Corpuz, Maria and Barnes, Paul H. (2010) ***Integrating information security policy management with corporate risk management for strategic alignment.*** In: Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010), 29 June – 2 July 2010, Orlando, Florida.

Integrating Information Security Policy Management with Corporate Risk Management for Strategic Alignment

Maria Soto Corpuz
ISI, Queensland University of Technology
Brisbane, Queensland/4000, Australia

Paul Barnes
ISI, Queensland University of Technology
Brisbane, Queensland/4000, Australia

Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010):
International Institute of Informatics and Systemics (IIIS)

ABSTRACT

Information security policy defines the governance and implementation strategy for information security in alignment with the corporate risk policy objectives and strategies. Research has established that alignment between corporate concerns may be enhanced when strategies are developed concurrently using the same development process as an integrative relationship is established. Utilizing the corporate risk management framework for security policy management establishes such an integrative relationship between information security and corporate risk management objectives and strategies. There is however limitation in the current literature on presenting a definitive approach that fully integrates security policy management with the corporate risk management framework. This paper presents an approach that adopts a conventional corporate risk management framework for security policy development and management to achieve alignment with the corporate risk policy. A case example is examined to illustrate the alignment achieved in each process step with a security policy structure being consequently derived in the process. It is shown that information security policy management outcomes become both integral drivers and major elements of the corporate-level risk management considerations. Further study should involve assessing the impact of the use of the proposed framework in enhancing alignment as perceived in this paper.

Keywords: Information security, security management, security policy, risk management, risk policy , risk analysis.

1. INTRODUCTION

Information security policy is a major element of an organisation's corporate governance and risk management strategy [1] [2] [3]. It defines information security program goals, assigns responsibilities and sets security control requirements [4] [5] that are continually reassessed and updated [6] based on evolving corporate business and risk management objectives [7] [8] [9].

The acknowledged drivers for information security policy management include the corporate requirements for ICT risk management and governance [10] and regulatory compliance [11], and the need for coordinated and integrated policies for coherent security management [6]. The requirement for a well-defined set of information security policies (alternatively referred to as security policy in this paper) has been recognised to provide clear assurance guidelines for security management [12] **[6]**. The set of information security policies usually consists of a hierarchical set of policies composed of an overarching policy and subordinate policies to address the different levels of control [13]. One representation of a set of security policies may be structured according to the organisational layers of internal controls [14]. Another alternative representation of a set of security policy provides categorization according to scope of objectives [9].

From these considerations, security policies should be developed and assessed in constant alignment with corporate business and risk objectives. An underlying requirement is for the security policy to have a policy structure that may be implemented to address all levels of security control requirement. An alignment approach that facilitates the development and management of security policy and its policy structure to address these issues is required.

Research studies on business planning (BP) and information systems planning (ISP) have presented various integration approaches [15] [16] [17] [18] that may be utilized to address alignment issues across corporate functions. One such approach is the BP-ISP *full integration approach* [17]. Corporate concerns that may benefit from applying the BP-ISP approach include information security and corporate risk management. A brief review of relevant literature however indicates a limitation in information security management methods on the utilisation of this approach from a corporate risk - information security alignment perspective.

This paper proposes to address this limitation by first presenting an overview of strategic alignment concepts and business planning-information systems planning (BP-ISP) integration approaches in Section 2. Section 3 briefly discusses the limitations of current information security management practices in presenting integrative alignment approaches are briefly discussed. Section 4 provides a short discussion on how the principles and concepts of the BP-ISP *full integration approach* can be applied for an alignment of information security policy and corporate risk policy alignment. A step-by-step process for such an alignment approach is presented in Section 5. A case example is provided to illustrate the alignment achieved in each process step with a hierarchical security policy structure being derived in the process. Finally, Section 6 provides a summary and some recommendations for future study.

2. BUSINESS PLANNING AND INFORMATION SYSTEMS PLANNING (BP-ISP) ALIGNMENT CONCEPTS

The need for aligning information system plans with business plans are well founded in research. Prescriptive [15] [17] and empirical studies [19] [20] [21] have established the need for aligning information systems planning with business planning in ensuring business objectives are met and effective information technology investments are made. Research findings have also confirmed the existence of evolutionary stages of integrative alignment through four types of business planning-information systems (BP-ISP) integration [22]: from the first stage of *administrative integration*, to the second stage of *sequential integration* [15] to the third stage, *reciprocal integration* [16] and finally the last stage of *full integration* [17] [23].

