@ISACA
RELEVANT, TIMELY NEWS
Volume 16, 1 August 2012

Five Recommendations For Your Information Risk Management and Security Strategy

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

The strategy associated with an enterprise's information risk management and security (IRMS) program becomes a road map for its activities. When developing or refreshing your IRMS strategy, there are many considerations that should be accounted for to make sure it is beneficial to your enterprise and plausible for implementation and ongoing success. Here are five things to consider when undergoing this effort:

1. **Validate your strategy with your intended audiences early in its development**—The key to any successful strategy is the positive perception and realization of its value by the people it will impact. Too often IRMS professionals assume they intuitively understand their enterprise's requirements and expectations, as well as the benefits that will be obtained by implementing their proposed strategies. While this may be the case, it is important to validate these assumptions with the customer of the strategy to ensure they agree. Without their support the strategy will have little chance of success. The easiest way to achieve this validation is to socialize the concepts and ideas that you intend to include in your strategy with key leaders and stakeholders early in the development process. If they are involved in shaping its development and agree with your views and approach, there is a much higher likelihood of successful execution.
2. **Align the IRMS strategy with your enterprise's information risk profile—**An enterprise's approach to IRMS should be about information risk first and security second. When developing your IRMS strategy, make sure you align your programs and activities with your enterprise's information risk profile. This profile will identify the information risk appetite of your enterprise. A risk-based strategy presented to a sponsor or leader has a high probability of gaining support since it is designed to align with needs and expectations. If your enterprise does not have a formal information risk profile, seek out the individuals who have risk management responsibilities in the enterprise (i.e., finance, legal, compliance) as well as business process and data owners to work with them to identify their information risk appetite and expectations of security to create a profile to support them.
3. **Leverage staff as a force multiplier—**Leaders and individual contributors associated with IRMS programs and capabilities often feel as though they are overworked and undersupported by their enterprises. One approach that can help to

ease this pain is to plan in your IRMS strategy to leverage your enterprise's overall staff as a force multiplier. One strategy that is often successful is to identify individuals who will be tasked as IRMS champions within the key functions and services within your organization. By empowering these champions with knowledge, capabilities and expectations, they can assist you in meeting your IRMS objectives without having to significantly expand the budget or staffing of your program. Beyond the establishment and support of champions, the creation of a risk-conscious and security-aware culture within your enterprise can provide an effective force multiplier for your efforts as individuals incorporate IRMS as a business as usual activity.

4. **Consider current and projected business conditions—**Current and projected economic and business conditions can have a distinct impact on ISRM strategy development. If your enterprise is currently or projected to contract or operate in an extremely cost-cautious manner, develop a strategy that accounts for this situation. Even when considering areas such as compliance, where many ISRM professionals assume their organizations will have to invest to ensure alignment, it is important to identify contingencies in cases where they are unwilling or unable to do so.

   Alternatively, if your enterprise is currently or plans to be operating in a business growth and expansion mode, this is an ideal time to invest in programs and capabilities that will ensure alignment with business needs and expectations. When developing strategies in either scenario, it is important to identify and validate the business value of your proposed strategy to gain the support of your enterprise's leadership and program sponsors.
5. **Ensure the strategy can be implemented and operate successfully with your existing budget and resources—**A common mistake made in the development of IRMS strategy is to assume that enhanced funding will be provided or sustained as part of its execution. Business conditions and information risk appetites of organizations can change quickly. IRMS can be an easy target for budget and resource adjustments. If the foundation of your strategy is based on the use of your current budget and resource allocation, your ISRM program and its capabilities will be more resilient during these types of fluctuations. Components of your strategy that require expanded budget and staff should be developed as modular initiatives whose business value can be clearly understood and monitored, but also easily adjusted if business conditions change

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