Information Security Governance:

Motivations, Benefits and Outcomes

By John P. Pironti, CISA, CISM, CISSP, ISSAP, ISSMP

As boards of directors and corporate executives wrestle with regulatory and legal requirements and the need to maintain the integrity and continuity of business processes, the concept of information security governance takes on added meaning and importance.

Governance, as defined by the IT Governance Institute (ITGI), is the “set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise’s resources are used responsibly.”

Since information is a vital resource for organizations, it is important that information security activities be integrated into the corporate governance structure. To help organizations understand information security as a component of corporate governance, ITGI first published *Information Security Governance: Guidance for Boards of Directors and Executive Management* in 2002. This landmark document provided a first definition of information security governance and helped leading organizations align information security with business strategy, manage risk and optimize information security investments. ITGI released a second and updated edition of this guide in 2006 to reflect current thinking and trends in information security governance. This guide for executives will be followed by an implementation guide that will be available later in 2006.

As part of the project effort to collect constituent information about the nature and status of information security governance within organizations, a web-based survey was conducted. One hundred forty-eight Certified Information Security Managers (CISMs) representing 41 countries participated in this survey, providing insight into the factors that motivate organizations to implement an information security governance initiative, what benefits are expected, and what outcomes are achieved.

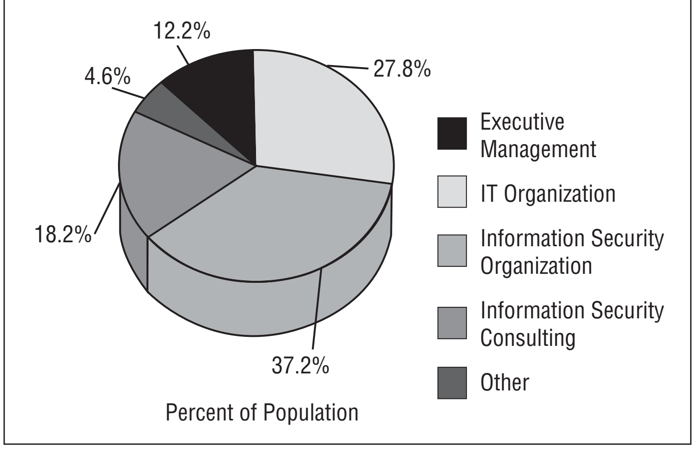
Participants in the survey, as depicted in **figure 1**, included executive management (12.2 percent), IT executives and management (27.8 percent), information security executives and management (37.2 percent) and information security consultants (18.2 percent). While executives and management were primarily drawn from financial services (20.9 percent), consulting (29.1 percent), and local and federal government (12.9 percent), industries such as retail, manufacturing, utilities and health care were represented. The greatest majority of survey takers were from North America (54.1 percent). Other regions included Europe and Africa (25.3 percent), and Asia and the Near East (13.7 percent). A small number of survey respondents were recorded from South and Central America and Oceania. Most of the survey participants were from organizations with fewer than 1,000 employees (43.9 percent) and almost one third (27.7 percent) represented organizations with more than 10,000 employees.

Factors That Influence Security Governance Project Initiatives

While many reasons justify the effort and expense of an information security governance program, the most important motivators, as identified by survey participants, were a concern for legal liability, protection of the organization’s reputation and regulatory compliance. The mean value for each of these categories was four or more on a five-point scale. The least important among all survey participants were process improvement, optimization of the use of security resources, and reliance on interactions with trading partners and suppliers. While the factors considered most significant across all survey participants were consistent, certain differences in priorities were detected among different groups. Executives, following the general trend, selected legal liability and the protection of the organization’s reputation as the most important reasons for initiating an information security governance program, but selected managing risk to an acceptable level as the third most important factor. IT management identified four factors as being almost equally important. These included legal liability and regulatory compliance but also assurance to the board for policy compliance and managing risk to an acceptable level.

