Information security risk assessment framework

Technology, Information Technology

Computer Sciences and Information Technology Annotated Bibliography Topic: Information Security Risk Assessment Framework and Metrics in the South Australia Real Estate Sector. Supervisor: Information Security Risk Assessment Framework and Metrics in the South Australia Real Estate Sector Australian Prudential Regulation Authority (2010) Prudential Practice Guide: PPG 234- Management of security risk in information and information technology. Web: http://www. apra. gov. au/Policy/upload/PPG_PPG234_MSRIT_012010_v7. pdf. Accessed on 10th April 2012. APRA records that Information Technology reporting and metrics has two issues that are paramount: regular reporting and effective IT security metrics. A formalized IT security reporting framework is necessary for adoption by a regulated institution. The framework should provide operational information and oversight in all sectors in IT security in relation to risk management framework. A clearly defined reporting and escalation thresholds are then incorporated by the framework. Mechanisms responsible for report coding must consider risk and control dimensions. According to APRA, sufficient management reporting enables effective oversight of performance in IT security management. Summary: Reporting strategy includes risk profile, exposure analysis, progress against strategy, incident analysis, system capacity and performance analysis, recovery status, infrastructure and software analysis, project assessment and analysis, audit findings and ageing reports and fraud analysis. Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys, Vol. 25. No. 4. New York, NY; U. S. A. Baskerville records that designers design information system

security models that are safe according to the set guidelines. Although some designs become unsafe, their motive is always right. The article analyzes security models developed in different computer generations. First-generation of computers applied checklist method. The second generation worked on mechanistic engineering methods and the third generation focuses on logical-transformational methods. Summary: Each method adopted in the tree computer generations differ in primary features, methods of system development and typical tools and security development methods and typical tools. Berghof Foundation for Peace Support (2008) Reflecting on Risk and Security Management: A learning case based on the experience of the Berghof Foundation for Conflict Studies in Sri Lanka. Sri Lanka. The case paper shares Berghof’s experience in coping with deteriorating security situation and how the foundation established its own risk and security management model. Security measures and activities adopted by Berghof in Sri Lanka create controversial issues and dilemmas in relation to security performance. From Berghof’s experience, security training should be availed to all staff. A smaller group of key staff should drive the initial process. They should be provided with knowledge and taught how to implement institutional changes. The initial security training sessions must be theoretical and more of hands on. Summary: Organizations that deal with conflict transformation should choose trainers who will implement a holistic approach to security. Chellappa, R. K. & Pavlou, A. P. (2002) Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management, Vol. 15 No. 5/6. MCB UP Limited. Chellapa & Pavlou reviews that commercial

transactions conducted electronically are occasionally prone to security threats. Consumer trust in these transactions is affected by perceived information security. Mechanisms designed to combat this form of security threat proposes protection, authentication and verification of perceived information. Technological solutions towards these strategies are derived from threats to consumers. Summary: The research conducted revealed a relationship between consumers professed information security and confidence in electronic commerce transactions. Dynes, S. (2008) Emergent Risks in Critical Infrastructure. IFIP International Federation for Information Processing, Vol. 290. Dynes records that from field studies, degree of dependence on information infrastructure in an organization and steps towards managing information risk are not well coordinated. Evidence still lacks about effective increase in IRM coordinating signals and robust inter-entity business process. IRM coordinating signals are required to increase resilience of inter-entity business process to cyber disruptions although not sufficient. Summary: Poorly understood modes of failure propagate information risks. This will in turn affect the ability of information security infrastructure. Ekelhart, A., Fenz, S. & Neubauer, T. (2009) AURUM: A Framework for Information Security Risk Management. From proceedings of the 42nd Hawaii International Conference on System Sciences-2009. IEEE. Pp. 1-8. The 42nd Hawaii conference discussed that currently, companies are forced to pay attention to security issues because of increased security threats. Companies are compelled to employ measures to measure security. To achieve this, they implement risk management approach. Risks are measured through assessment, mitigation and evaluation measures.

