2011

An exploratory study of ERM perception in Oman and proposing a maturity model for risk optimization

Arun N. Shivashankarappa
Coventry University, United Kingdom

D Ramalingam
Coventry University, United Kingdom

Leonid Smalov
Coventry University, United Kingdom

N Anbazhagan
Coventry University, United Kingdom

DOI: 10.4225/75/57b549eccd8ca
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

AN EXPLORATORY STUDY OF ERM PERCEPTION IN OMAN AND PROPOSING A MATURITY MODEL FOR RISK OPTIMIZATION

Arun N Shivashankarappa, D Ramalingam,Leonid Smalov, N Anbazhagan
Middle East College of Information Technology, Muscat, Majan College (University College), Muscat, Coventry University, United Kingdom, Alagappa University, Karaikudi, India
arun@mecit.edu.om , ramalingam.d@majancollege.edu.om,
csx211@coventry.ac.uk,anbazhagan_n@yahoo.co.in

Abstract

Enterprise Risk management is a process vital to enterprise governance which has gained tremendous momentum in modern business due to the dynamic nature of threats, vulnerability and stringent regulatory requirements. The business owners have realized that, risk creates opportunity which in turn creates value. Identifying and mitigating risk proactively across the enterprise is the purview of Enterprise Risk Management (ERM).However, key errors in the ERM process such as misinterpretation of statistical data, overlooking change management, inadequate attention to supply chain interdependencies, excessive trust of insiders and business partners, ambiguous grouping of risks and poor documentation has contributed significantly to the failure of ERM. To examine the ERM perception in Oman, the authors have conducted a survey among various risk management practitioners. Based on the findings, the authors have broadly classified risk into three types namely business risks, technical risks and regulatory risks and threat vs. consequence mapping is defined to provide direction to moderately group risks. Further, this article defines various ERM approaches including due diligence, probabilistic risk analysis, scenario-based analysis and system analysis which offers a wide range of decision-support tools to the management.

Keywords
Enterprise Risk Management, Maturity model for ERM, Information Security Risk Management.

INTRODUCTION

EnterpriseRisk Management is emerging as a new phenomenon in contemporary business. Risk is always a part of any business and managing risk is an essential function for any enterprise. Deloitte &Touches' report argues that risk management is gaining importance due to the dynamic nature and complexity in contemporary business environment (Deloitte& Touch LLP, 2009). The research report from (AESRM) also emphasis that enterprises are becoming more complex in a global economy where external partners are on the rise with significant outsourcing and value is shifting from physical to information based assets(Booz Allen Hamilton, 2005).

Due to the ubiquitous nature of computing, enterprises are increasingly dependent on information based assets to make strategic decisions and operationally run the business. With the heightened competition from globalization, new technologies emerge and thus introducing new threats and vulnerabilities which are not only complex but also unpredictable in nature(Shivashankarappa & Ramalingam, 2010). As a result of this, enterprises are witnessing a phenomenal thrust in information security related risks. On the other hand, many enterprises are recognizing that risks are no longer hazards to be avoided but, in many cases, opportunities to be embraced(Miccolis, 2003).

Identifying and mitigating risk proactively across the enterprise is the purview of Enterprise Risk Management (ERM), which may entail everything from avoiding suspension of business applications and loss of public trust to assessing regulatory risks.ERM has been implemented to a certain degree in financial institutions, health care and insurance industry, petroleum and energy industries due to the fact that these enterprises were governed by regulatory requirements such as SOX, HIPPA, BASEL-II and GLB(Calder, 2010).Later, ERM emerged to further include all areas of risk, and went beyond normal accounting rules, for writing down the assets and liabilities of a firm, working further to place a value both on the true market value of an item as well as on the risk associated with that asset(Cassidy, Gullive, & Terry, 2005).

ERM has to be fully functional by which it can increase the performance of the enterprise and provide a mechanism to the board and senior management to oversee the risks (Beasley, Clune, & Hermanson, 2005).

While ERM is on the rise, not all organizations are adopting it. Most organizations however are uncertain about how exactly to translate the concept of ERM to concrete actions steps that will help to enhance stakeholder value(Beasley, Clune, & Hermanson, 2005). This article aims at investigating the ERM implementation constraints in Sultanate of Oman and then proposes a novel maturity model for attaining optimized enterprise risk management.