As part of the survey, participants were asked the current state of their information security governance initiatives. Six response categories, ranging from completed or in progress to being discussed or not considered, were provided. The majority of survey participants (72 percent) said an information security

Figure 1—Security Governance Survey Participant Roles



governance initiative was completed, in progress or planned. Fifteen percent indicated that no action had been taken or was planned. Of those who had completed an information security governance project or were progressing toward information security governance, the most significant factors were to protect the organization's reputation, act out of concern for legal liability and provide assurance to the board of policy compliance.

Information Security Governance Outcomes

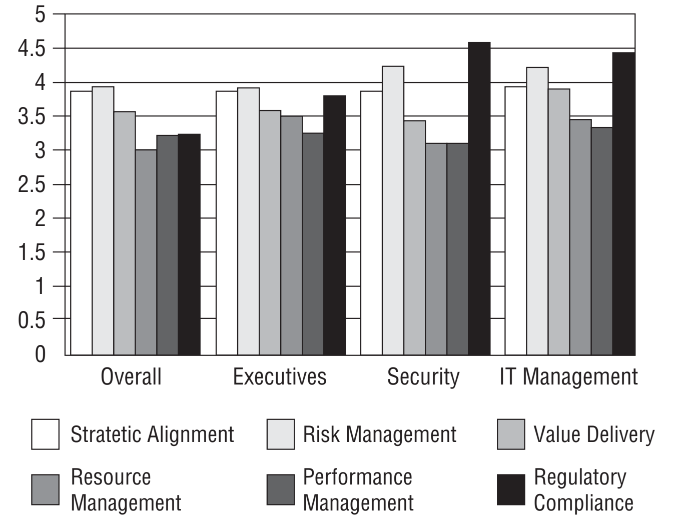
Five basic outcomes can be expected to result from developing an effective governance approach to information security:

- Strategic alignment of security with business strategy and organizational objectives
- Reduction of risk and potential business impacts to an acceptable level
- Value delivery through the optimization of security investments with organizational objectives
  - Efficient utilization of security investments supporting organization objectives
  - Performance measurement and monitoring to ensure that objectives are met

Due to the importance of regulatory compliance in today's business environment, compliance can be added as an emerging information security governance outcome.

The mean responses from survey participants on a five-point scale do not vary significantly among the outcomes. When all survey responses are examined, the three most important information security governance outcomes were risk management (3.96), strategic alignment (3.88) and value delivery (3.58). As depicted in **figure 2**, there are differences when specific groups are considered. For example, executives chose risk management, strategic alignment and regulatory compliance as their most significant outcome expectations, and placed performance management as their least important outcome. Security and IT executives and management chose regulatory compliance as the most important outcome, with mean scores of 4.57 and 4.45 respectively, which demonstrates the strength of this choice. It is also interesting to note that IT executives and management and their information security counterparts viewed regulatory compliance, risk management and strategic alignment as the most important information security governance outcomes, whereas executive management identified risk management, strategic alignment and then regulatory compliance as the most important outcomes.

Figure 2—Outcomes and Executive Positions



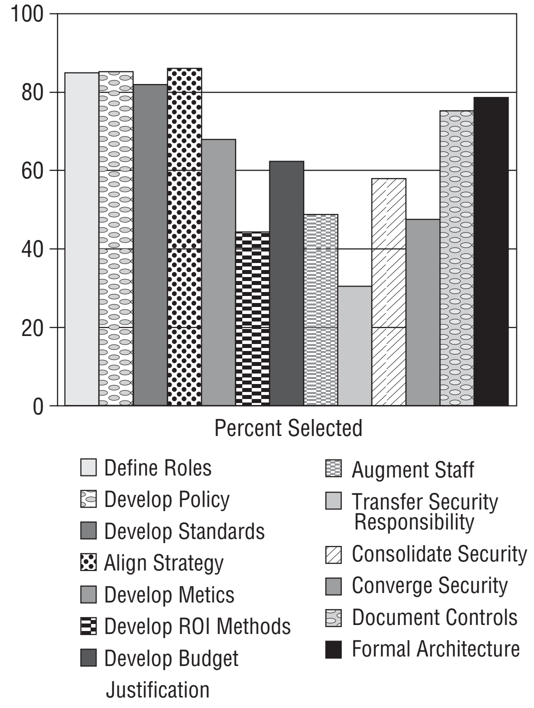
For organizations that had completed or were completing an information security governance project, the most important expected outcome was regulatory compliance (4.3) followed by risk management and strategic alignment with the business.

