Developing Metrics for Effective Information Security Governance

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

Information security governance has become an essential element of overall corporate governance activities. To facilitate effective governance of an organization's information security activities, business-aligned metrics and measures need to be developed, implemented, monitored and reported to management. This ensures that the risk management and business goals of the organization are being met and the information infrastructure of the organization is secure.

Key Performance Indicators

Key performance indicators (KPIs) are one of the most effective tools that can be implemented to measure the effectiveness of an organization's information security business processes and capabilities. When designed and implemented properly, they provide business-aligned quantitative measures of the success or failure of business processes, personnel, technology and organizational effectiveness. Information security governance-oriented KPIs provide an organization with valuable metrics and measures to help determine the effectiveness of its threat and vulnerability management capabilities and its information security program.

For example, the one overriding KPI that is constant when evaluating information security capabilities is the number of business-impacting information security events and incidents that have taken place within the defined period of measurement.

Defining the Measurement

When developing an effective measure for information security governance, it is important to always ask the question, "What is being measured?" Too often, this is lost during the measurement development process and the measures created are too complex, resulting in ineffective measures. When defining the measure, it is also important to define the boundaries of its success or failure. Every measure must have a clearly defined acceptable, unacceptable and excellent range of values that can be easily identified by the audience to which the measure is communicated. This can assist in the reporting process and allow the intended audience to understand the scope for the measurement.

For example, when evaluating the effectiveness of a network firewall, the scope can be defined as interest in understanding its operational characteristics, such as uptime and performance, or whether this technology adequately protects the business process it purports to protect given current threat analysis information.

Know the Audience

Measurements are made to provide insight and information to specific audiences about specific information. When developing measures for information security governance activities, it is essential to understand and appreciate the audience to which the measures will be communicated. Different audiences have different interests in the types and frequency of information that is communicated by a measure. If a measure is communicated to an inappropriate audience, it is ineffective and potentially may cause confusion and unwanted business impacts for the organization that is being measured.

For example, the senior leadership of organizations typically has less interest in technical measures and more in measures of the risks and costs associated with information security activities to business impact. Alternatively, operational elements of an organization typically have more interest in technological measures to understand the effectiveness of their service delivery capabilities.

Keep It Simple and Consistent

One of the most effective ways to create, measure and communicate metrics is to follow a very straightforward methodology: keep it simple. Too often, organizations overcomplicate the concept of metrics and measures in an attempt to gain granularity and credibility for these metrics. The most effective measurements are those that are easily recognized and comprehended by the audience for which they are intended. This is not to say that the metrics used should not have granularity and substance. The key to success in this area is to ensure that the metrics and measures being developed are focused, and their value is easily recognizable and apparent to the intended audience.

For example, a trend analysis graph that shows the total number of information security incidents measured within a defined reporting period compared to the previous reporting period is more effective for senior management than a detailed report for each identified incident.

Consistency is also essential to the success of any measurement concept. To ensure that the metrics and measures developed and implemented are effective, they must be collected and reported in a consistent fashion. This ensures that they have business value and can then be considered by third-party independent reviewers to be unbiased and to have integrity. This also allows trend analysis activities to be performed that show historical evidence to be used as KPIs.

Consistency is especially important in compliance reporting. Regulators and auditors often cite that consistency in processes they evaluate is of the utmost importance. Even if the

organization is acting in a less-than-ideal fashion, if it is doing so consistently, this is considered a positive point, because the organization can then improve its activities consistently as well. The measures that will become the KPIs for these reviews must be consistent in their development, implementation and reporting to be utilized by external parties for demonstrating compliance to policies and/or regulations.

For example, access control logs for critical information infrastructure elements are reviewed weekly, and inconsistencies or anomalies are documented and reported to business process owners in a timely manner.

Business Goal Alignment

When developing metrics and measures, it is important to align them to the business goals of the organization. An effective metric or measure must provide a benefit to the business it supports. When developing a framework of metrics and measures, it is important to work with business leadership and process owners to understand their business processes, and what is important and vital to their success.