Administrative integration equates to separate planning between BP and ISP whereas sequential planning allows for one-way linked planning in which BP provides direction for ISP [15]. Two-way linked planning indicates a reciprocal integration relationship between BP and ISP wherein ISP provides both support and direction to BP [16]. In the last stage of full integrated planning [23], an emphasis that information systems planning be integrated within business planning to achieve alignment is critical. This involves developing both the BP and ISP strategies at the same time using the same planning process and establishing an integrative relationship between BP and ISP. The presence of the alignment mechanisms of content, timing and personnel inherent in a full integrative relationship [24] provides benefits to organisations as a result of improved coordination of information systems plans with business plans [19].

In measuring the nature and degree of alignment, strategic alignment models have been developed [25] and related alignment components have been proposed [26] to provide support for practical applications. Major critical success factors have also been defined [27] to assist organisations in understanding the requirements for alignment. In assessing the stage of alignment maturity between business and Information Technology, a five-level maturity model based on the capability maturity model developed for software engineering [28] is also presented.

These studies provide important concepts and tools in establishing and assessing BP-ISP alignment. Together they represent a comprehensive reference base for considering practical solutions to alignment issues across corporate concerns. Such corporate concerns that may benefit from applying these alignment concepts include information security and corporate risk management. The BP-ISP theory that is of particular importance and is the focus of this paper is the utilisation of the concept of the full integration approach from an information security-corporate risk alignment perspective.

The following section presents a brief review of available literature on information security management principles and practices and their adequacy to support or provide full integrative alignment approaches for security policy development within a corporate risk management context.

3. LIMITATIONS OF INFORMATION SECURITY MANAGEMENT PRACTICES ON ALIGNMENT APPROACHES

Organisations refer to information security management systems (ISMS) standards and good practice guidelines for guidance in implementing information management systems. Among the most widely used information security management standards are the ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [7] (ISO/IEC:27001, 2005), the NIST Generally Accepted Principles and Practices for Securing Information Technology Systems Special Publication 800-14 [9] (Swanson and Guttman, 1996), the IT Infrastructure Library Best Practice for Security Management [29] (Cazemier, Overbeek and Peters, 1999) and the COBIT 4.0 Control Objectives Management Guidelines Maturity Models [8] (ITGI:COBIT 4.0, 2005). The common perspective for security policy development prescribed by these standards is the requirement for security policies to be consistently aligned with corporate risk objectives. These standards and best practice guidelines however only provide suggestive definitions and characteristics of information security policies. The standards don't provide the definition of a process approach for policy development and alignment approaches [7] [9] [29] [8] and are generally considered checklists of security controls defined in generic terms [30] (Hone and Eloff, 2002) [31] (Siponen, 2002).

Several theoretical approaches to security policy development based on the ISMS standards and practice guidelines have been developed. One theory proposes the alignment of high-level information security policy formulation [32] [33] and the overall ISMS [34] as part of the IT strategic planning process: usually utilising the ISMS-based process concept of the Plan-do-check (PDCA) cycle [35]. Another theory [2] proposes the adoption of the principles of the corporate risk management framework [36] [37] [38] for information security management. The limitation of these proposals is the lack of a defined approach to support the required activity for ensuring security policies are aligned with corporate risk management objectives.

Other proposed security policy development approaches [39] [40] [41] provide varying levels of detail and process chronology involving the activities of policy development, implementation and review. None of these policy development proposals however provides for a full integrative approach for aligning security policy development within a wider corporate risk management context.

These policy development theories and approaches represent either sequential integration which allows for one-way linked planning with corporate risk objectives driving the development of the security policy or reciprocal integration indicating a two-way linked planning relationship between security policy and corporate risk policy. Utilising these existing policy development frameworks do not provide for full integrative alignment between security policy development and corporate risk management.

4. INTEGRATING INFORMATION SECURITY POLICY MANAGEMENT WITH CORPORATE RISK MANAGEMENT: THE CRP-ISP APPROACH

A corporate risk policy defines the context for the set of objectives, roles, responsibilities and scope for an overall risk management process [37]. An organisation generally operates within the context of a corporate risk policy best formulated at the corporate level with input from business units and approved by the board [42].

Risk management standards offer several approach variations to the risk management process. A conventional risk management framework process usually consists of four parts [36] [37] [38]:

1: Risk assessment process (derived from Risk Management Policy)
2: Risk treatment process (facilitating the development and implementation of the Risk Mitigation Plans)
3: Risk communication process (facilitating awareness of the Risk Communication Plan)
4: Risk review and monitoring process (assuring accuracy of the overall risk assessment)

The security strategy should align with corporate risk management strategies and objectives [7] and as such may be considered in a similar strategic management perspective as the corporate risk policy. In this context, the principle of BSP-IS integration may be adopted for corporate risk policy (BP) and security policy (ISP). One way of establishing this BSP-ISP integration is by utilizing the corporate risk management framework for security policy management. In the next section, an alignment approach utilising the full integration planning concept for security policy development and management with corporate risk management is proposed.