Information Security Governance Project Components

The activities that can be part of an information security governance program vary depending on the current state of the program and the expected results of this initiative. Survey participants were offered 13 activities that ranged from defining roles and responsibilities to documenting the control structure, and had to identify whether the activity was part of an information security governance project.

For all survey participants, the activities that would be included in an information security governance project included defining roles and responsibilities, developing policy, defining security standards and procedures, and aligning security roles and responsibilities (see **figure 3**). These activities appear foundational in nature. Projects such as transferring information security responsibilities to other

Figure 3—Governance Project Components



departments, developing return on investment calculation methods, converging traditional and information security, augmenting information security staff, and consolidating security responsibilities within one department were the least favored project activities.

Among management groups represented in the survey, there was a difference of opinion as to what activities should be part of an information security governance project. In 88 percent of the responses, executive management selected policy development and security strategy alignment with business goals and objectives as a part of a governance project. Ninety-four percent of the information security management participants identified the definition and alignment of roles and responsibilities as part of a governance project. IT executives and management most often selected (94 percent) the development of a formal security architecture as part of a governance project. In organizations where information security governance projects have been completed or are underway, almost 92 percent of the survey participants identified aligning security strategy with organization goals and priorities as being part of a project. For those not currently pursuing information security governance, security strategy alignment was identified as a project component in only 75 percent of the responses. For this group, the most frequently cited parts of an information security governance project were policy development, defining roles and responsibilities, and developing standards and procedures.

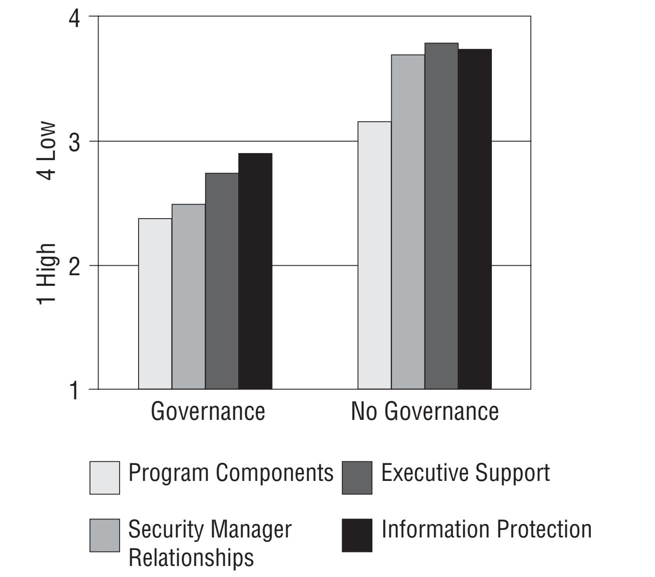
There were some interesting regional results. For North American survey participants, policy development, aligning roles and responsibilities, developing standards and procedures, and developing a formal information security architecture were most consistently identified as part of a governance project. For European survey participants, defining roles and responsibilities, alignment, and policy development were identified as part of a project in more than 90 percent of the responses. The development of an information security technical architecture was identified as part of an information security governance project in only 63 percent of the responses.

Information Security Governance Benefits

Survey participants were asked to indicate what they felt the quality of their organization's information security program was on a four-point scale, 1 indicating excellent and 4 poor. The content areas included security program components, the relationships between security and other business leaders, executive support for information security, and the quality of information protection. One would expect that, in organizations where there had been an investment in information security governance or where a project was in progress, there should be a marked improvement in quality in each of these categories. As indicated in **figure 4**, for each of the areas being considered, those who had completed or were completing an information security governance project felt that the quality of protection and relationships were better.