One of most effective ways to accomplish this is to use process flow diagrams and business intelligence tools to produce visual representations of business processes and activities. This information allows the key areas of importance of business processes to be clearly understood. These key areas then become the focus of the measurement and metric development activities.

It is important to recognize that the motivation behind development of metrics and measures for information security governance is risk management. These metrics and measures help organizations identify where, and to what degree, their business processes and business activities are at risk. They can make appropriate risk management decisions based on this information to adequately protect the business process.

For example, availability and user experience are two KPIs that business process owners often use to assist them in their activities. Providing metrics that depict the impact of security controls on these business processes will help them make appropriate and educated risk management decisions.

Baseline Framework of Metrics

It is important to establish a baseline framework of metrics for which measurements will be developed, and then be willing to add or remove measurements as the threats and business requirements of the organization evolve and change. This framework should include the people, processes, procedures, compliance activities and technology involved with information security activities. It should also include one overriding metric that is included in all categories and subcategories: the value provided by the service or control vs. its cost to the business process or organization. This cost should be presented in terms of a monetary impact to the business whenever possible, but can also be represented in the cost of labor, addition of complexity to the business process or impact on the user experience. This measure is extremely important when reporting information to management teams and business process owners since it represents information in a format they can easily recognize and understand.

For example, see the information security governance baseline framework shown in **figure 1**.

Once the baseline framework has been established, subcategories can be populated for each of the elements to account for audience- and concept-specific metrics that are developed (see the example in **figure 2**). These categories should include organizational and performance, operational and technological, business process, business value, and compliance metrics. Each of these metric categories has individual requirements and benefits to the business process owners as well as the entire organization.

Organizational and Performance Metrics

When developing metrics and measures to evaluate the performance and effectiveness of the information security program, it is important to make sure that the functions to be measured are well defined and easily understood. For example, it is important that the threat and vulnerability analysis function be separated from the vulnerability management and incident response function in the information security program, because the vulnerability management and incident response function has operational responsibilities while the threat analysis function typically does not.

Organizational metrics and measures should be designed to evaluate whether particular functions are meeting the business goals of the organization as well as the goals established for the information security program. Organizational goals should include specific measures of the effectiveness of a particular function in providing information infrastructure protection while still enabling the business to function efficiently and effectively. The key to organizational metrics is the assignment of goals to individual functions and the personnel associated