5. THE INFORMATION SECURITY POLICY (ISP) - CORPORATE RISK POLICY (CRP) APPROACH

At an enterprise level, the process of corporate risk management is concerned with weighing policy alternatives in selecting appropriate risk assessment, prevention and control options in consultation with stakeholders [43]. Information security policy as a strategic approach to implementing information security is part of these risk policy alternatives that require corporate consideration.

By adopting a corporate risk management framework the various security policy-related activities and outputs are fully integrated with related elements in the corporate risk activities. Alignment is achieved in four successive ways. First, by aligning intent and scope of both policies; second by coordinating policy roles; third by synchronising processes to implement the policies activities; and lastly by maintaining a reciprocal feedback mechanism. This integrative relationship is diagrammatically presented in Fig. 1.

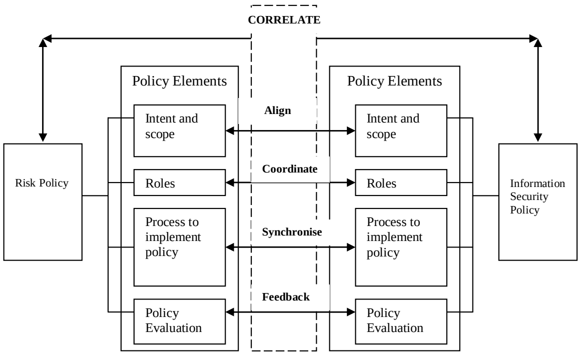


Fig.1: Security and Risk Policies Alignment

In the following paragraphs, the four steps of the corporate risk management framework are adapted in defining the process activities for security policy management. Each process step contains subordinate activities represented in a process diagram to show alignment relationships. Double-edged arrows signify integrative relationship between activities with the triangle arrow pointing to related output. To demonstrate the practicability of the approach and illustrate the alignment achieved in each step, a case example is taken through the process. The case example involves a scenario where a change in the organisational risk management policy requires a modification in the assignment of roles in incident and disaster management.

Step 1: Security Risk Assessment (Develop information security policy) - The security risk assessment step integrates with the environmental scanning, risk analysis and risk evaluation activities of the corporate risk management framework and is presented in Fig 2. Input information for this step includes the corporate risk policy and risk register. The main objective of the security risk assessment activity is to develop the information security policy and its policy structure.

For the case example, the change in corporate risk policy for role assignment might involve information security risk management and implementation being coordinated on the corporate risk management level instead of being delegated to the IT team alone.

Step1.1: Perform environmental scanning –the context of the security risk management process is established in this step. Information management and technology assets are classified under the categories of *people, process* and *technology*. This is because IT is considered as an operational risk that may result in inadequacies or failure in any of these categories [44]. SWOT (strengths-weaknesses-opportunities-threats) analysis [45], a tool used in strategic management and business policy development, can be employed in environmental scanning for developing the information security policy.

Corporate Risk Management	**Information Security Policy Management**
Risk Assessment Process **(Risk Management Policy)** - Intent and scope - Roles statement - Process to implement. 1. Develop risk policy 2. Develop risk registers 3. Develop risk controls register - Evaluation of compliance	**Step 1** Activities 1.1 Perform environmental scanning 1.2 Perform security risk analysis 1.3 Perform security risk evaluation
	Output: **Information Security Policy** - Intent and scope - Roles statement - Process to implement 1. Develop information security policy 2. Develop security risk and threat registers 3. Develop security controls register - Evaluation of compliance

Fig. 2: Security Risk Assessment Process

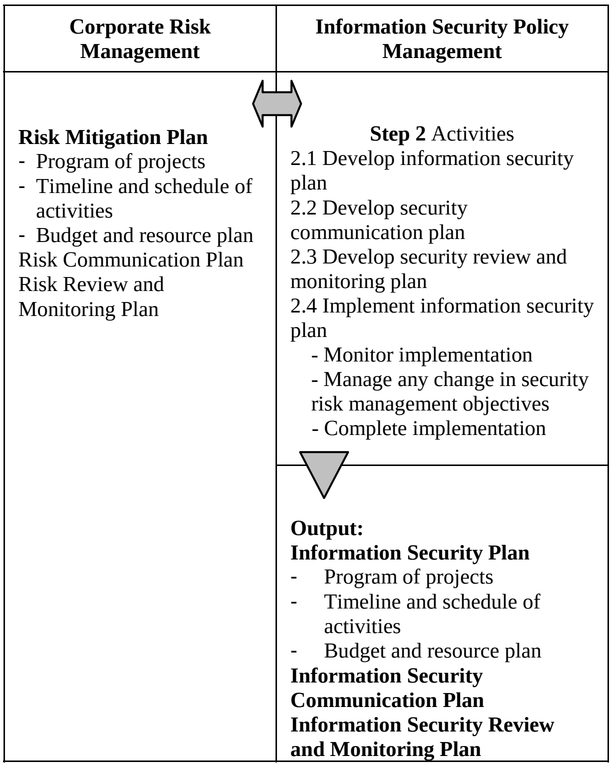
The information security policy addresses the risk mitigation requirements of the *people* asset category. It represents the top layer of the security policy hierarchy and serves as the basis for deriving the security procedural policies (developed to protect the process assets) in the second layer and the system technology policies (designed to protect technology assets) in the bottom layer. For existing security policies, this step provides a review process for alignment between the security policy and the evolving corporate risk objectives.