Detailed understanding of information technology security domain and company environment is essential in risk management approach. Summary: AURUM is a new method used in supporting NIST SP 800-30 risk management standards. It benefits modelers more than other models like GSTool and CRISAM. Federal Information Processing Standards Publication (FIPS PUB 199) (2004) Standards for Security Categorization of Federal Information and Information Systems. U. S. A. This publication records that the E-Government Act called Federal Information Security Management Act of 2002 (FISMA) became a public law in December 2002. The act recognized the importance of information security to economic and national security interests of U. S. The law tasked NIST to set guidelines and standards. Standards used to categorize information and information systems were developed. This categorization provides a common framework and understanding to express federal government security. Summary: Management of effective information systems is developed from the framework developed from the act. Fovino, N. O., Guidi, L. Masera, M. and Stefanini, A. (2010) Cyber security assessment of a power plant. Electric Power Systems Research 81 518-526. Elsevier B. V. The article reviews new trends of insecurity that pose a threat to infrastructure and systems. Insecurity risks are caused by new vulnerabilities and design weaknesses. These problems are facilitated by extensive use of information systems and technologies (ICT) into the complex systems. An intensive security framework requires a well distributed and integrated control system. The framework proposed relies on ISO/IEC 17799 standard because it fulfils three purposes. One, it frames the problem by stating information and

communication elements of the ICS that need protection. Two, categorize confidentiality, integrity and availability needs of ICS and three, define important security policies. Methods for security assessment are many although they depend on ICT based systems and infrastructure like CORS, EIBOS, INSAW and OCTAVE among others. Summary: INSAW methodology best fits ICT infrastructure of complex industrial systems. The methodology does not describe the system in terms of components, assets and the external world. Gordon, A. L. & Loeb, P. M. (2002) The Economics of Information Security Investment. Information and System Security, Vol. 5 No. 4. Pp. 438-457. ACM Transactions. From the article, computer-based information should be confidential, of integrity and available to responsible members only. The designed model to protect information systems of an organization should meet these requirements. Companies spend heavily for adoption of best models that offer security to their needs. Spending increase in the purchase of soft wares that detect viruses, firewalls, sophisticated encryption techniques, automated backups and hardware devices. Summary: Most companies that ignored to protect their systems recorded massive losses. Companies need to derive an economic model that will determine the optimal amount they should invest in information security. Hoo, S. J. K. (2000) How Much Is Enough? A Risk-Management Approach to Computer Security. CRISP, Stanford University. Pp. 7-27. How can security be determined to be enough? This is a complex issue in computer related risks. Binary view of security raised computer security risks to modelers during the first generation of computers. The view has complicated computer risk modeling into an endless web of assessment, disagreement and gridlock.

Approaches taken by second-generation offer temporary solutions to computer risk management. A modeling approach that concentrates on uncertainty and flexibility leaves room for further modifications. Summary: The techniques used for modeling should analyze decisions, be quantitative as well as analytic. Humpreys, E. (2008) Information security management standards: Compliance, governance and risk management. INFORMATION SECURITY TECHNICAL REPORT 13. Pp. 247-255. Elsevier Ltd. Humphrey reveals that one threat to information security is insider threat. Insider threats are threats caused by employees, staff, management or on-site contractors that take advantage of weaknesses in the systems, processes and applications. Their aim could be for personal gain and for reckless behavior. It may involve a person in Board of Directors level either the CEO or senior staff in management level. Summary: Cases for insider threats are common in firms and are on the rise. Successful management of security should therefore, start from the top. Kbar, G. (2008) Security Risk Analysis for Asset in relation to Vulnerability, Probability of Threats and Attacks. IEEE. In Kbar’s analysis, organization’s health in computer infrastructure depends on the process of network security management. The purpose of network security is to provide an organization’s computer infrastructure. An efficient network security is related to a well structured risk assessment. Network specialists need to identify particular risks facing the organization, potential impact of the risk and analyze the threats posed by the risks. Security network risk assessment depends on distinctive variables. The variables are; priorities set by network security supervisors and capability of security systems to threats. The distinctive elements and an effective risk

