

Information Risk Management**Patrick A. Morin, CPA, CISM**

Organization managers have been facing risk management issues and included it as part of sound business practices for years. More recently, regulations, such as Gramm-Leach-Bliley and Sarbanes-Oxley, have included an information risk management process as part of their compliance requirements. The results of risk management activities are also required when an organization is undergoing business continuity planning.

Information risk management is the ongoing process of identifying information assets; evaluating the corresponding threats and controls; and implementing appropriate responses. Organizations typically consider information systems; however, for proper risk management all types of information assets must be included – both electronic and non-automated. Risk management is an iterative process and should be performed on a scheduled basis and whenever an organization has undergone substantial changes to information assets, systems, or controls.

Business leaders should go beyond the minimum compliance requirements and view risk management as an effective business tool. Risk management can help organizations ensure that management is aware of the risks their organization faces, that adequate control resources are allocated according to risk, and that adequate control systems (technology and people) are in place to mitigate risks. Risk management can also serve as an opportunity to centralize controls and streamline certain procedures.

Risk Management is not an event, it is a process. Effective risk management requires an on-going commitment from the organization leadership. All too often, risk management falls on the information systems (IS) department to implement. Risk management is a team activity and should begin by forming a risk management committee. The committee should include representatives of management, user departments, and the IS department. The risk management committee should divide the information activities (such as production and payroll) among the functional areas of the organization and should involve representatives from the respective departments in the asset identification process.

The three major components of a risk management program are: performing a risk assessment to identify the organization's information assets and the threats to each asset, identifying and implementing controls to mitigate the threats, and evaluating the controls to assess their effectiveness.

Risk Assessment

The risk management committee should begin by identifying the organization's information assets. Information assets include information systems and the data they contain, records and documentation, and people. The criticality of each asset should be determined by the committee based on a pre-defined scale (such a critical, high, medium, or low). The committee should consider the organization's legal requirements when quantifying criticality. The criticality of each asset will determine the level of controls that are required.

For each information asset, the committee should consider any methods used to Access, Collect, Store, Use, Transmit, Protect, and Dispose of the information. The committee should complete a risk assessment exercise for each information asset to identify and enumerate the foreseeable threats for each method, and for each applicable method, the committee should further consider any threats that impact the asset's Confidentiality, Integrity, and Availability. Then each threat should be evaluated by the committee based on the probability of occurrence (high, moderate, or low). Within each asset, the threats with the highest probability of occurrence require the strongest controls.

In order to maintain the integrity of the assessment process, the committee should organize the risk assessment records according to the respective information assets. The documentation should cross-reference to the respective systems that could impact the asset.

The risk management committee should prioritize their activities for identifying and implementing controls and evaluating control effectiveness based on the criticality of the assets and the probability of the threats. The most critical assets and the highest probable threats should receive the most attention.

Controls

Once the risk assessment has been completed, the risk management committee should identify the existing controls for each identified threat. The committee should identify and document any existing (or newly implemented) controls that mitigate or eliminate the corresponding risk. In places where the organization does not have controls, the committee should develop and implement new controls.

Control Evaluation

Based on the controls identified for each threat, the committee should assess whether the controls sufficiently reduce or eliminate the risks associated with the threat. The organization should develop a control testing and monitoring plan to test each control identified. The committee may determine that additional controls are required. When weak or missing controls have been identified for specific threats, the committee should plan and implement procedures to expand or develop missing controls. Once these controls are implemented they should be evaluated following the same control evaluation process used on the existing controls.

Ongoing Activities

Once the initial risk assessment has been completed, the risk management committee should develop a schedule for re-performing the assessment activities. The schedule should be based on the criticality of each information asset and should include opportunities for expanding the list of information assets.

At a minimum, controls should be retested on at least an annual basis; complex controls should be tested more often. Further, each critical information asset should be re-evaluated on a semi-annual basis and low priority assets on a biannual basis. All information assets should be re-evaluated whenever there has been a significant change to the systems, records, or people that comprise that asset. Software tools can assist business leaders in performing a risk assessment, but software cannot replace sound risk management processes.

The committee should maintain a centralized record of risk management activities. The risk management process is typically evaluated with equal importance to the risk management results when critiqued by internal and external auditors, regulators, and other evaluation groups. The risk management record can also be used to quantify risk management results.

Patrick A. Morin, CPA, CISM is the Director of Baker Newman Noyes' Information Technology Consulting Division. For more information about Risk Management, please contact Pat at (207) 879-2100 or pmorin@bnn CPA.com.