT-GRC. The scientifically proven methodology called DEMATEL is used for analysis of expert’s opinion thereby calculating the “Influence and Cause” of security controls of the overall system. Further, FoM attribute was calculated to gives the “Fair Value” for each set of solutions in which the maximum value is considered as an optimal value. This approach provides a simple and effective IT-GRC implementation mechanism for organizations thus eliminating the need to buy commercial GRC platforms / tools which are relatively expensive. The approach gives the liberty to choose any suitable information security control framework/standard and predict the effectiveness of the security control thus enabling informed decision making.

Balancing between the need for continual mastery of system and application configuration on the one hand and the need to stay ahead of the numerous
requirements of internal and external stakeholders on the other forms the foundation of the series of recommendations provided in this research.

8.2. Recommendations

Following are the recommendations provided:

A strategically balanced GRC model should be adopted to maintain optimized risk management, governance and enterprise information security policies in synchronization with each other and at the same time attaining a high level of transparency.

Enterprise information security policy should be used to ensure that its taxonomies created and outputs can be used for compliance and effective governance.

Information security should not be treated as just a technical issue rather as a business issue which can stimulate high degree of transparency and information velocity throughout an enterprise.

Risk management function should be integrated across the enterprise with insights into just how mitigation of risks, cost controls and process integration are all contributing to overall financial performance.

IT governance should be implemented using COBIT framework by identifying critical success factors in an enterprise and make use various best practices available. Further, the data collected from analytics has been used to track performance and revisit the control objectives thus making the adoption of COBIT controls more consistent.

Emerging technologies such as virtualization and cloud computing should be utilized to enhance revenue opportunities with optimal security.

Management should develop a culture of compliance through auditing such that security functions and accountability within the enterprise fit the governance structure.
Auditing framework should be used to audit virtual infrastructure for compliance that leads towards achieving certification through evaluation and a structured and reporting mechanism to the senior management for effective governance.

8.3. Future Work

Outsourcing aspect of cloud computing raises serious concerns about the security and privacy of the data assets that are outsourced to providers of cloud services especially in public cloud is worth researching.

This work can be extended by selecting the security controls rather than control objectives and calculating the FoM for governance, risk management and compliance exclusively for more precision. In order to arrive at higher accuracy multiple subject experts’ opinion can be considered.