Key Elements of an Information Risk Management Program:

Transforming Information Security Into Information Risk Management

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

Information security and protection are critical to an organization, but cannot guarantee its success. To facilitate effective protection of information, a risk management approach that balances the need for information security against the needs of the organization enables the organization to be efficient and successful in its activities. Information has always had associated value, but only recently have capable and motivated adversaries truly understood and exploited this value.

The current trend in global enterprises has been to establish individual organizational units to address compliance, information and physical security, privacy, and operational and financial risk to facilitate corporate governance in each of these areas. Each of these groups is effective at achieving its own goals; but because they work independently and are aligned to separate leadership, they may not achieve the overall goal of effective information risk management. By combining these groups into a singular business function or organization, effective information risk management is possible.

Why Is Information Security So Challenging?

Information security is the most challenging aspect of information processing because it is ever-changing and evolving. The simple reason for information security being so challenging is that the adversary only has to be right once, but the defender has to be right all of the time. The defender is plagued with a lack of investment, resources, time and knowledge. The organization expects the defender to be able to prevent any damage to its information infrastructure, even with the limited resources and capabilities available to it. As soon as the defender creates and implements a control or set of controls to defend against an attack from an adversary, the adversary develops a new and more effective attack that forces the defender to develop yet another control.

Ethics, laws, morals, lack of funding and lack of resources do not restrict adversaries. The global communication capabilities that have grown as a result of the adoption of Internet capabilities have allowed the adversary community to come together, without ever having a verbal or in-person conversation, to develop innovative attacks, share research and knowledge, and develop capabilities that far surpass what any one organization could achieve. The best chance the defender has to defeat the adversary is to take a risk management approach to information protection that facilitates the protection of the essential and critical elements using the available resources and capabilities.

Current State of Information Security

Information security still narrowly focuses on the use of technology to mitigate threats. Experience has proven that policy, process and procedure, complemented by technology, provide more effective defense, in most cases, than technology alone; however, most do not routinely implement these components. This is because policy, process and procedure are difficult to implement and operate compared to the instant perceived value achieved by purchasing and installing a technological control. This lack of patience has allowed the threat landscape to expand and the ability for adversaries to exploit information infrastructure to significantly increase.

There is also a very dangerous global trend today known as "security by compliance." This is the act of focusing all information protection efforts on requirements established by government and industry regulations. Regulations such as the Payment Card Industry (PCI) standard, US Sarbanes-Oxley Act, European Data Protection and Privacy Act, and information disclosure laws provide guidance on the protection of information in some form or fashion. Some of these standards, e.g., PCI, provide prescriptive guidance on the specific technologies and controls that an organization needs to implement, even though the controls may not be effective or even relevant to that organization. This concept is extremely risky since it focuses the organization's efforts on meeting compliance standards instead of understanding and mitigating the actual risks and threats to its information and information infrastructure.

The threat landscape organizations face has dramatically changed in the past few years. The attack community has shifted its focus from proof of concept and status-seeking attacks to highly targeted, highly effective and nonadvertised attacks. This means that the traditional intelligence, technological control frameworks, and methods and practices used to protect information and information infrastructure may no longer be effective, or may have a reduced level of capability. Organizations must implement new capabilities based on risk-based decision processes and frameworks to face this new challenge.

Information Risk Management vs. Information Security

Information risk management defines the areas of an organization's information infrastructure and identifies what information to protect and the degree of protection needed to align with the organization's tolerance for risk. It identifies the

business value, business impact, compliance requirements and overall alignment to the organization's business strategy. Once this information has been identified, it can be presented to the business leadership to make decisions about the level of investment (both financial and resource) that should be utilized to create appropriate information protection and risk management capabilities.

After making these decisions, the information security team can implement the appropriate capabilities to align with the business leadership's decisions. The information security group identifies threats, develops and implements controls, and monitors the effectiveness of these capabilities on a regular basis to ensure alignment. The key difference in this risk management model compared to the current information security state in most organizations is the disempowerment of the information security team. In the risk management model, the information security team no longer has the authority within the overall organization to make decisions of what to allow and not allow related to the security of information and information infrastructure. Instead, it provides valuable insight and information to the business leaders who then make these decisions in a business-appropriate way. This fundamental change dramatically improves the effectiveness of this team because the organization considers its members to be advisors who enable business, not police officers who impede business.