BACKGROUND

Sultanate of Oman; petroleum rich country in Arabian Gulf has now envisioned diversifying towards industrial developments (Ministry of National Economy, 1996). This vision has initiated multinational organizations to setup their business units or partner with enterprises in Oman to broaden their business opportunity and exchange technical expertise(Information Technology Authority, 2008). Recently, the nation's e-government strategy became priority and aims at interlinking government sectors and services through a unified system thus empowering its people through e-Oman initiatives. An interoperability framework was thus built by the Information Technology Authority (ITA) to enable government entities to integrate seamlessly to exchange business related data between e-government systems in order to provide efficient services to its subjects(Information Technology Authority, 2008). Research study by Pulkkinen, Naumenko and Luostarinen states that there are several issues to be addressed before such complex heterogeneous information systems are integrated irrespective of the geographical locations of the collaborating partners(Pulkkinen, Naumenko, & Luostarinen, 2007).

Public and private organizations have realized the need for effective risk management strategy after the cyclone "GONU" which hit the shores of Oman in the year 2007, causing a total of four billion US Dollar losses to many organizations. This incident taught enterprises across the country that the unthinkable can happen and they must be proactive in managing risks and necessary processes need to be implemented and reviewed periodically to minimize the impact of consequences (Al-Badi, Ashrafi, Al-Majeeni, & Mayhew, 2009).

Research reveals that risk is a business notion, not a technical one, in the sense that risks for a business are owned by the owners of the business and typically must be accepted by responsible management. Sarbanes Oxley Act (SOX) of 2002, expresses this by placing legal responsibility with the chief executive officer (CEO) and chief financial officer (CFO)(Zhi, 2009). This is what is intended, but oftentimes doesn't happen. As researchers argue, even though ERM is well defined and adopted in developed countries, the enterprises face major issues due to the non-operation of policies, lack of transparency and the lack of management commitment that led to the collapse of the high profile enterprises such as Satyam computers, Parmalat, WorldCom, Lehman Brothers, Merrill Lynch and American International Group(Bhandari, 2009)(Lees, 2004)(Kutsikos & Bekiaris, 2007).

PROBLEM STATEMENT

The management of enterprise risk is undergoing a phenomenal change worldwide since they are moving away from the silo-by-silo approach to manage risk to more comprehensively and coherently (Gordon, Loeb, & Tseng, 2009). Due to the complexity of contemporary enterprises, risk managers cannot efficiently list all the possible threats, vulnerabilities and consequences. The vulnerability of one enterprise can affect another enterprise's security and a breach in one enterprise can have a cascading effect on its partners(Huang, Behara, & Hu, 2008). However the Committee of Sponsoring Organizations (COSO) of the Treadway Commissionis available that requires senior management to look at risk-related issues and implement risk management processes. Unfortunately in COSO framework, the grouping of risks is done excessively which is vagueand leads to confusion.Another issue in COSO is that, "*it does not get into risk management approaches and processes that can be easily implemented across the enterprise, rather focuses on philosophy and vision of ERM*". Further, it lacks emphasis to technical risks such as information technology (IT)/security controls(Rasmussen & Koetzle, 2007).

The major problem in ERM is the tendency to misinterpret statistical data. Since emerging threats produce very little statistical information, as a result of which vulnerability assessment becomes unreliable, and the inferences made out of this model will not be useful.As threats, vulnerabilities, and consequences change over time, effective risk management must be an adaptive process. For example, a system that has been assessed at some point in time permits it to operate in an acceptable risk profile relative to that context. After that point, small changes in the system are made over time, but these incremental changes rarely result in new risk management decisions. This is because the decisions are not recorded due to lack of documentation which is essential while revisiting risk management decisions.

Another major source of failures in risk management is excessive trust in insiders and business partners. The executives who have risk management responsibility poorly understand business risks to the extent necessary to assess and control business risks since the top management does not engage personally in this process.Globalization enabled by extended networks and outsourcing has diminished the perimeter of control, which has led to new regulatory environments and conflicting compliance obligations(The Economist Intelligence Unit, 2008).

