Key Elements of an Information Security Program

By John P. Pironti, CISA, CISM, CISSP

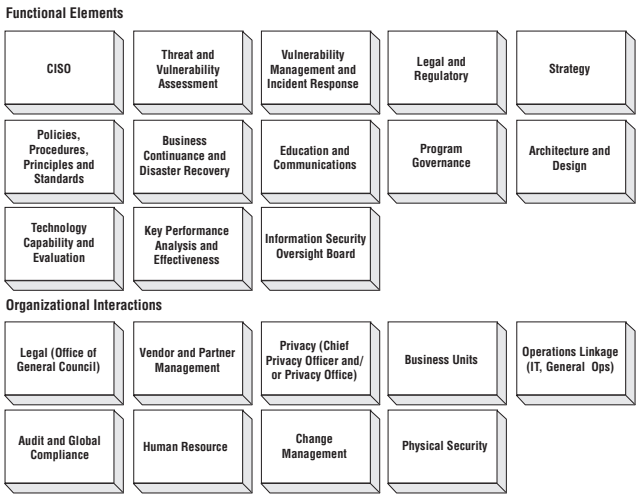
The information security function has evolved from a back-office technical specialty into a recognized and required business function in the modern-day organization. A key component of this evolution is the introduction of the information security program.

The information security program brings structure and governance to the information security function within an organization. This structure and governance allow the information security organization to function as a key element within the enterprise to support its business goals. It also allows an organization to achieve the goal of transforming information security incidents into operational anomalies.

Functional Inventory

There are many elements included within an information security program (see **figure 1**). These elements are modular in nature, but depend upon one another for success. They are represented in the functional inventory, which includes functional and organizational interaction modules. Each of these elements has a corresponding role and function associated with it. They also have individual key performance indicators associated with them to ensure their ability to be measured for their success or failure as well as their maturity.

Figure 1—Information Security Program Office Functional Inventory



Program Benefits

Introducing an information security program is cornerstone to an effort to transform information security into a proactive activity driven by the business leadership, instead of a reactive one driven by technologists within an organization. By introducing a structured approach to information security, an organization can increase its security posture and reduce the costs surrounding information security. It can also gain an advantage in its efforts to ensure compliance to existing and future information infrastructure-related regulations.

There are currently information security elements to multiple regulations by which global organizations are overseen, including the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, Basel II, the European Data Privacy Directive and various other regulations that have a significant impact on how organizations maintain the security and integrity of their information assets (see **figure 2**). These regulations were put in place to maintain a baseline standard for security in organizations, since it was demonstrated that they had not been doing an adequate job of this without regulation. Organizations had not been effectively protecting themselves from malicious adversaries or incidents created by user error. As information becomes more valuable in the eyes of the user and the adversary, more regulation will be put in place to ensure that even higher levels of security are in place. The introduction of an information security program that aligns to leading industry practices and methods allows an organization to achieve compliance with current information security regulations and be well suited to comply with future regulations.

An information security program also enables the organization to make mature risk management decisions by providing information about the organization's information security capabilities in a business-friendly context. This

Figure 2—Gramm-Leach-Bliley Act Section III

Development and Implementation of Information Security Program, Section B

- Assess risk. Each bank shall:
  - Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems
  - Assess the likelihood and potential damage to these threats, taking into consideration the sensitivity of customer information systems
  - Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks

information allows business leaders to understand their capabilities to withstand security events and the impact that these events can have on the organization's ability to function. The transformation to a proactive environment, from a reactive one, allows the organization to use these data to take preventive measures prior to being the victim of a malicious or accidental security situation.

Key Performance Indicators and Role Summaries

To implement an effective governance structure for the information security program, it is important to identify the roles and key performance indicators (KPIs) for each element of the functional inventory. These roles and KPIs allow the management team to have an effective way of identifying competency models for staffing the different elements of the organization as well as an effective way of measuring the success and maturity of each element. The elements of the functional inventory follow.