Evolution to Information Risk Management

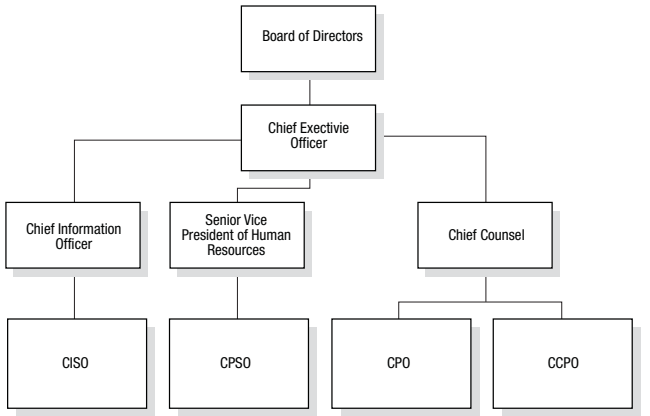
Information protection and assurance capabilities and programs exist in various stages and forms within most organizations today. The capabilities are typically segregated by function and have leaders with titles such as chief information security officer (CISO), chief privacy officer (CPO), chief physical security officer (CPSO) and chief compliance officer (CCPO). Unfortunately, the reality of most of these positions is that they are given the title of "chief," but they do not have regular access to senior leadership or insight into key business strategy or activities, and report to separate leadership categories. They also tend to work independently of each other with some degree of interaction based on necessity, not business strategy.

These capabilities must evolve to meet today's current and emerging challenges to information and information infrastructure. The evolution of these capabilities (**figure 1**) requires integration of all of these independent capabilities into a singular business entity, known as the information risk management program.

Information Risk Management Program

An information risk management program provides an organization a 360-degree holistic view of the risks to its information assets and associated information infrastructure. This program represents an evolved corporate governance model for information-risk-management-related concepts and activities. It also consolidates the individual leadership and program elements that currently exist to provide information protection and assurance into a single functional organization led by a single individual who has access to senior business leadership on a regular basis and has insight into all aspects of the business activities and strategy.

Figure 1—Evolution of Information Risk Management



When effectively implemented and operated, this program provides value to the organization by enabling it to conduct business in a risk-aware way. Instead of limiting an organization from being able to operate, it provides guidance in more effective ways, allowing it to operate while still protecting its information infrastructure and assets. The program changes the paradigm of how an organization operates by finding a way to enable business activities and capabilities instead of limiting them based on perceived threats. For example, it does not stop the organization from providing access to systems and information, but instead evaluates how much access is required and when this access is appropriate. Too much information security can be a disabler to business. This program's goals are to ensure that only the minimum level of risk is taken with information assets while still allowing the business to meet its goals.