Step 1.2: Perform security risk analysis – A security risk and threat register based on the categorised assets (people, process and technology) is the main output of this activity. In deriving the business impact for each risk, the qualitative and quantitative techniques used in corporate risk management can be adopted. These techniques can include Bayesian and Monte Carlo analysis techniques [46].

Step 1.3: Perform security risk evaluation – In this step, the required security subordinate policies and controls related to the *process* and *technology* assets are identified. It is to be noted that this approach in developing security controls ensure that security implementation is policy-driven and not technology-driven. The top-layer information security policy provides the direction for the development of the procedural security policies that address the process asset-related risks in the middle layer of the policy hierarchy. From the security procedural policies are derived the security systems technology policies in the bottom layer that provide system-specific controls to mitigate the technology-related risks and vulnerabilities. Useful techniques for evaluating risks involve group decision-making employing the Delphi technique [47] and deriving decision trees to arrive at resolutions by quantifying risks [48] [49].

In the case example, any change in the assignment of roles in incident and disaster management contained in the corporate risk policy is a direct input to the updating of the information security policy on security incident management responsibilities. The alignment of roles and responsibilities between corporate risk policy and information security policy at the top layer of the security policy hierarchy is achieved. Issues in duplication or gaps in role assignment for disaster and incident risk mitigation are addressed.

Step 2: Security Risk Treatment (Implement Information Security Policy) – Inputs from corporate risk activity consist of the risk mitigation plan, the risk communication plan and the risk review and monitoring plan. The objective of the security risk treatment activity, shown in Fig. 3, is to implement the information security policy through the information security plan. In developing the information security plan which details the implementation strategy for the information security policy, useful strategic management and business policy development tools include the SWOT analysis [45], and the process life cycle Plan-Do-Check-Act (PDCA) method [35].



Corporate Risk Management	**Information Security Policy Management**
Risk Mitigation Plan - Program of projects - Timeline and schedule of activities - Budget and resource plan Risk Communication Plan Risk Review and Monitoring Plan	**Step 2** Activities 2.1 Develop information security plan 2.2 Develop security communication plan 2.3 Develop security review and monitoring plan 2.4 Implement information security plan - Monitor implementation - Manage any change in security risk management objectives - Complete implementation
	Output: **Information Security Plan** - Program of projects - Timeline and schedule of activities - Budget and resource plan **Information Security Communication Plan** **Information Security Review and Monitoring Plan**

Fig. 3: Security Risk Treatment Process

Step 2.1: Develop information security plan - In developing the information security plan, the mitigating controls contained in the security control register are finalised and drawn into a program set of initiatives or projects. The information security plan provides the implementation approach for new security risk treatments, additional controls or modifications to current security controls. Major input for this step is the risk mitigation plan with direct reference to the program of projects defined in the corporate risk mitigation plan. This referencing provides the synchronisation between the development activities of the corporate risk mitigation plan and that of the information security plan. A major element of the information security plan is the implementation plan for the information security policy and its subordinate policy structure (developed in Step 1) and the interconnected security controls.

Referring to the case example, the change in role assignment in the information security policy (people asset) will be reflected on the procedural security policy and implementation for disaster management (process asset) and incident reporting. In conjunction, this is followed by the modification of the security system policies (technology asset) for the deployment of a virtual private network or firewall system to facilitate the access requirements based on the new assignment of roles. This interconnected nature of development and modification of the security policies in the hierarchy derived for the case example to facilitate business impact may be similar to the diagram shown in Fig. 4. Diagram arrows indicate the influential flow that may be affected by any change in the strategic policy element (people aspect) on the subordinate policies (process and technology aspects).