Chief Information Security Officer (CISO)

- *Role*: The chief information security officer element represents the leadership and overall management aspect of the program. The CISO is responsible for all elements of the program—reporting meaningful data points to senior management as well as establishing the threat level for the entire organization.
- *KPIs*:
  - Number of information security-related incidents that impact the operational effectiveness of the business each year
  - Effectiveness of the information security program in aligning with business goals and initiatives of the organization
  - The awareness of the information security program and its capabilities within the organization
  - The impact of security threats and attacks on the organization compared to the impact of these same threats and attacks on competitors and peer organizations

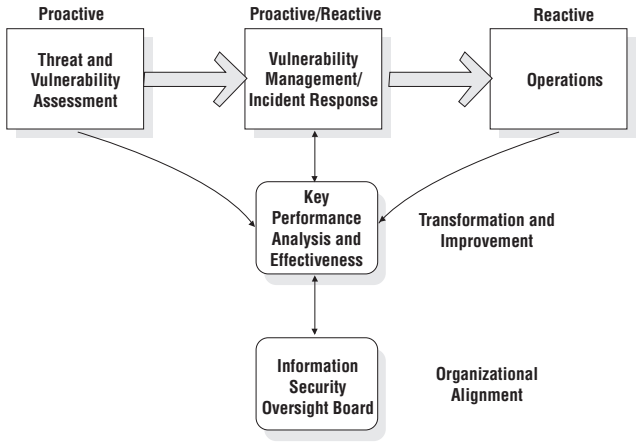
Threat and Vulnerability Assessment (TVA)

- *Role*: The threat and vulnerability assessment role has proactive and reactive elements. This role provides the business elements of the organization with an educated and analyzed view of the risk and likelihood of threats that exist to the information infrastructure of the organization. It accomplishes this by utilizing a threat analysis methodology to accurately assess the existence, likelihood and business impact of threats to individual solutions within the organization as well as the organization as a whole. The outputs of this threat analysis activity establish the individual threat-level designations for each solution that is reviewed. This information is also conveyed to the CISO to assist in the establishment of the current threat-level designation for the overall organization.

  The TVA team also provides threat mitigation and identification information to the vulnerability and incident management element of the functional inventory, providing this element a more educated view of what a potential attack would look like. With this information, technological controls can be put in place to establish an early warning capability for attacks and maintain a developed attack mitigation plan available to combat the attack.

  The reactive element of the TVA function is put into place when an active attack exists that may affect the organization. In this case, it is the responsibility of the TVA role to provide near real-time threat assessments of the potential business impacts of the attack on the information infrastructure of the organization.
- *KPIs*:
  - Accuracy of the threat analysis activities:
    - Likelihood and impact projections
    - Threat designations
    - Threat identification characteristics
  - Responsiveness to emerging threats
  - Ability to communicate appropriately to the organization

Figure 3—Threat and Vulnerability Management Process Flow



Incident and Vulnerability Management

- *Role:* The incident and vulnerability management function contains proactive and reactive elements (see **figure 3**). The proactive element of this function gains inputs from the TVA function as well as other sources to understand what vulnerabilities exist and the risk they pose within a particular solution or the organization as a whole. This function is then responsible for implementing controls and measures to mitigate the risk posed by these vulnerabilities.

  One way by which the vulnerability management function can accomplish this goal is through the creation of response plans to attacks against the identified vulnerabilities within the solution. These response plans can include prescriptive guidance on how to identify and appropriately respond to an attack. They can then forward these identification and response plans to the operations organization via a linkage role, so they can utilize this information to include the identification and remediation steps within their automated monitoring systems and incident response training systems.

  The reactive role for this function covers traditional incident response activity. In this role, the element is responsible for the remediation of malicious activities that are hindering the

organization's ability to function appropriately. The one difference in this case is that the incident response team now becomes the second tier of response in the case of an incident, instead of the first. The first tier of response is now handled by the operations teams. The incident response element of this function is invoked only when the incident that is occurring has not previously been identified and an appropriate response plan created for use by the operations teams. The incident response team may also be invoked when the response plan that was created does not work appropriately, or the operations team does not have the appropriate resource pool available to effectively execute the response plan.

- *KPIs*:
  - The effectiveness of the developed remediation plans and controls
  - Number of identified vulnerabilities and remediation plans created for these vulnerabilities
  - Time required for remediation of business-debilitating information security events
  - Number of incidents that required invocation of incident response team to remediate security incident

Legal and Regulatory

- *Role*: The legal and regulatory function ensures that appropriate legal and regulatory considerations associated with information security activities are appropriately considered for the organization. This function does not replace the traditional legal department within an organization; it is a complementary function that addresses specific issues associated with information security and regulatory considerations.