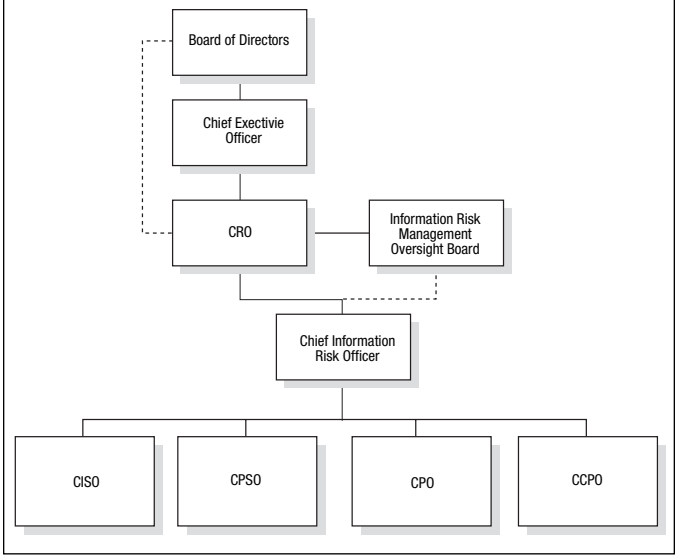
Evolved Organization Design

To effectively meet the risk management needs of an organization, a consolidated and streamlined approach to the organization structure for management activities (**figure 2**) needs to be implemented. This streamlined approach allows all risk management activities that take place within the organization to report into a single leader—the chief risk officer (CRO). This leader is the focal point for all communications regarding risk identification, mitigation and management. This leader also has regular interaction with senior leadership to provide insight, guidance and direction to the organization about the information-related risks involved in business decisions, strategies and activities.

Key Performance Indicators

Key performance indicators (KPIs) are essential measurement tools implemented to provide business intelligence about the performance of a business function, process or capability. To effectively govern information risk management within an organization, each function and process must be associated with measurable KPIs. These indicators need assigned thresholds so the organization has insight about when the business capabilities are working within normal

Figure 2—Evolution of Organization Design



operating boundaries and when they require attention. KPIs also provide valuable insight into the value provided by the information risk management program and assist in the maturing of its capabilities.

For KPIs to be effective, they must be designed with the business function and process in mind, speak the language of the business, and be effectively communicated to the organization. KPIs that do not meet these criteria are typically ineffective and can cause confusion and damage within an organization. It is important that the developed and introduced KPIs have recognized value within the organization. To facilitate this business process, owners and the audience to which they are communicating must be involved in their creation, operation and dissemination; this will ensure that they are serving the business instead of being just another data point that will be ignored or misunderstood. Ineffective or inaccurate KPIs can cause as much, if not more, damage than not having them in the first place.

Key Elements of an Information Risk Management Program

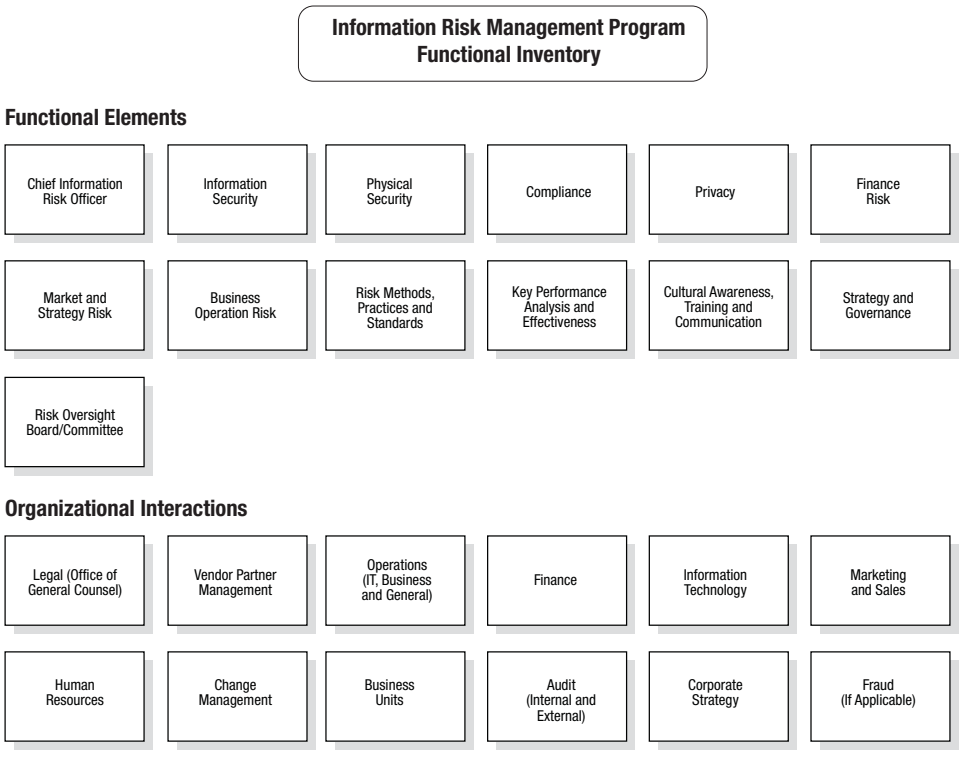
The information risk management program (**figure 3**) provides a structured approach to enterprise information risk management. It utilizes many of the capabilities that exist within an organization and implements processes and capabilities that enable more effective communication and information sharing. It increases the efficiency of these capabilities by consolidating functions and developing consistent methods, processes and procedures.