assessment should be considered in designing network security system. The paper highlights a new risk assessment methodology. The method relates risks on a particular asset to vulnerabilities prone to the asset. Risk for particular assets is analyzed based on varying possible vulnerabilities. Summary: Different values obtained from probability of attacks are calculated according to security control gates used to stop attacks. According to this methodology, when risks are high, vulnerability values of a particular asset also rise. Kjell, J. H. & et al. (2009) Assessing PKI: Risk Assessment of a National Security Infrastructure. The IEEE Computer Society. In the assessment, collection of all components essential in public-key infrastructure provides security that relies on public-key cryptography. Hard-wares, soft-wares, processes and people are required in the process. Most countries have introduced large-scale security frameworks in implementation of PKIs. Nationwide PKIs offer strong verification services and reduce risks related to security breaches. PKIs offer better security protection than frameworks that use frameworks allowing fixed or one-time passwords. Authentication provides a clear understanding of confidence that an identifier refers to a user or a Web site. The stronger the authentication, the higher the confidence. PKI authentication relies on certificates, corresponding private keys and an option for information revocation like CRL. The strength of authentication depends on three factors. Summary: One a well-tested authentication protocol like Transport Layer Security (TLS) protocol secure private-key storage and computational difficulty in the calculation of the private key. Kotulic, G. A & Clark, G. J. (2003) Why there aren’t more information security research studies, Information &

Management 41 (2004). ELSEVIER B. V. pp. 597-607. Information security environment for organizations is a complicated issue. Kotulic & Clark suggest that factors dealt with in information security are; IT platform, exploitation of electronic integration and network connectivity among others. Decision-making process in security strategies depends on business entities and strategies. Most organizations use the down-side nature of risk in determining decision-making behavior. The SRM program is a model developed with the same concept. The posture for the model is based on governance, countermeasures, structure, policy and procedures. Summary: The model considers expectations of an organization in Information Security area outside EUC domain and includes the role of executive management support. Ma, Q., Johnston, C. A. and Pearson, M. J. (2008) Information security management objectives and practices: a parsimonious framework. Information Management & Computer Security Vol. 16 (No. 3). Emarald Group Publishing Limited. From an empirical study conducted, the dimensions of information security, objectives and practices were examined. Inter-relationships between information security objectives and practices developed from a parsimonious framework were explored. The proposed framework should be used as a starting point in developing particular information objectives that reflect an organization’s environment and business goals. The proposed framework for ISM was derived from development of prioritized objectives and suggestions from reports and academic standards. Summary: The objectives should be refined depending on survey data received from certified security professionals and examination of inter-relationships between information security objectives

and practices. Matulevicius, R. et al. (2008) Adapting Secure Tropos for Security Risk Management during Early Phases of the Information System Development In. Dubois, E; Pohl, K. (Eds) CAiSE 2008, LNCS 5074. Pp. 541-555. The review states that most designers of information system target security in their models. Decisions are crucial in the early phase of modeling. The decision making-approach focuses on risk analysis and effective communication of information prone to risks. Current languages used in modeling can improve security in information systems and at the same time the languages can be improved. Summary: Secure Tropos is a language used in supporting information system development methodology and supports security risk management. Metayer, D. (2007) IT Security Analysis Best Practices and Formal Approaches. Springer-Verlag, Berlin Heidelberg. Metayer emphasizes that information technology security analysis does not have a well defined framework by actors and authors. Security analysis is the initial stage in security management. Situations are analyzed I relation to IT product to initiate decision making process. Security analysis and management should be a continuous practice trough a product’s design phase. Security analysis is also achieved in the evaluation process within internal improvement procedure or in official certification procedure. Currently, industrial security analysis methods fall into two categories: commercial methods and standards. Some examples of commercial methods are; FRAAP, STRIDE, ASTRA and Cigital method. Summary: Standards methods originate from international organizations like ISO or national bodies like SEI (Software Engineering Institute or NIST (National Institute of Standards and Technology). Molloy, I., Cheng, P. and Rohatgi, P. (2008)