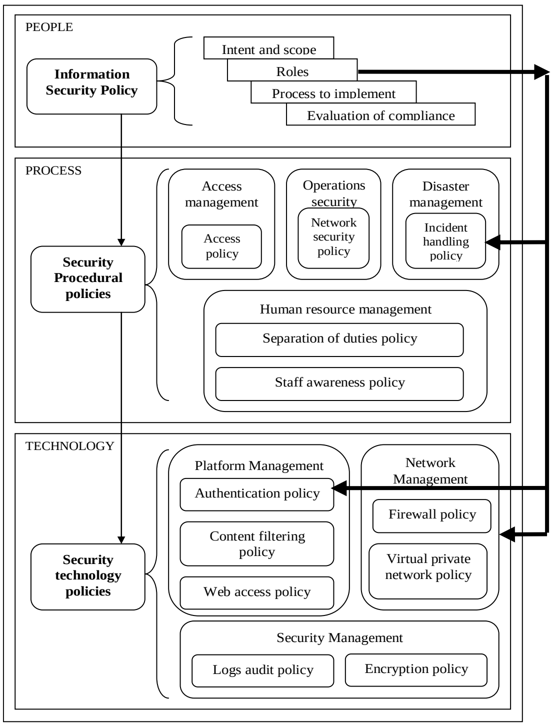


Fig. 4: Example of Information Security Policies Hierarchy Structure

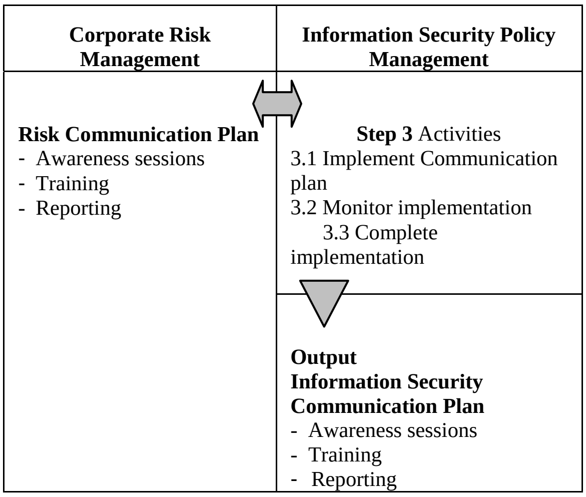
Step 2.2: Develop security communication plan - The security communication plan provides the approach for information dissemination with the objective to gain consensus, support and commitment of resources for the information security policy and plan across the corporate management environment. Communication includes regular reporting to stakeholders both internal and external to the organisation.

Step 2.3: Develop security review and monitoring plan - The security review and monitoring plan details the methods, procedures and monitoring timeline to assess and review the effectiveness of the security policies and controls. Review and assessment provides a corporate assurance in the adequacy of the policy implementation to meet security risk mitigation requirements.

Step 2.4: Implement Information Security Plan - The deliverable output of this activity is the completion of the implementation of the program set of projects detailed in the information security plan. This entails the propagation of the security procedures and security technologies required by the information security policy.

When applied to the case example where roles have been modified, Step 2 ensures that the information security management and program of activities are defined based on the modified roles statements contained in both the corporate risk policy and the information security policy. Any modification in the corporate risk mitigation plan as a result of the role assignment change is reflected in the information security plan consistently in a timely manner and alignment between corporate risk implementation of activities and information security policy plan is ensured.

Step 3: Security Risk Acceptance and Communication (Communicate Information Security Policy) - The objective of this step is to communicate the information security policy and the information security plan. The relevant input is the corporate risk communication plan. Correlating the communication plans of corporate risk management with information security policy management as shown in Fig. 5 provides consistent and accurate information regarding risk mitigation activities. The exchange of information and reporting also helps identify any gap or duplication in activities.



Corporate Risk Management	Information Security Policy Management
Risk Communication Plan - Awareness sessions - Training - Reporting	**Step 3** Activities 3.1 Implement Communication plan 3.2 Monitor implementation 3.3 Complete implementation
	Output **Information Security Communication Plan** - Awareness sessions - Training - Reporting

Fig. 5: Security Risk Communication Process

Step 3.1: Implement communication plan - The information distribution approach detailed in the security communication plan is undertaken in direct relationship with the corporate risk communication plan. Groups that may be involved in the communications plan for both information security and corporate risk management are able to coordinate consistently and in alignment eliminating any duplication in effort and gaps in the implementation.

Step 3.2: Monitor implementation - regular content review and monitoring of the reporting and publishing of information is undertaken to provide updated and accurate information in all phases of the information security policy management. Arising out of this monitoring activity will be any adjustments that may need to be undertaken to ensure that accurate and complete information is provided.