The risk management program acts in an advisory or consulting capacity with minimal operational responsibility within an organization. Instead of making decisions about information protection and assurance for the organization, it provides credible and valuable information to decision makers to assist them in making appropriate business decisions.

Chief Information Risk Officer

The chief information risk officer (CIRO) is the natural evolution for the role of the chief security officer (CSO) and has overall ownership of the information risk management

Figure 3—Information Risk Management Program



program and leads its activities. This individual is the focal point for all risk-related communications to the leadership of the organization, as well as the organization as a whole. This individual should be a senior leader within the organization and is expected to be involved in key leadership activities. The CIRO establishes and communicates the information risk levels for different business elements and processes within the organization, as well as for the organization as a whole.

The KPIs of CIROs include:

- Number of information risks identified, evaluated, categorized and mitigated
- Awareness of information risk management program (internally and externally)
- Impact of information-related events or incidents compared to competitors and peers

Information Security

Information security is effective at providing information about threats and vulnerabilities that affect the organization, but is not effective at identifying risks. The information security organization often has the task of identifying risks to the organization's information and associated information infrastructure. This is something that most information security organizations cannot properly carry out since they do not have the insight of corporate strategy, audit, compliance, finance and marketing required to provide this type of service.

The role of the information security organization in the risk management model is to identify and evaluate threats and vulnerabilities to the information assets and the information infrastructure of the organization. This group defines, implements, monitors and matures the controls and control frameworks utilized to mitigate the identified threats and vulnerabilities. The group does this once it has been given direction from the business about the risk-tolerance level associated with the threats and vulnerabilities with which the organization is comfortable. With this information, the group develops appropriate controls that map to the business needs of the organization.

One of the key benefits the information security function provides to the information risk management organization, using threat and vulnerability analysis, is information about the threats and vulnerabilities to information and information infrastructure. By carrying out this activity, information security can provide credible information on the business impacts and viability of potential threats and vulnerabilities to the information risk management organization. These data are invaluable input for the development of risk profiles and risk information communicated to the organization. They allow the most viable and business-affecting threats and vulnerabilities to be addressed in a timely fashion and others to be monitored for future consideration.

The KPIs of information security include:

- Accuracy of threat and vulnerability analysis activities and information
- Effectiveness of vulnerability management plans and controls
- Effectiveness of policies, procedures, methods and standards

Physical Security

The physical security organization provides insight into threats and vulnerabilities to the physical infrastructure elements of the organization and to personnel. This group defines, implements, monitors and matures physical controls and control frameworks that are used to mitigate the identified threats and vulnerabilities. This is done after receiving direction from the business about the risk-tolerance level associated with the threats and vulnerabilities with which the organization is comfortable. Based on this information, appropriate controls that map to the business needs of the organization are developed.

The KPIs of physical security include:

- Number of business-impacting physical security events or incidents
- Number of physical threats identified and associated remediation plans developed
- Effectiveness of physical security controls

Compliance

The compliance function identifies the policies, standards and regulations with which the organization is required to comply; ensures that the organization has the appropriate controls in place to meet these requirements; and monitors the organization. This function also ensures the proper communication of this information throughout the relevant portions of the organization and to the external regulatory and oversight organizations.

The compliance function establishes a metrics and measurement framework to ensure that ongoing compliance measurement and management can occur. This allows the organization to understand the areas that currently do not comply with applicable regulatory and policy requirements and to identify areas where too much has been invested to achieve compliance goals and requirements.