  One of the primary functions of this element is to provide legal language for vendor/partner/customer agreements and contracts for information security-related activities. These can include language that allows an organization to ensure that intellectual property and information are protected by appropriate controls and measures to ensure compliance with organizational policy and regulation.

  The legal and regulatory function also has a responsibility to understand the emerging global legal and regulatory landscape and how it can affect the way an organization does business in regard to information security-related activities. This function provides analysis of these trends and regulations and ensures the current business-as-usual policies, processes and procedures.
- *KPIs*:
  - Number of legal actions taken against an organization related to information security
  - Number of legal issues highlighted through the research and analysis of legal and regulatory trends and activities
  - Timeline for regulatory compliance to new regulatory requirements by which the organization is regulated
  - Number of policies, agreements and contracts that are updated with required language to provide appropriate risk mitigation from legal actions

Strategy

- *Role*: The strategy function is primarily an internal function ensuring that the information security program is aligned with leading industry and organizational practices. It does this by monitoring trends within the information security community as well as trends and business activities with the organization. With this knowledge and insight, this function can provide guidance for information security processes and technologies within the organization while ensuring the goals of the program are always aligned with the goals of the organization.
- *KPIs*:
  - Number of security-related incidents per year
  - Adoption of identified leading information security practices within the organization
  - Identification and effective communication of emerging information security-related trends, regulations and standards
  - Positive compliance and audit reports from internal and external auditors or examiners

Policies, Principles, Procedures and Standards

- *Role*: This function provides a centralized area for the development of policies, principles, procedures and standards concerning information security to support the business goals of the organization. It also defines the control structure required to ensure that the created/developed materials are being followed to ensure compliance with organizational guidelines and regulatory considerations.

  This function provides a structured approach to the adoption of information security concepts and practices for the organization as a whole. The materials it creates should be designed to be complementary instead of prohibitive to the business objectives and activities of the organization. This will ensure that these materials are adopted within the organization and transformed into business-as-usual activities.
- *KPIs*:
  - Number of security incidents before and after the introduction of policies, principles, procedures and standards
  - Time frame for introduction of a supporting policy or procedure after a business or regulatory need is identified
  - Adoption of materials by intended user community as a business-as-usual activity
  - Awareness and knowledge of policies, principles, procedures and standards within the organization

Business Continuance/Disaster Recovery

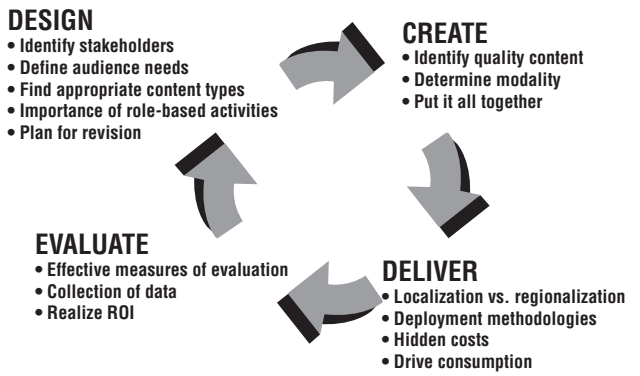
- *Role*: The business continuance/disaster recovery role identifies critical business functions and processes to create a capability to continue these services in the event of a business-debilitating event. Information security becomes a key issue during a business-debilitating event, since many attacks occur during times of perceived weakness. This function has ongoing responsibilities to continually evaluate the organization as a whole and create a prioritization schedule of the key capabilities for business operations to continue. Once this schedule has been created, this function creates an operational

plan to ensure that the business capabilities can continue while the organization is dealing with the business-debilitating event. The plan also includes a detailed analysis of security risks that can arise during the use of the plan, and tools and techniques that will be implemented to mitigate these risks.

The business continuance function also has the responsibilities to create and implement controls within the organization that identify when the business continuance/disaster recovery plan needs to be initiated. These controls ensure that the core business functions can continue to operate even if the primary operation is affected by a business-debilitating event. Controls that identify when the business-debilitating event has been resolved and the primary capabilities can begin to function again are also developed by this function.

