@ISACA
RELEVANT, TIMELY NEWS
3 March 2010

10 Tips for Developing an Information Security and Risk Management Strategy

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

Developing an information security and risk management strategy can be a challenging activity even for the most seasoned leader. Consider these 10 tips on what to account for in your development activities:

1. Understand the enterprise's current business conditions, risk profile and appetite before you begin to develop capabilities. An enterprise's financial status is a key performance indicator (KPI) of its current business conditions. If the enterprise is conservative, delay the implementation of enhanced capabilities. If it is in a growth state, demonstrate the business value of introducing robust capabilities.
1. Develop a prescriptive annual strategy, followed by a rolling, three-year plan that includes frameworks, goals and objectives.
2. Clearly identify the point of arrival for the strategy based on management guidance and input at the onset of the strategy development.
3. Ensure both the availability and capabilities of staff necessary for the execution of your proposed strategy. Do not assume you will be able to add staff or use part-time staff from other organizations for baseline capabilities.
4. Develop KPIs based on points of arrival for your strategy and program that you have agreed upon with the enterprise's leadership team.
5. Make sure you have acceptable and unacceptable thresholds established for KPIs that include enforceable consequence management. A laddered approach to consequence management often is the most successful and should be based on risk and business impact.
6. Convene oversight boards that include business leadership and key stakeholders, to meet on a monthly or quarterly basis. Key metrics and requests for approval of program activities should be presented at these meetings.
7. Be aware that threats and risks can vary significantly based on geography. Physical threats to information tend to be less probable in developed nations and

environments, due to the intention to steal data instead of infrastructure.

8. Examine socioeconomic data for regions within which the enterprise operates to understand cultural and economic considerations that can impact strategy development and execution.
9. Utilize capability maturity assessments and benchmarks of processes and capabilities to identify areas that need more focus than others for future strategy development and investment.

Developing an information security and risk management strategy is a fluid process that needs to constantly adapt to business conditions and requirements. The most successful strategies are those that can quickly adapt to change and align with adjustments in business activities and changing business conditions.

John P. Pironti, CISA, CISM, CGEIT, ISSAP, ISSMP, is the president of IP Architects LLC.