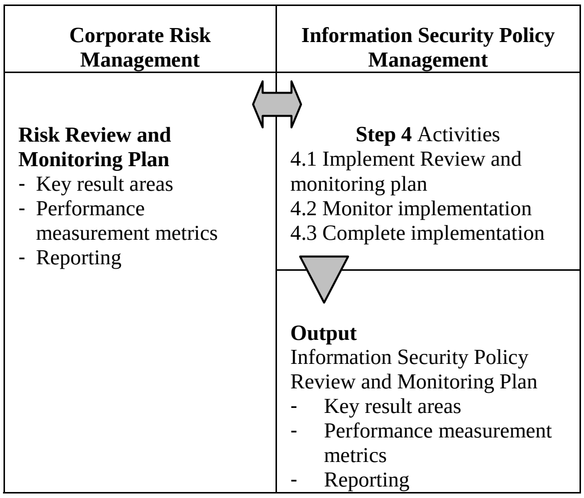
Step 3.3: Complete implementation and sustain communication - Communication of the information security policy is an activity that is maintained to provide update on what ever change is made in the security policy. An essential part of the communication strategy is the gathering and consolidation of feedback emanating from both corporate risk management and information security as input information for policy revision and improvement in implementation.

In the case example where roles have been modified, this step in the security policy management process ensures that the communication and acceptance of both the corporate risk management program of activities and the information security policy and plan of activities are consistent and aligned. Role assignments for information dissemination are clarified and consistently maintained. There is a single point of information in communicating information and gaps or inconsistencies are minimised if not eliminated. Alignment between corporate risk communication and information security policy communication is ensured.

Step 4: Security Risk Review and Monitoring (Review and monitor Information Security Policy) - In developing the approach for policy review and assessment, the corporate risk review and monitoring plan provides important input details regarding performance measurement methods and metrics to meet corporate risk management objectives.

The results from monitoring and review in this step will indicate the efficiency and effectiveness of the security policies in addressing the security risk mitigation objectives. Fig. 6 presents the related inputs, outputs and processes.

Step 4.1: Implement review and monitoring plan - the security policy is continually updated to align with the evolving corporate risk management objectives. In conducting the monitoring and review activity as prescribed in this step, feedback information from the corporate risk assessment exercise provides critical input that is often overlooked. Target key result areas between corporate risks and information security risks are maintained in alignment. Review and assessment may be undertaken utilising the Balanced Scorecard approach [50] used in strategic management planning.



Corporate Risk Management	Information Security Policy Management
Risk Review and Monitoring Plan - Key result areas - Performance measurement metrics - Reporting	**Step 4** Activities 4.1 Implement Review and monitoring plan 4.2 Monitor implementation 4.3 Complete implementation
	Output Information Security Policy Review and Monitoring Plan - Key result areas - Performance measurement metrics - Reporting

Fig. 6. Security Review and Monitoring Process

Step 4.2: Monitor implementation – monitoring is conducted during the review and assessment activities to foster the sharing of resultant outputs between the corporate risk review and the security policy review. The results can be shared, consolidated and summarised to provide a better strategic view of the overall risk mitigation activities.

Step 4.3: Complete implementation – completing implementation of the review process for each policy development cycle provides the basis for the next round of policy development activities. Coordinating and correlating lessons learned for the security policy review process with that of the corporate risk policy review activities facilitates meeting the organisational risk mitigation objectives. In reviewing next steps in security strategy planning, real options approach to security investment portfolios may be considered [51].

For the case example, Step 4 ensures that the review and assessment of corporate risk management program of activities are defined based on the modified roles statements contained in both the corporate risk policy and the information security policy. Alignment between assessment and review activities between corporate risk and information security policy plan is ensured providing a more meaningful analysis of review findings.

6. Conclusion

Utilising current policy frameworks that lack integrative alignment approaches for security policy development can result in the development of weak security control procedures representative of an unstructured checklist of security controls. Resultant security policies are developed without the understanding of their relationship to corporate risk objectives to substantiate the requirement for functionality and value of such security policies and controls. Security policies are rendered as IT-focused initiatives with little reference to wider corporate risk objectives. Ultimately, as observed in previous studies [27], corporate management considers matters relating to information security to be mainly technical issues under the domain of information technology and commonly delegated to the Information Technology department rather than as a corporate governance concern.

The adoption of a common development and management framework for security policy and risk policy can result in an alignment approach that establishes an integrative relationship between these two corporate concerns. Through the use of a case example, it is clear that information security policy management outcomes become both integral drivers and major elements of the corporate risk policy, thus facilitating the development of the security policy structure. Alignment is maintained as processes are correlated and standardised every step of the way.

A key advantage of this approach over existing security policy development frameworks is that the alignment between corporate risk issues and information security risk management through security policies is central. A meaningful security policy structure connecting corporate-level security requirements with subordinate security procedures and technologies is created and provides better understanding of the dependency aspects of the people, process and technology categories of organisational assets. This approach ensures a policy-driven implementation of the information security.

