Chapter XI
Managing IT Security Relationships within Enterprise Control Frameworks

Brian Cusack
AUT University, New Zealand

ABSTRACT

Security is a subprocess that affects all processes within an organization structure. The control frameworks of CobiT and ITIL provide a mapping of organizational roles from the capital interest at the highest level, through to the implementation level in an enterprise system. Both control frameworks provide varying capability for control at different levels in an organization and leave the problem of making control functional to the managerial layer. In this chapter the security process is mapped from two control frameworks at the strategic layer and the issue of effective management tactics discussed from the theoretical structures within the problem area. No attempt is made to transgress theory into practice.

INTRODUCTION

Security is a subprocess that impacts with different degrees on all processes within an organization structure. A security strategy is often described as defense in depth and conveys a metaphorical image of structured rigidity in the face of assessed risks. An effective business security strategy has elements of defense in depth theory but also other philosophical insights that include flexibility and rapid response. In the CobiT control framework security is defined as "Ensure Systems Security" (Delivery & Support (DS 5)) (ITGI, 2007a). The goal of security is to ensure systems security "to safe guard information against unauthorized use, disclosure or modification, damage or loss." In the ITIL control framework security is described as "Security Management" and has three distinct roles associated with the management (van Bon, 2004b). Its objective is to protect "the value of information in terms of confidentiality, integrity and availability". Both of these control frame-

works acknowledge defense in depth and in the ITIL security management guidelines an additional discussion of flexibility is found: "While it is important to protect information assets with traditional stronghold / fortress approaches it has become equally important to have a skirmish capability when it comes to skirmish events. … The organization must have the capability to rapidly put resources on the ground where trouble is before that trouble has a chance to spiral out of control" (van Bon, 2004a, pp. 181-183).

Protecting information strategically is consequently more than establishing defense in depth and related to strategic positioning and repositioning. Positioning occurs within the enterprise subsystem and in relation to the enterprise system as a whole. In the control frameworks of CobiT and ITIL careful specification of the security process is made and elaboration of the interrelation of the process to others. In CobiT the security process (defined as DS 5; see ITGI, 2007a; 2007b; 2007c) has three input processes, direct input to nine output processes, and influence on "other IT processes". Similarly in the ITIL control framework security management has relationships with eleven other management processes. The ITIL framework is more explicit as to the nature of the relationship and the consequence of the security process than is CobiT and the CobiT management guidelines. The importance of the security process is emphasized in both control frameworks in relation to the outcomes for the enterprise system. It would appear then that an understanding of process management for successful process outputs is more than the systematic control of one process and as it is acknowledged in the literature, security management has an enterprise wide (across all processes) mandate (Siponen, 2000). It is contended that the current elaboration of the enterprise wide management is lacking in specification for variation in process relationships, variation in impacts, and guidelines for flexible positioning. Analysis and clarification of variation can add knowledge to what is already advocated in the control literature (ITGI, 2005a; Straub & Welke, 1998).

At the strategic level sufficient detail is provided for enterprise planning and goal and objective setting for protecting information. However at the tactical (managerial) level the specification of the relationships between different processes is inadequate to adequately plan for effective defense of the information system (Von Solms & Von Solms, 2005). For example in the CobiT framework, of the three inputs to the security process (PO9, AI6, DS1) (van Bon, 2004a) two are inward looking (within process) and one considerate of the external environment. Effective planning for flexible defenses at the tactical level would expect both PO9 and AI6 would also be considerate of both the internal and external process environments. PO9 adequately considers the external risk context by stating the goal to be, "Assess risks to support management decisions … and responding to threats by increasing objectivity and identifying important decision factors" (van Bon, 2007). However, it would be expected that AI6 "Manage Changes" also had an outward consideration to define changing external factors and relationship weightings as well as the internal process concerns. The many-to-many relationship of security process to other processes has more variation and complexity than a good manager could be expected to control. The following sections define the problem area in greater detail and then consider possible scenarios where a manager may gain sufficient control that information protection may be assured.

CONTROL FRAMEWORKS

Control frameworks attempt to provide a one-stop-shop for business and systems managers. The differences between different control frameworks (for example, CobiT, ITIL, PRINCE2, PMBOK, and so on) are found in the evolutionary (historical) development, proprietry interests and also the