The KPIs of compliance include:

- Number of external or internal audit findings
- Cost associated with regulatory compliance requirements
- Number of exceptions applied for and granted to internal policies and regulatory requirements

Privacy

The privacy function establishes the privacy requirements and associated policies and procedures for the organization. This function defines and identifies the utilization of nonpublic personal information (NPPI) within the organization, identifies business and personnel risks associated with its use, and defines the appropriate and acceptable uses of this information within the business processes of the organization. The privacy function also produces and governs the implementation of the official privacy statement and the associated control requirements for the organization to communicate to internal stakeholders, customers, vendors and partners.

The KPIs of privacy include:

- Number of privacy-related disclosures or incidents
- Awareness of privacy policies and procedures by internal and external stakeholders
- Number of exceptions requested and granted to privacy policies

Finance Risk

The finance risk function evaluates financial risks to the organization, including credit, capital, investment and financial risks, and fraud associated with business-process activities or company initiatives related to information assets within the organization. The finance risk function provides insight into

the potential financial impacts of business decisions as well as incidents and events that impact business. Other functions within the risk office with financial impact analysis information associated with their individual activities and functions are also provided.

The KPIs of finance risk include:

- Costs associated with information risk management controls
- Costs associated with information risk management events and incidents
- Number of financial risk models developed for identified credible threats and vulnerabilities

Market and Strategy Risk

The market and strategy risk function provides insight into the potential impacts of business activities and events derived from market-focused activities and corporate strategy associated with information assets. This function analyzes current market conditions applicable to the organization and identifies risk areas that could prevent the success of the organization in its overall activities or particular business processes. The strategy element of this function analyzes the business strategy of the overall organization and of individual business processes and activities, to identify information risks that could affect success. This element also examines new business initiatives and concepts to assess the associated risk to information.

The KPIs of market and strategy risk include:

- Number of negative media items related to information events
- Impact of information protection activities and requirements on go-to-market strategy
- Accuracy of risk analysis compared to actual consequences of identified strategic activities

Business Operation Risk

Business operation risks are those that cause the organization to no longer function in a business-as-usual fashion. This function analyzes business-process-specific risks to appropriately identify, classify and manage them to account for activities associated with information assets that may potentially affect business. This function also implements metrics and measures to monitor the capabilities and effectiveness of controls utilized to mitigate identified threats and risks to business operations.

The KPIs of business operation risk include:

- Impact of risk-mitigating controls on business processes
- Number of identified credible risks to business operation
- Accuracy of metrics and measures that are implemented to monitor identified risks and controls

Risk Methods, Practices and Standards

To properly identify, analyze and manage the information-related risks to an organization, the organization must develop, utilize and maintain a consistent set of methods, practices and procedures. These capabilities include both human processes and automated systems that generate credible and actionable risk intelligence for the organization in order for business-appropriate decisions to be made. This function is responsible for creating these capabilities and ensuring that they evolve and mature. These capabilities should be auditable by an independent review board to ensure that they are accurate in their capabilities and the information they generate is credible risk information.

The KPIs of information risk management methods, practices, procedures and standards include:

- Adoption rate of methods, practices, procedures and standards by the intended user base
- Maturity level compared to capability maturity model standard of methods, practices, procedures and standards
- Number of new capabilities introduced within the organization to enhance risk management capabilities

Key Performance Analysis and Effectiveness

Each functional element of the information risk management program includes a series of KPIs utilized to ensure that they are functioning as designed and bring value to the business. It is important to monitor, analyze and mature these KPIs to make certain they are appropriate for the functional area and for measuring the performance they are designated to monitor. This function is responsible for defining KPIs for functional areas and gathering all of their associated data points. Once this information is gathered, it is analyzed to create meaningful and actionable reports about the risk posture of the organization and provide insight into the effectiveness of the risk management program.

This function is also responsible for the identification and development of KPIs, as well as their maturity and life cycle. Certain KPIs are effective only for the life of a specific business process or function within the risk management program, while others are indicators that are consistent for the life of the program. Once a new functional area has been identified, this function develops and monitors the KPIs for that function. Reports on the maturity of these KPIs are generated to make sure the organization consistently improves and high levels of integrity and accuracy are achieved.