The business continuance function also becomes an integral element in the incident management model associated with the threat analysis and vulnerability management functions. The business continuance/disaster recovery element becomes the third tier in the incident response activity. The first tier is the operations team, which responds to security incidents until they grow beyond their response capability. Then, the incident response function assists in the remediation of the security incident. If the incident grows beyond the control of the incident response function, then the business continuance function is called upon to ensure that the core business functions continue to operate while the security incident is being addressed.

Figure 4—Programmatic Approach to Education and Communication



• *KPIs*:
  – Results of testing the elements of the business continuance/disaster recovery plan as well as the complete plan
  – Competency levels of staff needed to operate in a business continuance/disaster recovery mode
  – Effectiveness of controls to identify potential business continuance/disaster recovery situations
  – Awareness of the plan in the organization and the individuals' knowledge of their responsibilities as they relate to the plan

Education and Communications

• *Role*: The education and communications function provides the primary source of structured information for the organization concerning information security (see **figure 4**). This function designs and implements training on information security awareness, technologies, and leading industry and organizational practices. This function is also responsible for the effective deployment of the applicable elements of this training to the employees of the organization and its partners, vendors and customers. The effectiveness of the deployment is gauged by utilizing feedback mechanisms that can act as controls for the function.

For the education and communications function to be effective, it must be flexible enough to allow personalization and localization to the audience with which it is attempting to communicate. This is because each element within the organization interprets and utilizes information differently. This can include language and culture considerations as well as role considerations within the organization.

• *KPIs*:
  – Testing of individuals who received training
  – Number of information security incidents before and after training solutions have been put in place
  – Input from feedback loops
  – Feedback from employees, partners and customers

Program Governance

• Role: The program governance function provides controls and measures for all of the functional elements within the organization. This ensures that the program is effective in meeting its objectives and goals. It also provides the tactical and strategic administrative functions for the information security organization. These include competency models for staffing of each functional element, organizational structure, performance evaluations, and goal establishment and measurement.

The program governance element also is responsible for the definition of future requirements for the information security organization as well as the management of the life cycle of current capabilities. This element is responsible for the seamless introduction and integration of new elements to the organization as well as the end-of-life activities for elements that are no longer benefiting the program and/or organization.

• *KPIs*:
  – Ability for the organization to achieve regulatory compliance with minimal investment
  – Number of information security incidents
  – Costs associated with information security activities
  – Time to identification and remediation of information security-related events

Architecture and Design

• *Role:* The information security architecture and design element represents the technological aspects associated with information security for the organization. This element is responsible for the development of reference security architectures. These architectures are designed to provide the minimum technological security requirements necessary to

provide an appropriate level of security for the solution to which they are applied.

The information security architecture and design element is also responsible for the design technological information security controls for business solutions. These controls should be business-enabling and transparent to the user community, whenever possible, but must ensure the confidentiality, integrity and availability of information for the organization.

This element also plays an integral part in the development of business applications and solutions. It is responsible for providing information security technology, methodology and process guidance to the solution development groups. The architecture and design element constitutes a knowledge base for these groups as well as an invaluable resource for guidance on how to improve the security of current legacy solutions that exist within the organization.

The architecture and design element is also responsible for evaluating new technologies that are introduced into the organization's information infrastructure from an information security perspective. This element evaluates the risks and benefits that are introduced by the technology and provides this information to the threat analysis element. It is also responsible for the design of appropriate controls to mitigate the risks that have been introduced.

- *KPIs*:
  - Number of information security events related to improper technological controls
  - Impact of security-related events on business operations
  - Impact of suggested or mandated design requirements on user experience
  - Number of reference architectures produced

Technology Capability and Evaluation

- *Role*: The technology, capability and evaluation role serves as a certification and accreditation element of the information security program. This element reviews the technological elements of the information infrastructure that is already in place to evaluate the capabilities and risks associated with information security. This evaluation is designed to ensure that the configuration and design specifications that were prescribed by the architecture and design element have been properly implemented in the operational environments.

  This element also monitors the technological elements of the information infrastructure for its alignment and compliance to the organization's information security policy. It will do this by performing periodic reviews of the technology being utilized to ensure that it still meets the information security standards and guidelines approved for use within the organization. The results of these reviews are provided to both the threat and vulnerability assessment and vulnerability management elements of the program to allow them to include this information in their evaluation of threats and vulnerabilities that exist within the organization's information infrastructure.