APPROACH

To address the above said problems, a survey was administered to 110 security practitioners in Oman through Google documents available at the following link.
https://docs.google.com/spreadsheet/viewform?formkey=dGNGcjVRNm1GM2N6SmlVbEdGWkVHRGc6MQ
There were sixty respondents out of one hundred and ten distributions making an average of 54.5 % response rate. Key findings from the survey illustrates (figure 1&2) that the practitioners are aware of COSO framework but most of them were unable to understand it, since it is too complex from an implementation perspective. Others said that they outsourced to third party consultants who unfortunately put checklists in the hands of relatively inexperienced individuals rather than performing the in-depth analysis of business issues.

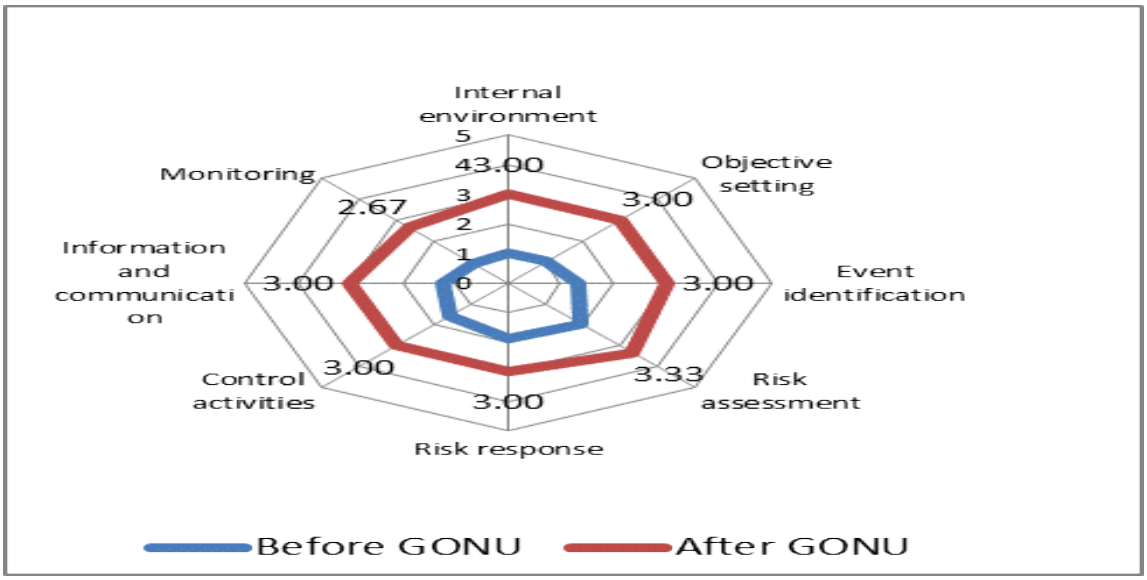

Figure 14 COSO awareness before and after GONU

Before "GONU", security was viewed as a liability and most CEO's believed that security is a technical problem and the responsibility lies with the IT managers. Hence, there was minimal or no comprehensive risk assessment and risk response as a result of which few controls were applied without periodic monitoring. Interestingly, "GONU" became an eye opener and the graph illustrates that there is a steady improvement in all the factors of risk management.Another vital finding is that most enterprises are not giving attention to regulatory risk especially cross borderregulatory requirements since it lacks clarity. The detailed findings and suitable recommendations are provided in the next section.

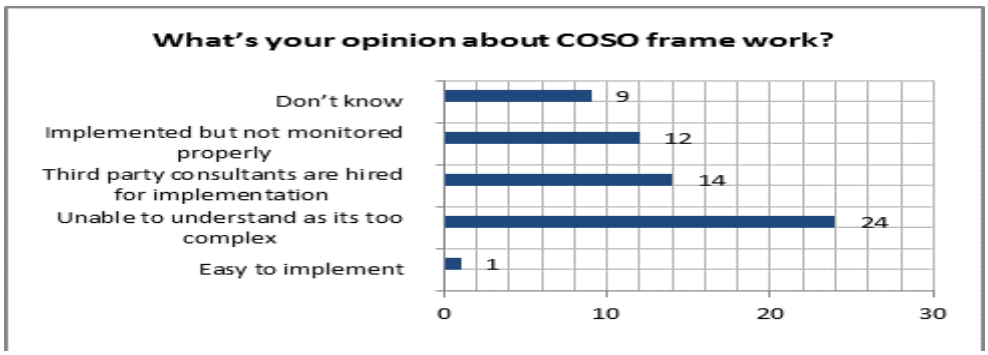

Figure 15 COSO Opinion

FINDINGS AND RECOMMENDATIONS

Detailed findings of the survey and recommendations are compiled in Table-1.