Figure 1—Baseline Metrics Framework

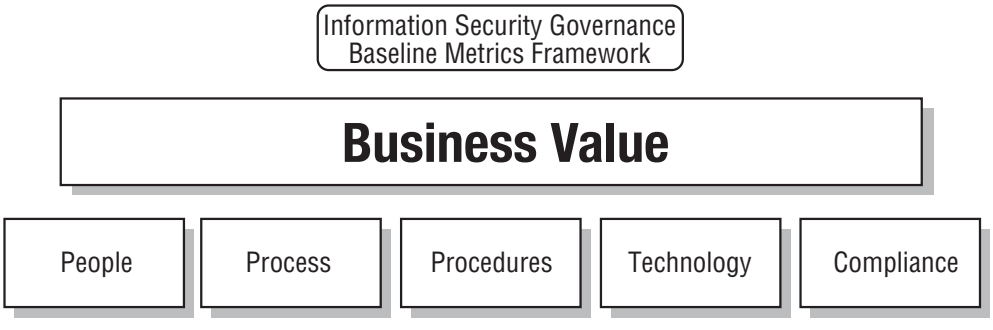
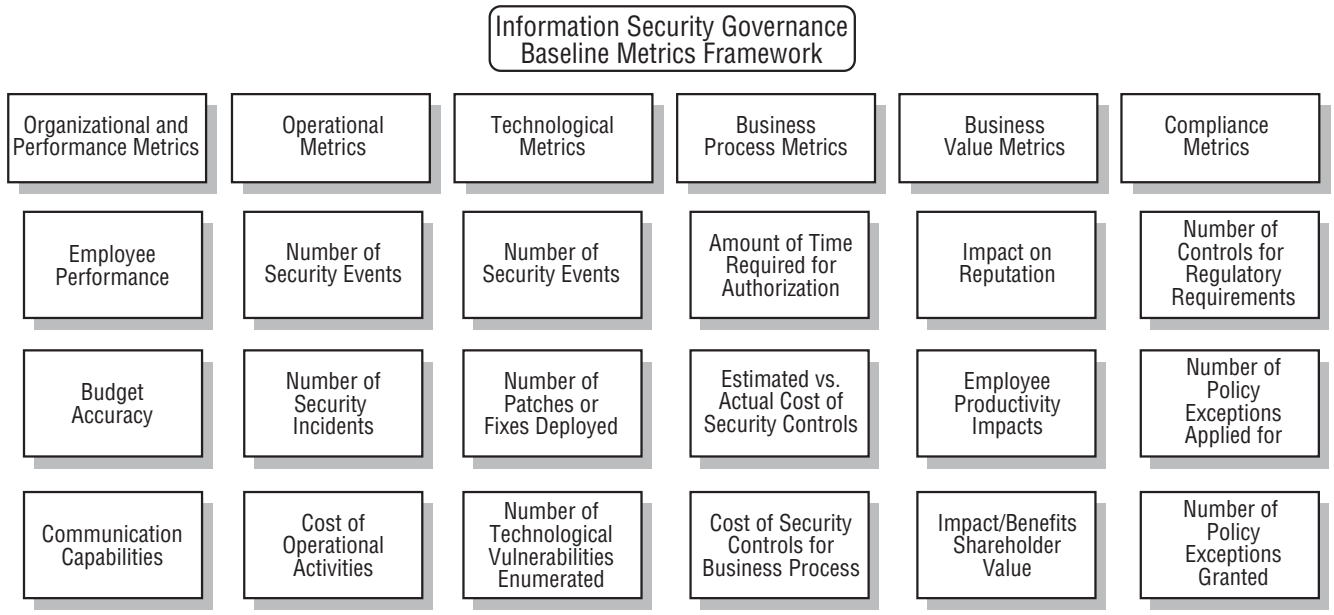


Figure 2—Sample Metrics Framework



with these functions. Once these goals have been established, accurate measures of the success or failure of the function and personnel to meet these goals can be measured and utilized as a KPI.

For example, a key organizational and performance metric is to measure how effective the information security organization is at communicating information and its capabilities to the enterprise. This metric can be measured by annually polling product and program management individuals within the organization to see how much of the information that has been communicated to them over the year from the information security organization has been retained and utilized to enhance the security of the information infrastructure elements they oversee.

Operational Metrics

Operational metrics evaluate the effectiveness and capabilities of security controls that have been designed and implemented to protect information infrastructure. All key controls (or controls that have significant value in protecting business processes) should have measurable values associated with them, or they may not be effective. Without the ability to measure the effectiveness of controls, an organization cannot mature these controls or recognize when they are no longer effective.

Operational metrics are typically associated with the effectiveness of the controls that are being used and their impact on business activities. These measures can range from personnel effectiveness to the performance and health of equipment utilized in the control framework. Operational metrics should also include measures that gauge the ability for the operational elements of the organization to introduce countermeasures and new controls to counteract evolving and emerging information security threats.

An example would be the number of information security-related malicious activities for which an intrusion detection or security event monitoring system accurately accounted within the measurement period.

Technological Metrics

Technological metrics provide insight into the effectiveness of technological controls that are deployed. Information security technology is an essential tool that is often utilized as a risk management control within an organization. The attack methods that technological adversaries utilize to compromise an information infrastructure is constantly evolving and maturing. It is important to measure the effectiveness of the technology, as it has been deployed on a regular basis to ensure that it is still effectively providing the intended protective capability to the organization or business process.

An example would be the number of spam messages that a spam e-mail filtering tool was successfully able to block in a given period of measurement.

Business Process Metrics

Business process metrics associated with information security governance are related to the impact of information security activities on the success or failure of a particular business process, as well as the business activities of the organization as a whole. To understand what measures to implement to effectively monitor the information security controls associated with business monitoring, the business model or process and its associated threats must first be understood.