Trading in Risk: Using Markets to Improve Access Control. ACM Publishers, USA. Research on information security has been classified into two classes; good and inadequate or safe and dangerous and ensures that no violation takes place. This is seen in virus scanners, intrusion detections, firewalls and spam filtering. Access control is used a mechanism for safe division between the two classes. Access control differentiates between allowed and denied at various levels. Risk is not considered as a finite resource. Tragedies that occur in systems under access control are beyond understanding. Access control system model’s an organization’s notion of risk. The goal of access control system is to manage access to sensitive data of an organization. Summary: The model suits best for risk market analysis. Malicious behaviors are easily detected because all participants must go through the market to access resources. National Institute of Standards and Technology (NIST) (2012) Security and Privacy Controls for Federal Information Systems and Organizations. U. S. Department of Commerce. Web: hhtp://csrc. nist. gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd. pdf. Accessed on 10th April 2012. Research conducted by NIST reveals that security controls for organizations and information systems are essential and have implications on operations and assets of organizations. Organizations have the responsibility in addressing information security considerations. Risks incurred in information coding processes and information systems need mitigation measures. Realistic implementation plans and security controls should be considered. Assurance levels must be realized in the process of security analysis. Organizations therefore need a risk management process that identifies, mitigates and monitors daily basic risks arising from

information and information systems. A set of guidelines for organizations is necessary. The guidelines apply to all components in information system network; information processing, storage or transmission. Summary: The guidelines support information systems security as well as effective risk management. Neudorfer, W. Marinos, L. and Schaumuller-Bichl, I. (2010) Business and IT Continuity Benchmarking. IFIP International Federation for Information Processing. Neudorfer, Marinos & Schaumuller-Bichl highlight that organizations are exposed to threats and vulnerability that hinder business lifespan. Business continuity process aims at improving an organization’s resilience. Establishment of such processes are time consuming and expensive. Though organizations vary in size, the need for risk management cannot be ignored. Organizations have to focus on their survival in the harsh exploitative environment. Business continuity is developed from relevant methodologies and standards. The test plan drafted includes scope of test, timetables and success criteria worked out. The BCM is finally sustained. Summary: Modification of the BCP is possible, depending on the demand for the program developed. Benchmarking Approach is used in risk assessment and risk management. Pfleeger, L. S. (2010) Security Metrics. Why Measuring Security Is Hard. The IEEE Computer and Reliability Societies. According to Pfleeger, calibration of security is a complex phenomenon for the past years. Ways of measuring security gives a lee way on its determination. Security measurements are used to answer issues related to decision making. Metrics is used in the depiction of a system’s immunity and resilience. Measurement of security proves difficult because of various reasons. Furthermore, causes of insecurity like terrorists change the

environment frequently. The fact that measurement is an expectation and organization’s objective, security cannot be measured. Different perceptions about gain and loss in human beings make measurement of security complicated. Security requirements cannot be tested since they vary from individual to individual. Despite this, any exploitation needs to be controlled. Planning for efficient use and critical analysis on causes of misuse must be considered. Most systems developed are evolutionary and designed to institute change. Summary: The system through which a system reacts to change is enough proof to support that measurement of security is difficult. Proctor, E. P. McKibben, D. and Oliva, V. (2008) A Risk Hierarchy for Enterprise and IT Risk Managers. Gartner Inc. The Gartner Guidance offers assistance to enterprise and IT managers to develop appropriate effective risk practices to meet their needs. There is no definite definition for risks that suit all enterprises or organizations. Businesses that create and manage risks are responsible for accountability and risk acceptance. Tools available in IT are effective for risk management processes. The results produced by these tools depend on the framework developed, processes and data structures. The article recommends for concrete definition of risks by enterprises and well defined organizational structure that aligns and eliminates conflicts and overlaps. An overarching framework should be created by the enterprise and ensure that staff members understand risk related responsibilities. Summary: Enterprises should take a proactive approach to risk assessment and management. Radack, S. (2011) Managing Information Security Risk: Organization, Mission and Information System View. ITL BULLETIN FOR MARCH 2011. Radack highlights activities involved in risk management. The