Table-1: Findings and Recommendations

Security Context	Information Security Policy
Finding	Executives have a fair knowledge about security policies but it is not implemented across the enterprise since it is not ratified and communicated.
Recommendation	Policies and standards must be created with well-defined roles and responsibilities. A formalized compliance program must be developed and closely monitored.
Security Context	Enterprise Security Architecture
Finding	A few Project design artifacts and network diagrams do exist which are developed by IT managers and it solely depends on their expertise. No Security Architect role exists.
Recommendation	Enterprise security architecture must be developed that is aligned to risk strategy and policies. A security architect role must exist who in turn seeks advice from security experts to architect solutions.
Security Context	Governance Structure
Finding	Roles and responsibilities for enterprise security are not clearly defined and no formal governance structure exists. Security is handled in an ad-hoc basis or addressed reactively.
Recommendation	Governance framework needs to be created and aligned to risk strategy. Roles and responsibilities must be spelt out clearly specifying compliance requirements.
Security Context	Asset Profiling
Finding	Asset classification is not done in most enterprises.
Recommendation	Asset profiling process must be done which is aligned to risk strategy and governance framework.
Security Context	Enterprise Risk Management
Finding	Enterprise Risk Management strategy is mostly undeveloped.
Recommendation	Enterprise Risk Management strategy has to be developed with senior management commitment.
Security Context	Archiving
Finding	Most organizations do not have a archiving policy however periodic backup is taken and stored locally.
Recommendation	Archiving policy must be defined and information must be encrypted and stored at a remote location in safe and secure environment.
Security Context	Disaster Recovery and Business Continuity Planning
Finding	Some organizations have disaster recovery and business continuity plan however it's not tested.
Recommendation	Testing strategy has to be devised and periodic testing of DR/BC plan needs to be enforced.
Security Context	Awareness and Training
Finding	There is no scheduled awareness training program. However management shows keen awareness only when an incident is reported but it loses focus over a period of time.
Recommendation	Training and awareness program must be scheduled periodically, and ensure that all employees have basic knowledge of security issues.

Besides this, eight practitioners were interviewed and it was evident through interviews that, management tends to neglect security mechanisms that are in place. Hence, measuring and monitoring the effectiveness of security controls needs to be done periodically to provide clarity about the controls that are protecting the organizational assets. Next aspect that's found is that extended enterprises produce information supply chains which create interdependencies among business partners which are mostly ignored by the managers. In these situations, interdependency analysis using scenarios will be helpful. Also, it's evident that most managers underestimate insider threats and rarely attend to the business risks. Due to the cultural setup in Oman, social engineering attacks are relatively easy due to excessive trust in relationships. Therefore, attention should be given to create awareness among employees and manage business risks to avoid negative publicity which can lead to loss of reputation and brand value. Finally, the threat due to IT is mostly taken care; however it lacks proper documentation which is essential for risk management.

To achieve the recommendations presented in table-1 an ERM program should be selected based on the severity of threats and consequences the enterprise actually faces. Hence, threats and consequences must be expressed in business related terms which should be easily understood by non-technical executives. The following figure (see figure 3) provides direction for classifying severity vs. consequence of risks. In this figure, the authors have broadly classified risk into three types namely