  The technology capability and evaluation element will also be responsible for evaluating new technologies that are introduced into the organization's information infrastructure from an information security perspective. They will evaluate the risks and benefits which are introduced by the technology and provide this information to the Threat Analysis element. They will also be responsible for the design of appropriate controls to mitigate the risks which have been introduced by the new technology.
- *KPI's*:
  - Number of security events
  - Number of control exceptions applied for and granted
  - Accuracy of data analysis compared to actual events and activities
  - Percentage of information infrastructure technologies evaluated

Key Performance Analysis and Effectiveness

- *Role*: The key performance analysis and effectiveness element utilizes measurements gathered from controls and key performance indicators to analyze the effectiveness of the information security program and its associated activities. This element provides the governance role with key data points to assist it in attaining constant improvement for the program. It also provides data points to the oversight board members to allow them to make a more informed opinion about the effectiveness of the program and provide appropriate guidance for future activities.

  The element also creates transformation plans with the governance element to increase operational effectiveness within the program. It does so by using the metrics it gathers to create objective baselines and then works with the governance element to create transformation plans based on improvement goals against the baseline metrics that have been established. These transformation plans can include adjustments to, or the introduction of, technology, process, procedures and standards.
- *KPIs*:
  - Number of security events
  - Number of control exceptions applied for and granted
  - Accuracy of data analysis compared to actual events and activities
  - Adoption of processes, procedures and standards defined in the transformation plan as business-as-usual activities

Information Security Oversight Board

- *Role*: The information security oversight board is comprised of representatives from all aspects of the organization and is designed to provide a check-and-balance mechanism for the information security program. This element's primary function is to provide guidance and direction for the information security program. It also ensures that the program's activities align with the goals of the organization.
- *KPIs*:
  - Consistency of the representation of all organizational elements
  - View of the information security program by organization and external influencers
  - Ability to easily integrate with business-as-usual functions within the organization

Organizational Interactions

- *Role*: The organizational interaction element provides a communication channel between the information security program and specific elements within the organization that require direct interaction beyond that provided through the communication and education function. This is to ensure that the information security program and its goals and objectives are represented appropriately in key organizational activities. The organizational interaction element also provides a check-and-balance mechanism and feedback loop for the program to ensure that it is aligning with the business goals of the organization. By having constant and meaningful interactions with key business functions within the organization, the program can understand what it is doing well and what it needs to improve to be a business-enabling function within the organization.

  The following is a list of organizational interaction categories that are suggested for a successful implementation of the functional element. This list is a guideline and should be adjusted based on individual organizational goals and structure:
  - Legal (office of general council)
  - Vendor and partner management
  - Privacy (chief privacy officer and/or privacy office)
  - Business units
  - Operations linkage
  - Audit/global compliance
  - Human resources
  - Change management
  - Physical security
- *KPIs*:
  - Ability to effectively communicate with other portions of the organization
  - Awareness of information security requirements and information in key organizational elements
  - Confidence of organization in information security capabilities and operations
  - Number of security-related incidents

Final Thoughts

With the increased regulation of the information infrastructure, the need for an information security program becomes more apparent. Regulations are put in place to ensure that baselines of activities are being carried out by organizations to protect consumers and the public at large. These regulations are typically based on, and measured against, industry leading and best practices. By implementing an information security program, an organization will be well suited to be in compliance with current and future regulations, since the program prescribes alignment with industry best and leading practices and, in some cases, develops such practices.

To reach the goal of transforming security incidents into operational anomalies, a structured, measurable and mature business model must be in place within an organization. Information security has matured from a concept that is dealt with technologically and is event-driven, to one that is approached from a business perspective and is process-driven. The information security program is the best approach to reach these goals.

John P. Pironti, CISA, CISM, CISSP
is an enterprise solutions architect and security consultant at Unisys. In this position, he has designed and implemented enterprisewide electronic business solutions, information security programs, and threat and vulnerability management solutions for key customers including American Express, Boeing, Citizens Bank, Embraer Aircraft Corporation, Microsoft, Scudder Kemper Investments, Sun Microsystems and Starwood Hotels. Pironti is a published writer and a frequent speaker on electronic business topics at domestic and international industry conferences. Before joining Unisys, he was the enterprise solutions architect and security consultant for Genuity Inc.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.