The most effective way to understand the business process that is being measured, the effectiveness of the controls that it utilizes and its potential threats is to create visual process flow representations of the business process and its dependencies. These flows allow the data that it utilizes to be easily tracked

as they pass through the business process. They also establish behavior patterns for data-related activities, which can be monitored for anomalous activities that can represent threats. Most important, it will allow the viewer to easily relate the business value and benefits of the business process to the organization.

When presenting information associated with business process metrics to business management, it is important to represent these values in currency valuations whenever possible. Since most business managers are interested in profit and loss activities, this is the most effective way of communicating the significance of the measures to them. This also allows risk management investment decisions to be made more easily, since the return on investment can be more easily calculated.

An example would be the estimated vs. actual material and operational costs associated with the introduction of strong authentication or complex passwords into a customer self-service web environment.

Business Metrics

Business metrics represent the direct impact of information security activities on the business. These metrics speak to macro-level areas that represent external and internal perceptions as well as actual activities that have a direct impact on the performance and success of the organization. Business metrics are typically the areas in which business leaders are most interested and focused. These metrics typically have a direct correlation to shareholder value, market perception and, most important, the profit and loss of the organization. To develop appropriate business metrics associated with information security activities, it is important to interact with the members of the organization's leadership team to understand the areas that they are most interested in tracking and measuring. This ensures that expectations are being met and the reports that are generated are most effectively utilized.

An example would be the number of negative public media items associated with information security that have been published about the organization.

Compliance Metrics

The measurement of controls associated with compliance activities has become a key area of interest for many organizations. Regulation has caused many new controls and information infrastructure protection concepts to be introduced into business processes. Regulators and auditors are interested in ensuring that these controls are effective in protecting physical and logical assets within an information infrastructure, as well as meeting regulatory and compliance requirements. To satisfy regulatory agencies and auditors, it is important to identify with them the specific information security-related controls that they are interested in and then provide them with measures of the effectiveness of these controls. This allows an organization to minimize the impact of regular audit activities by having consistent reports and measures that they can provide to these individuals and organizations to demonstrate their current state of compliance.

An example would be the time elapsed between the recognition that an employee's access to an information resource is no longer authorized and the time his/her access to this resource has been revoked.

Meaningful Reporting

Metrics are only an effective tool if they are accurate in their measurements and beneficial to the organization. Meaningful reporting is the key to the success of any metric framework or solution. If the metrics and their value are not easily understood and digested by the intended audience, they are considered ineffective and are viewed negatively.

Different audiences have different requirements and varying interests in the measurements that are gathered and reported. By aligning reporting strategies to the various types of metrics themselves, there is a higher probability of utilization by the intended audience. For instance, a business process owner is most interested in the impact of information security controls on the business process, but is less interested in the technical or operational elements of the controls themselves.

A tiered reporting model is an effective way of presenting information to different audiences within an organization. At the top tier, senior leadership is most interested in high-level, risk-oriented information that provides insight into costs and benefits associated with information security activities and information infrastructure protection.

The middle tier is most likely focused on communicating information to business process owners and managers. These individuals are typically most interested in measures of effectiveness for controls that have been put in place, as well as their impacts on the ability of the business process to operate efficiently.

The lowest tier of the model typically includes operational elements for stakeholders who are interested in understanding the details of the measures and their associated outputs. These individuals are typically charged with the operation of the controls and are most interested in ensuring that defined controls have been implemented appropriately and are functioning within established boundaries.

Trend analysis is an important element of effective reporting of metrics (see the example in **figure 3**). It is important to provide baselines for the established measurements and then present the results of the newly generated measurement activities compared to these baselines. This allows the organization or the individual reviewing the reports to understand whether the information security capabilities being supplied are providing positive or negative business value to the organization or business process over a period of time.

Benchmark Reporting

Management and leadership teams often request that reports be presented to them that benchmark the performance of their organization to the performance of peers and competitors in the same industries. The information used to provide this reporting can be gathered through publicly available surveys, individual data-gathering activities, or analysts or third-party consultants. The most effective way of representing these data is the use of radar or "spider" charts, which map key data points of an organization and then overlay the data points gathered about other organizations or industry benchmarks.