The information security program components in the survey include performance metrics, incident response, effectiveness, activity monitoring, trend analysis, the ability to accommodate changing business conditions, the ability to accommodate regulatory changes, and current state and gap analysis. For organizations in which an information security governance program was in the process of being put in place or currently in operation, quality excellence was identified for the ability of security plans to accommodate regulatory requirements (1.94), security measures reduce the impact and duration of incidents (2.13), security infrastructure is used effectively (2.13), and security activities are integrated into business operations. For organizations in which an information security governance project had not been considered, the areas where quality was most lacking focused mostly on reporting and metrics. These organizations identified the areas of least quality as formalized security performance metrics (3.65), security trend analysis (3.65), security metrics demonstrate the effectiveness of risk control measures (3.7), and current-state evaluations are performed to evaluate program effectiveness (3.25).

Figure 4—Governance-No Governance Comparison



Information security program management support of quality items for the survey included management understanding of the security program relevance to business objectives, process owner support for the security program and seeing security as an enabler, support for the security culture, process owner acceptance of security responsibility, and process owner accountability for security. The areas of highest reported quality in this category for organizations that had invested in information security governance included the optimization of security investments to support business objectives (2.3) and support by business owners for the information security program (2.34). Organizations that had not made an information security governance investment reported the least quality in process owner accountability (3.65), security being seen as a business enabler (3.6), process owner support for the security program (3.55) and the development of support for a security culture (3.55). In these organizations, the highest quality was in the area of process owner acceptance for security responsibilities, but this received a mean score of only 3.4 out of a possible high score of 4.

Survey participants were asked to rate the quality of executive support for the information security program. As would be expected, the quality of relationship with executives was high. Survey results indicate the highest level of executive relationship quality in executive understanding of the relevance of information security to the organization (1.81), executive active support for the security program (1.96) and executive understanding of liability for not executing information security responsibilities (1.98). Almost the inverse response was received from participants where an information security governance program had not been planned. The areas of least quality for these organizations were executive promotion of security governance (3.45), support for the information security program (3.25) and understanding the liability of not executing information security responsibilities (3.05).

In a prior study released by ISACA, *Critical Elements of Information Security Program Success*, the six most critical factors reported by a focus group and an international group of survey respondents were:

- Senior management commitment to information security initiatives
- Management understanding of information security issues
- Information security planning prior to implementation of new technologies
- Integration between business and information security
- Alignment of information security with the organization's objectives
- Executive and line management ownership and accountability for implementing, monitoring and reporting on information security.

The *Information Security Governance* research project supports these findings and indicates that a strong information security governance program can address these six critical factors to the benefit of the organization.

The last area of quality examined addressed the protection of information. Elements of protection included the identification of sensitive and critical resources, classification, ownership and data retention. For organizations where an information security governance program had been developed or is in progress, the highest areas of quality performance included the identification of critical business applications (1.9), the identification of applications that process sensitive information (2.05), that data retention requirements are known (2.14) and that information classifications are applied to information provided to outside entities. For organizations that have not undertaken an information security governance project, the areas of best performance included knowing data retention requirements (2.7) and identifying critical applications (2.9). The areas of least quality included the enforcement of data classifications (3.25), ownership assignment (3.4), the application of classifications to information received from outside entities (3.4), the identification of all information in use in the organization (3.3) and assigning criticality levels of information (3.25).

The information that was gathered through this research activity aligns with industry activities and trends. The results of this study support the assertion that properly governed information security can be an asset to the success of an organization vs. a drain on productivity and resources. Organizations that are investing in information security are beginning to see the benefits of their efforts. They are able to address information security as a business initiative, and monitor and measure the effectiveness of their efforts in a fashion that is meaningful to their executive leadership and their organization as whole.

John P. Pironti, CISA, CISM, CISSP, ISSAP, ISSMP
is a principal enterprise solutions architect and principal security consultant at Unisys Corporation. He has designed and implemented enterprisewide electronic business solutions, information security programs, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, government, hospitality, aerospace and information technology. He is a published author and writer, and a frequent speaker on electronic business and information security topics at domestic and international industry conferences. Before joining Unisys, Pironti was a principal enterprise solutions architect and security consultant for Genuity Inc. Prior to that, he held technical and management positions at AT&T.

Editor's Note:

Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, is available as a complimentary download from the ITGI web site, *www.itgi.org*. A print edition is available for purchase at *www.isaca.org/bookstore*.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal. Information Systems Control Journal* does not attest to the originality of authors' content.

www.isaca.org