As the scope of this paper is limited to the development of the conceptual approach for security policy alignment, further study should involve assessing the impact of the use of the proposed framework in enhancing alignment, possibly through the use of the Strategic Alignment Model (SAM). Another opportunity for future research may also involve developing a security policy assessment model to gauge the efficiency and effectiveness of the security policy set derived from the use of the proposed conceptual approach.

In the areas of strategic planning and corporate governance, further studies may include exploring the adoption of BP-ISP theories for developing alternative full-integration perspectives on developing security policies within the strategic planning process exemplified in the ISP-CRP approach proposed in this paper.

7. References

[1] B. von Solms and R. von Solms, The 10 deadly sins of information security management, **Computers and Security**, 2004, Vol. 23, pp. 371-376.

[2] E. Humphreys, “Information Security Management Standards: Compliance, governance and risk management”, **Information Security Technical Report**, Vol. 13, 2008, pp.247-255.

[3] Institute of Chartered Accountants ICA, **Internal Control: Guidance for Directors on the Combined Code**. Institute of Chartered Accountants (England and Wales), 1999.

[4] W. Caelli, **Information Security Handbook**. Macmillan Publishers Ltd, 1991.

[5] V. LeVeque, **Information Security A Strategic Approach**, John Wiley and Sons Ltd, 2006.

[6] Organization for Economic Co-operation and Development OECD, **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**, OECD , 2002.

[7] International Standards Organization ISO/IEC, **ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements**, International Standards Organization, 2005.

[8] IT Governance Institute ITGI, COBIT 4.0 **Control Objectives Management Guidelines Maturity Models**, ITGI, 2005.

[9] M. Swanson and B. Guttman, **NIST Generally Accepted Principles and Practices for Securing Information Technology Systems Special Publication 800-14,** National Institute of Standards and Technology, 1996.

[10] Standards Australia, **Australian Standard. AS 8015-2005: Corporate Governance of Information and Communication Technology**, Standards Australia, 2005.

[11] Organization for Economic Co-operation and Development OECD, **Working Party on Information Security and Privacy. Summary of Responses to the Survey on the Implementation of the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**, OECD, 2004.

[12] Information Systems Security Association (ISSA). **Generally Accepted Information Security Principles** *(GAISP V3.0)*, 2004, ISSA.

[13] R. Baskerville and M. Siponen, “An Information Security Meta-Policy for Emergent Organizations”, **Logistics Information Management**, Vol. 15 No.5/6, 2002, pp. 337-346

[14] M.D. Abrams and D. Bailey, “Abstraction and Refinement of Layered Security Policy”, **M.D. Abrams, S. Jajodia and H.J. Podell (Eds), Information Security - An Integrated Collection of Essays,** IEEE Computer Society Press, New York, 1995.

[15] W. R. King, “Strategic Planning for Management Innformation Systems”, **MIS Quarterly**, Vol 2 (1), 1978, pp. 27-37.

[16] W. R. King and R. W. Zmud, “Managing Information Systems: Policy Planning, Strategic Planning and Operational Planning, **Proceedings of the Second International Conference on Information Systems**, Boston, 1981.

[17] N. Goldsmith, “Linking IT Planning to Business Strategy”, **Long Range Planning**, Vol. 24, No. 6, 1991, pp. 67-77.

[18] A.L. Lederer and V.Gardiner, “Strategic information systems planning: The Method/1 approach. **Information Systems Management**, Vol. 9(3), 1992, pp. 13-20.

[19] A. L. Lederer and A. L. Mendelow, “Coordination of Information Systems Plans with Business Plans”, **Journal of Management Information Systems**, Vol. 6. No. 2, 1989.

[20] T. S.H. Teo and W. R. King, “Assessing the impact of integrating business planning and IS planning”, **Information and Management**, Vol. 30, 1996, pp. 309-321.

[21] Y.E. Chan, R. Sabherwal and J.B. Thatcher, “Antecedents and Outcomes of Strategic IS Alignment: An Empirical Investigation”, **IEEE Transactions on Engineering Management**, Vol. 53, No. 1, 2006, pp.26-47.

[22] T. S.H. Teo and W. R. King, "Integration between Business Planning and Information Systems Planning: An evolutionary-Contingency Perspective", **Journal of Management Information Systems**, Vol. 14, No. 1, 1997, pp. 185-214.

[23] W. R. Synott, **The Information Weapon: Winning Customers and Markets with Technology**, New York, John Wiley, 1987.

[24] J.K. Shank, E. G. Niblock and W. T. Sandalls Jr., "Balance Creativity and Practicality in formal planning", **Harvard Business Review**, 51 (1), January/February 1973, pp. 87-95.