1. Business risks,
2. Technical risks and
3. Regulatory risk.

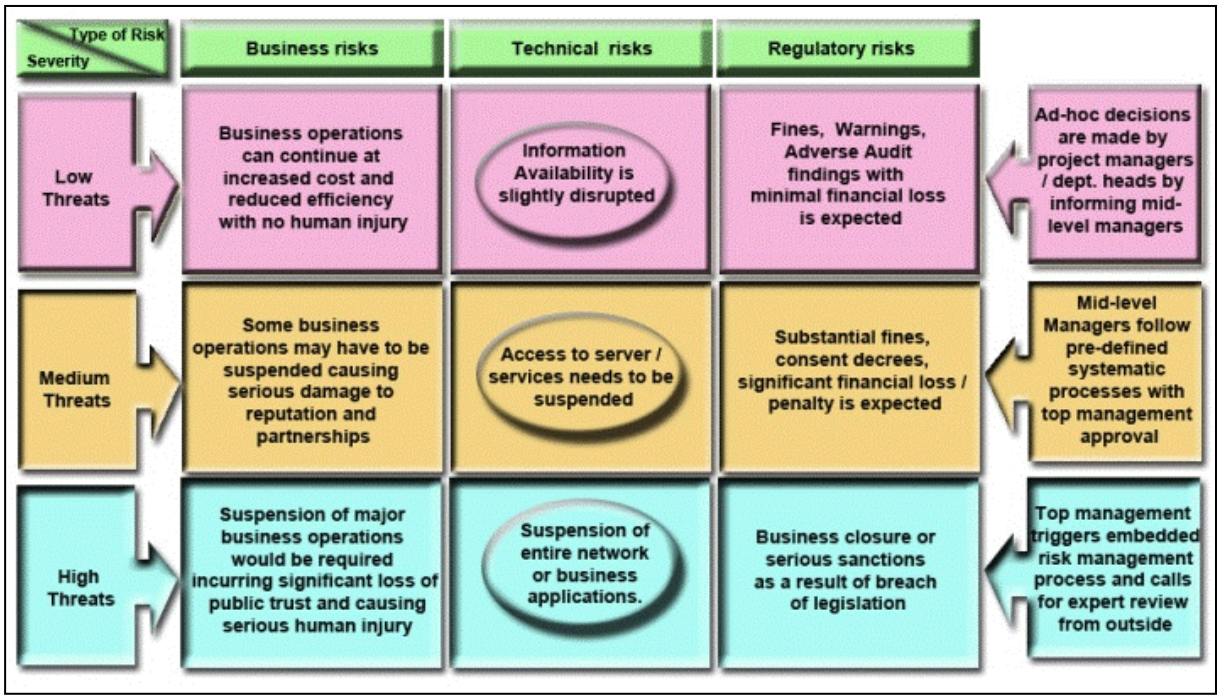

Figure 3: Classification of risks based on its severity

Based on the severity, there are three criteria set such as low, medium and high consequences. Further, for each criterion, the nature of decisions and the typical decision makers are defined. The above classifications will help the CEOs', CFO's and CIOs' to better understand the business risk and establish a standard of due care and derives from practical experience and knowledge in the business. The IT managers and enterprise security architects will understand technical risks and develop enterprise security architecture which is aligned to risk strategy and apply control standards to drive the security objectives of confidentiality integrity and availability. Legal advisors need to understand thoroughly the specific regulatory mandates for guidance and legal risks associated with contracts, vendors, employees, and national and transnational jurisdictions. COSO is really the only viable candidate for top-level risk management which is also supported for regulatory compliance by SOX regulators, making it a de- facto standard for that purpose(Rasmussen & Koetzle, 2007). COSO ERM fails to give enough practical advice from an implementation viewpoint and the approach to ERM is confusing. Rasmussen in his research report argues that COSO ERM focuses excessively on threats/hazards but it fails to

give practical guidance on how you should measure the effectiveness and efficiency of controls(Rasmussen & Koetzle, 2007).

CHOOSING A RISK MANAGEMENT APPROACH

The vital parameters in deciding an appropriate enterprise risk management approach encompasses business risks, caused due to external entities, technical risks evolving due to extended networks and regulatory risks caused due to cross-border relations. The spectrum generally runs from ad-hoc approach used with due diligence by relatively low level employees to an integratedenterprise risk management achieved through system analysis approach. In the informal stage, enterprises use manual controls with no best practices whereas in reactive stage, it's more project oriented and compliance based. In proactive stage, automated risk assessment and monitoring is done with appropriate process control in place whereas in the optimized stage of maturity, automated risk mitigation/predictive risk analysis is done with an integrated ERM process. The following figure (see Figure 4) illustrates such an approach.

