Why Perform a Security Risk Assessment?

Organizations have many reasons for taking a proactive and repetitive approach to addressing information security concerns. Legal and regulatory requirements aimed at protecting sensitive or personal data, as well as general public security requirements, create an expectation for companies of all sizes to devote the utmost attention and priority to information security risks. An IT security risk assessment takes on many names and can vary greatly in terms of method, rigor and scope, but the core goal remains the same: identify and quantify the risks to the organization's information assets. This information is used to determine how best to mitigate those risks and effectively preserve the organization's mission.

Some areas of rationale for performing an enterprise security risk assessment include:

- **Cost justification—**Added security usually involves additional expense. Since this does not generate easily identifiable income, justifying the expense is often difficult. An effective IT security risk assessment process should educate key business managers on the most critical risks associated with the use of technology, and automatically and directly provide justification for security investments.
- **Productivity—**Enterprise security risk assessments should improve the productivity of IT operations, security and audit. By taking steps to formalize a review, create a review structure, collect security knowledge within the system's knowledge base and implement self-analysis features, the risk assessment can boost productivity.
- **Breaking barriers—**To be most effective, security must be addressed by organizational management as well as the IT staff. Organizational management is responsible for making decisions that relate to the appropriate level of security for the organization. The IT staff, on the other hand, is responsible for making decisions that relate to the implementation of the specific security requirements for systems, applications, data and controls.
- **Self-analysis—**The enterprise security risk assessment system must always be simple enough to use, without the need for any security knowledge or IT expertise. This will allow management to take ownership of security for the organization's systems, applications and data. It also enables security to become a more significant part of an organization's culture.
- **Communication—**By acquiring information from multiple parts of an organization, an enterprise security risk assessment boosts communication and expedites decision-making.

The enterprise risk assessment and enterprise risk management processes comprise the heart of the information security framework. Depending on the size and complexity of an organization's IT environment, it may become clear that what is needed is not so much a thorough and itemized assessment of precise values and risks, but a more general prioritization.

Security risk assessment should be a continuous activity. A comprehensive enterprise security risk assessment should be conducted at least once every two years to explore the risks associated with the organization's information systems. An enterprise security risk assessment can only give a snapshot of the risks of the information systems at a particular point in time. For mission-critical information systems, it is highly recommended to conduct a security risk assessment more frequently, if not continuously.