[25] J. Henderson and N. Venkatraman, "Strategic Alignment: A Model for Organisational transformation through information Technology", **Transforming Organizations** (T. Kochan and M. Unsen, eds) Oxford University Press, NY, 1992.

[26] J. Luftman and T. Brier, "Achieving and Sustaining Business-IT Alignment", **California Management Review**, Vol. 42, No. 1, 1996, pp. 109-121.

[27] T S.H. Teo and J. S.K. Ang, "Critical Success Factors in the Alignment of IS Plans with Business Plans", **International Journal of Information Management**, Vol 19, 1999, pp. 173-185.

[28] J. Luftman, "Assessing Business-IT Alignment Maturity", **Communications of the Association for Information Systems**, Vol. 4 No. 14, 2000.

[29] J. Cazemier, P. Overbeek, L. Peters, **IT Infrastructure Library Best Practice for Security Management**. Office of Government Commerce, Crown Copyright, 1999.

[30] K. Hone and J.H.P. Eloff, "Information Security Policy – What Do International Information Security Standards Say", **Computers and Security**, Vol. 21, Issue 5, 2002, pp. 402-409.

[31] M. Siponen, Towards Maturity of Information Security Maturity Criteria: Six Lessons Learned from Software Maturity Criteria", **Information Management and Computer Security Vol. 10 (5)**, 2002, pp. 210-224.

[32] N. F. Doherty and H. Fulford, "Aligning the Information Security Policy with the Strategic Information Systems Plan", **Computers and Security** Vol. 25, 2006, pp. 55-63.

[33] V. LeVeque, **Information Security A Strategic Approach**, John Wiley and Sons Ltd, 2006.

[34] J.C. Sipior and B.T. Ward, "A Framework for Information Security Management Based on Guiding Standards: A United States Perspective", **Issues in Informaing Science and Information Technology**, Vo. 5, 2008, pp.51-60.

[35] E. W. Deming, **Improvement of Quality**. MIT Press, 1986.

[36] Standards Australia/Standards New Zealand, **Australia New Zealand Standard AS/NZS ISO 31000:2009 Risk Management- Principles and Guidelines**, Standards Australia/Standards New Zealand, 2009.

[37] The Institute of Risk Management IRM, The Association of Insurance and Risk Managers and The National Forum for Risk Management in the Public Sector, **A Risk Management Standard**, 2002, AIRMIC, ALARM, IRM.

[38] International Risk (IRGC), "**Critical Infrastructures**", Governance Council, IRGC, 2005.

[39] M.E. Kabay, **The NCSA Guide to Enterprise Security**, McGraw-Hill, New Yor, 1996.

[40] J. Rees, S. Bandyopadhyay and E. Spafford, PFIRES: A Policy Framework for Information Security. **Communications of the ACM,** Vol. 45. No. 7, 2003, pp. 101-106.

[41] N.L. Flynn, **The Epolicy Handbook: Designing and Implementing Effective E-mail, Internet and Soaftware Policies**, American Management Association, New York, 2001.

[42] J. Lam, **Enterprise Risk Management: From Incentives to Controls**, John Wiley and Sons Inc. USA, 2003.

[43] European Network and Information Security Agency ENISA (2007), **Glossary of Risk Management**. Available: http://www.enisa.europa.eu/rmra/glossary.html

[44] C. L. Culp, **The Risk Management Process: Business Strategy and Tactics,** John Wiley and Sons Inc. USA, 2001.

[45] M. Porter, **The Competitive Advantage**, The Free Press, New York, 1985.

[46] G. Koller, **Risk Assessment and Decision Making in Business and Industry: A Practical Guide**, CRC Press LL, 1999.

[47] T. Merna, **Risk Management at Corporate, Strategic Business and Project Level. MPhil Thesis**, 2002, UMIST, Manchester.

[48] M. Sahinoglu, "**Security Meter: A Practical Decision Tree Model to Quantify Risk"**, IEEE Security Privacy, Vol 3, pp. 18-24, 2005.

[49] M. Sahinoglu, **Trustworthy Computing: Analytical and Quantitative Engineering Evaluation**, John Wiley and Sons Inc, 2007.

[50] R. Kaplan and D. Norton, **The Balanced Scorecard: Translating Strategy into Action**. Harvard Business School Press, 1996.

[51] P. Petratos, "Real Option Applications to Information Security", **Communications and Strategies**, Vol. No. 70, 2nd Quarter, 2008, pp.15-25.

[52] D. F. Lohmeyer, J. McCrory and S. Pogreb, **Managing Information Security**, McKinsey Quarterly Special Edition, 2002, pp. 12-15.