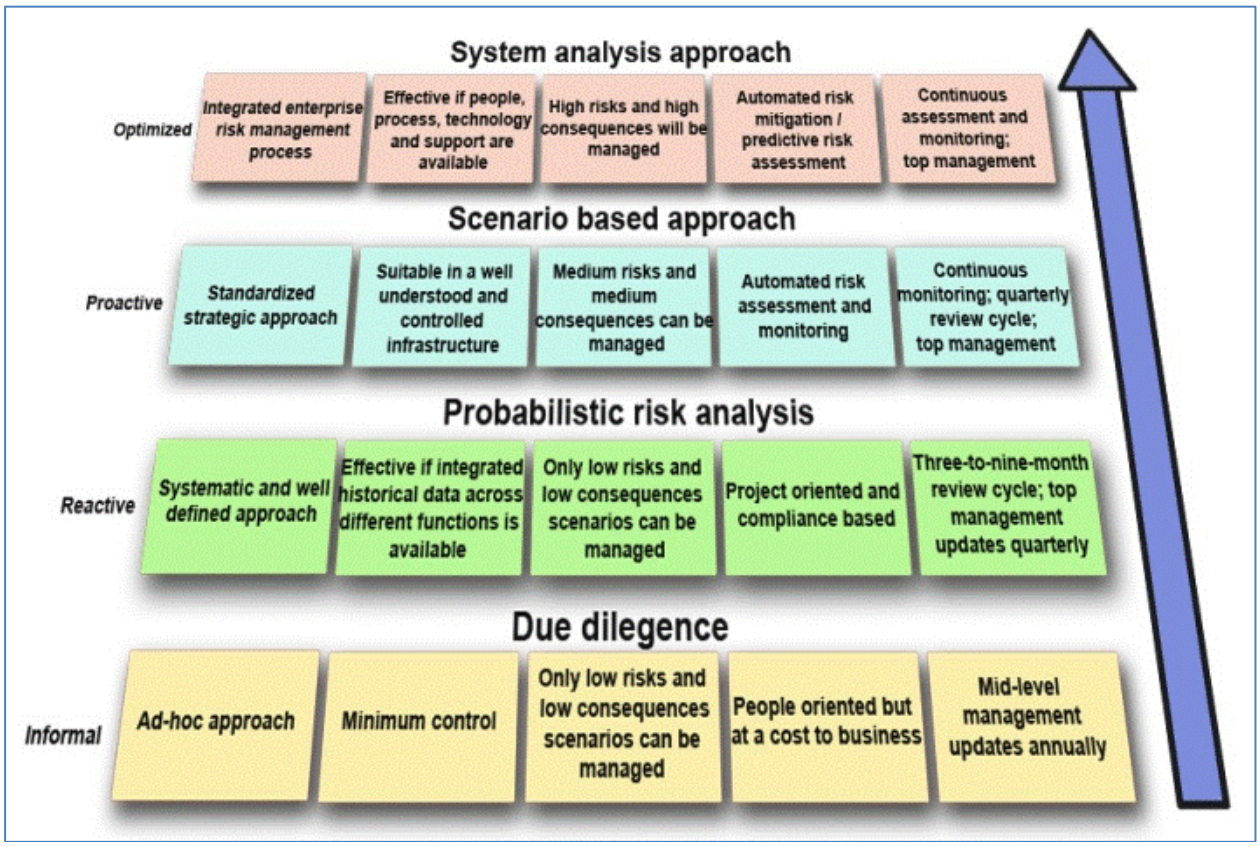

Figure 16 Risk Management Approaches

Due diligence

By this approach, operational managers make ad-hoc decisions with mid-managers approval. This approach is mostly people oriented rather than process oriented, where the decisions made are biased towards the individual's opinion and capabilities rather than giving significance to the organizational objectives. This approach should be applied at bare minimum although it is not sufficient but can address low risks with low consequences.

Probabilistic risk analysis

This approach can help in quantifying security risks for both externally initiated and internally initiated events by understanding the likelihood of occurrence and the consequences(Satoh & Kumamoto, 2009).This approach is effective when there is access to integrated historical data across different functions and the frequency of change is slow.

Scenario based approach

This approachis useful in a controlled environment where what-if scenarios can be explored and group consensus can be considered. Scenarios are generated to try to cover important events and outcomes. These scenarios can be "gamed" to explore various options and generate group agreement for dealing with the medium-risks.

System analysis approach

This is suitable for high risk situations which are tedious and costly since a sequence of events and interactions between disparate systems needs to be evaluated. It is applicable for analysis of petrochemical plants and defense organizations where the consequences are high. Normally managers ignore interdependencies among business partners, logistics outsourcing and ignore indirect losses. In high-consequence systems, managers should conduct interdependent system analysis with increasing detail at higher levels of threats and consequences.