One method used to achieve insight into the maturity of the capabilities and KPIs of the program is to map them to the Capability Maturity Model standard. This standard allows the organization to have insight into the level of maturity associated with the risk management organization's capabilities and understand the level of confidence and integrity that should be expected from the information and guidance provided by the organization.

The KPIs of key performance analysis and effectiveness include:

- Number of measurements analyzed and metrics developed
- Benchmark of capabilities against industry standard or peer group data points
- Usability of reports generated by intended user base

Cultural Awareness, Training and Communication

One of the key challenges to information risk management is a lack of awareness of risks as well as risk identification and mitigation capabilities within organizations. In many cases, the human is the most effective risk mitigation control an organization can utilize. This function is responsible for effective communication of risk information, capabilities and the value of the information risk management organization throughout the enterprise; its associated vendors, partners and customers; and any other audiences that the enterprise believes would benefit from risk management education and knowledge.

To provide this capability to the organization, this function must develop tools and capabilities to help understand, educate and communicate the organization's culture. Cultural considerations such as language, learning styles, geopolitical considerations, and personalities and backgrounds of individuals are identified by this function. After gathering this information, training and awareness activities can accommodate individual requirements for learning and processing information and incorporate them into beneficial business activities.

The KPIs of cultural awareness, training and communication include:
- Number of information-related events or incidents
- Adoption of information risk management practices and capabilities within organization
- Effectiveness of training and awareness materials for intended audiences

Strategy and Governance

The information risk management organization is a business unit within the enterprise that provides advisory services as well as operational activities to provide value. The strategy and governance function provides structured management and strategic thinking to the information risk management program to ensure that constant value is provided to the organization. The governance portion of this function establishes the operational requirements that include competency models, organizational structure, metrics and measures for analysis of business processes provided by the program, and operational processes.

The strategy element of this engagement identifies future direction for the information risk management organization to ensure alignment with business requirements and leading practices, standards and methods that exist within the enterprise and the global information risk management community. This function ensures that the appropriate business processes exist within the individual functional areas to properly support its capabilities, and identifies and integrates new activities or capabilities to be more effective and bring more value to the entire organization.

The KPIs of strategy and governance include:
- Cost of information risk management activities
- Maturity of competency models and their accuracy to meet business needs and requirements
- Organizational feedback on the effectiveness of the information risk management program

Risk Oversight Board/Committee

The information risk oversight board/committee ensures that the activities of the information risk management organization align with the business activities and requirements of the overall organization. This board/committee is composed of stakeholders who are leaders from all key business functions within the enterprise. They provide both tactical and strategic guidance to the information risk management program.

The KPIs of the risk oversight board/committee include:
- Number of key business stakeholders represented in oversight board/committee
- Effectiveness of guidance provided by the oversight board/committee

Organizational Interactions

For the information risk management program to be effective within the organization, it should align with other key business groups to obtain input for its activities and provide results of its activities to help make better risk management decisions. These organizational interactions extend beyond training and awareness activities to include regular communication methods and channels among functional organizations.

The KPIs of organizational interactions include:
- Number of information-related events or incidents
- Effectiveness of communication techniques and capabilities between organizational elements
- Feedback on effectiveness and value of the information risk management program and its capabilities

Final Thoughts

Information risk management is the maturation and evolution of information security within an organization. The introduction of an information risk management program allows an organization to have a holistic view of risks that can affect its productivity and success. It also enables the organization to have educated insights and data points of reference from a wide spectrum of considerations to make business-appropriate risk management decisions. The information risk management organization is essentially a consulting organization that provides information to decision makers instead of making decisions for them. By doing so, it delivers more value to the organization and is welcomed into the business rather than avoided until risks become reality.

John P. Pironti, CISA, CISM, CGEIT, CISSP, ISSAP, ISSMP is the chief information risk strategist for Getronics. He designs and implements enterprisewide electronic business solutions, information risk and 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, on a global scale. He is a published author and writer, and a frequent speaker on electronic business and security topics at international industry conferences.

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*.