Figure 3—Business-impacting Information Security Events

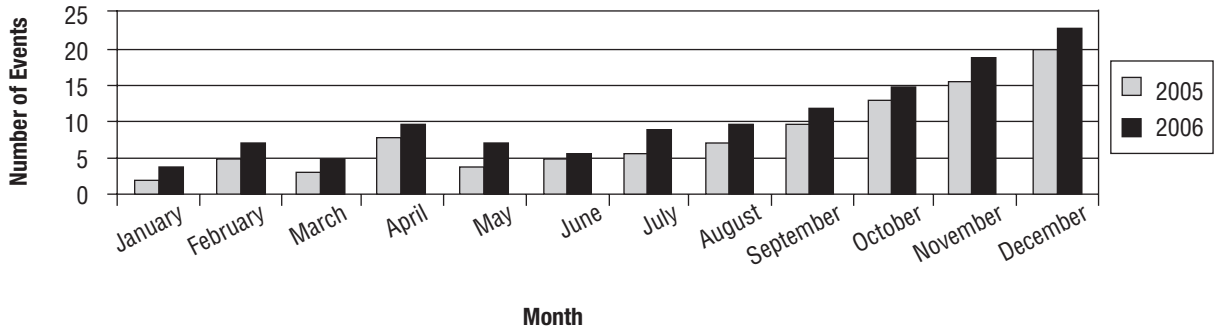
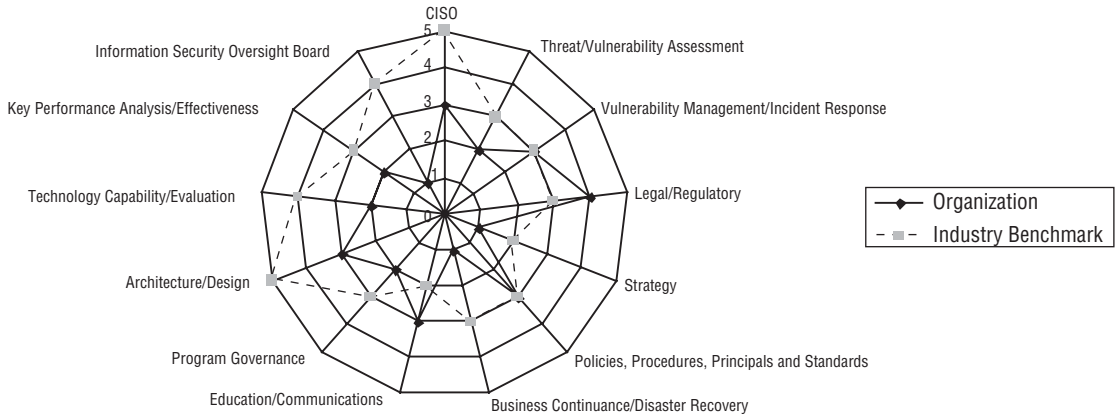


Figure 4—Information Security Program Functional Inventory Capability Maturity Model



See the example in **figure 4**. This allows the viewer of the chart to immediately understand where there are commonalities and where there are differences in capabilities and performance between the organization and the benchmark that has been represented.

Final Thoughts

Information security is an ever-changing and evolving activity. To have accurate visibility to these changes, an organization must establish, maintain, monitor, interpret and report effective metrics and measures. The threats that an organization's information infrastructure faces, along with the controls and capabilities that must be deployed to counteract these threats, are constantly changing and evolving. This requires the measures and metrics that are employed to monitor the performance of information security governance to be adaptable and flexible to be a positive and valuable asset to the organization. Once these metrics and measures have been established, reports that effectively represent them to their intended audience in a meaningful fashion must be created and presented to management. Otherwise, misleading information is recognized, ineffective information security controls are utilized, and the organization is put at risk.

John P. Pironti, CISA, CISM, CISSP, ISSAP, ISSMP is the chief information risk strategist at Getronics. 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 on a global scale. He is also a published author and writer, and a frequent speaker on electronic business, risk management and information security topics at domestic and international industry conferences. He can be contacted at *John.Pironti@getronics.com*.

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*.