CONCLUSION

ERM becomes a means of helping the organization shift its focus from crisis response and compliance to evaluating risks in business strategies proactively to enhance investment decision making and maximize stakeholder value. This research article critically investigates the risk management strategies adopted by enterprises in Oman and to determine how predictive risk assessment could be integrated into enterprise management process. Based on the findings, COSO implementation issues were identified, risk grouping have been done and a conceptual maturity model is proposed to attain optimal risk management. The proposed model defines various approaches such as due diligence, probabilistic risk analysis, scenario-based analysis and system analysis which offer a wide range of decision-support tools to the management.Enterprises can mature over a period of time from an informal ad-hoc approach to an optimized integrated enterprise risk management process through continuous assessment and monitoring.

REFERENCES

Ali H. Al-Badi, R. A.-M. (2009, September 14). IT disaster recovery: Oman and Cyclone Gonu lessons learned. *Information Management & Computer Security, 17*(2), 114-126.

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy, 24*(6), 521-531.

Bhandari, B. (2009). *The Satyam Saga.* (T. N. Ninan, Ed.) New Delhi: Business Standard.

Booz Allen Hamilton. (2005). *Convergence of Enterprise Security Organizations.* Reserch report, The Alliance for Enterprise Security Risk Management.

Calder, A. (2010). *Selling Information Security to the Board : A Primer.* Cambridgeshire: IT Governance Publishing.

Dainel P, C., William B, G., & Terry, T. S. (2005). *Addressing the Financial Risks from Retirement Systems Changing Our Focus: Consulting About Risk.* New Orleans Health/Pension Spring Meeting- 2005. New Orleans: Society of Actuaries.

Deloitte& Touch LLP. (2009, March). *Global Risk Management Survey, Fifth Edition.* Survey Report, Deloitte& Touch LLP, New York 10019-6754 USA. Retrieved May 12, 2011, from http://www.deloitte.com: http://www.deloitte.com/view/en_GX/global/industries/financial-services/48725312b90fb110VgnVCM100000ba42f00aRCRD.htm

Gordon, L. A., Martin P, L., & Chih-Yang, T. (2009, July-August). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), 301-327.

Huang, C., Behara, R., & Hu, Q. (2008, July-August). Managing Risk Propagation in Extended Enterprise Networks. *T Professional, 10*(4), 14-19.

Information Technology Authority. (2008). *e.oman Strategy* . Government Strategy, Information Technology Authority, Sultanate of Oman, Muscat.

Kutsikos, K., & Michail G, B. (2007). IT Governance Auditing in Virtual Organizations. *Management of International Business & Economic Systems, 1*(1), 35-45.

Lees, G. (2004). Improving strategic oversight: the CIMA strategic scorecard. *Measuring Business Excellence, 8*(4), 5-12.

Miccolis, J. (2003). *Overview of Enterprise Risk Management.* Casualty Actuarial Society, Enterprise Risk Management . Washington, D.C.: Enterprise Risk Management Commitee 2002.

Ministry of National Economy. (1996). *http://www.moneoman.gov.om/loader.aspx?view=planning-diverse&type=plan.* Planning and Development Strategy: Vision 2020, Ministry of National Economy, Sultanate of Oman, Muscat.

Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007, October). Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool. *The Journal of Systems and Software, 80*(10), 1607-1620.

Rasmussen, M., & Koetzle, L. (2007). *AS/NZ 4360 — A Practical Choice Over COSO ERM.* Best Practices, Forrester.

Satoh, N., & Kumamoto, H. (2009). An Application of Probabilistic Risk Assessment to Information Security Audit. *Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC '09)*, (pp. 436-443). Kyoto.

Shivashankarappa, & Ramalingam. (2010). Governance, Risk and Compliance Equilibrium Model for Optimizing Enterprise Information Security. In H. Arabnia (Ed.). Las Vegas: WORLDCOMP'10.

The Economist Intelligence Unit. (2008, October). *From Burden to Benefit: Making the most of regulatory risk management.* The Economist Intelligence Unit.

Zhi, L. (2009). The research on the problems of CEOs' legal status and legal liability. *International Journal of Law and Management, 51*(4), 245-259.