activities involve programming, investing, budgeting, legal action and safety issues. These activities lead to the success of organizations. Adoption of an integrated approach with these activities is essential. Most organizations use state-of-the-art and legal information systems. The companies depend on information systems to realize their mission and business functions. Risk-based decisions assist organizations to balance between benefits gained from operations and use of information systems in risk operations and system errors. Summary: Effective management of information security risks is, therefore, essential. Rainer, B. (2010) Security Metrics and Security Investment Models. International Computer Science Institute, Berkeley, California, USA. Rainer comments that companies spend billions of dollars on information security. Since 2009, expenditure on information security is projected to grow by 14% from $13 billion. This has triggered management of information security. Costs are measured by investment theory that looks at the ratio of cost to benefit. Production function based on the amount of output per unit of input can also be used. Security investment model addresses the relationship formally for information security purposes. Summary: Security metrics are used as a basis on which security model is structured. Security metrics defines inputs, outputs and parameters of models. Solms, B. & Solms, R. (2004) The 10 deadly sins of information security management. Elsevier Ltd. Pp. 372-376. Solms identifies risk in neglect of the ten aspects highlighted in information security governance plan causes flaws in the security plan of an organization. An organization can also use the 10 aspects as a checklist by management. The aspects emphasize the basis of information security for organizations. Summary:

When organizations commit the ten sins, they cannot implement measures of security. Solms, B. (2005) Information security governance: COBIT or ISO 17799 or both? Computers & Security Vol. 24, pp. 99-104. Elsevier Ltd. Two models used in information security governance are COBIT and ISO 17799. The two frameworks are compared depending on model structure and analysis. The two frameworks are complimentary and preferred frameworks for information security governance. Summary: A combination of the models provides synergy beneficial to companies. Stewart, G. (2009) A safety approach to information security communications. Information Security Technical Report 14. Pp. 197-201. Elsevier Ltd. The need for improved understanding of human attitudes to information security risk is paramount. Human attitude influences the interpretation of several models like; mental model, heuristic model and risk compensation concept. Information security communication lacks reliable structures and evidences in comparison to safety communications. Summary: Safety methodologies are used to represent exciting areas of the possibility for information security. Trcek, D. (2009) Security Metrics Foundations for Computer Security. The Computer Journal, Vol. 53 No. 7. Oxford University Press. This article discusses several issues that require metrics in computer information’s security systems can assist in assessment of the best software design. Level of security for an organization, the type of security to be adopted, the measure, and benefits are of importance. The GIT-RM model derived from standards of risk management. According to risk management, analysis of assets and threats are essential. Many risks are related to assets exposed for longer periods leading to exploitation. Through this principle, appropriate control measures

are taken. Two metrics are used in measuring vulnerability; DVE and SIF. Summary: The model can only be implemented in Making Security Measurable and Manageable achieved through two elements. One, through an established enumeration of common concepts, and two encoding and communicating through a coded language. Turpe, S. (2009) What Is the Shape of Your Security Policy? Security as a Classification Problem. Fraunhofer Institute for Secure Information Technology (SIT), Germany. Turpes evaluates security systems in two different ways; mechanism centric evaluation and hacking. The common criteria are mechanism centric evaluation. Evaluation of a system is done on the basis of its security frame and determining its validity. The common criteria approach has one weakness in that it loses focus on the relevant threats and security considerations after their exclusion from the framework. System hacking follows no protocol in security design. The strength of a hacker relies on his or her ability to interact with a target. Through the hacker’s goals, a system is made vulnerable to attack suppose the hacker becomes successful. The difference between the approaches is that though the system can be certified under common criteria, it can be vulnerable to ordinary effective attacks of a hacker. The purpose of security mechanism is to prevent causes from having effects. Summary: The security of a system is determined by permitted cause-effect relationships that aim at security policy. United States Government Accountability Office (GAO) (2010) BEST PRACTICES. DOD Can Achieve Better Outcomes by Standardizing the Way Manufacturing Risks Are Managed. Web: http://www. gao. gov/new. items/d10439. pdf. Accessed on 10th April 2012. This article reviews acquisition of defense

weapon systems proves to be costly. Delays are recorded in the manufacturing processes that cause insecurity crisis. Program transition from development to production transfer risks spontaneously. In the early developments, programs used neither identified nor resolved manufacturing risks. Manufacturing Readiness Levels (MRLs) were developed from various sources including defense, industry and academic resources. MRLs were developed to improve identification and management of management risks. Manufacturing Readiness Levels assist in assessment of risks related to manufacturing of artillery. When MRLs are used in acquisition of weapons, security measures are easily monitored. Summary: The DOD recommends the use of MRL in process control of weapons; assess the importance of tools and the workforce.