@ISACA
RELEVANT, TIMELY NEWS
Volume 9, 27 April 2011

5 Considerations When Evaluating ISRM Programs and Capabilities

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

The following are 5 key items to consider when evaluating information security and risk management (ISRM) programs and capabilities:

1. **Does a defined and business-endorsed strategy exist?** It is important to assess whether an organization has developed and implemented a formal strategy for the ISRM program, that associated capabilities exist, and that the strategy has been documented and approved within the organization. A comprehensive strategy will include, at minimum, the following key elements:
   - Comprehension and acknowledgement of current business conditions
   - Governance models that will be utilized
   - Alignment with the organizational risk profile and appetite
   - Budget considerations and sourcing plans
   - Metrics and measures
   - Communication and awareness plans
2. **How effective are the methods and practices for threat, vulnerability and risk assessment?** The methods and practices that are used as part of ISRM programs and capabilities to evaluate threats, vulnerabilities and risks should be consistent, repeatable and easily understood by their target audiences. These methods and practices should minimally include the following components:
   - Business process mapping
   - Asset inventory and classification
   - Threat and vulnerability analysis methodology
   - Risk assessment methodology
   - Intelligence gathering, processing and reporting capabilities
3. **What is the approach to compliance?** Compliance has quickly become an integrated part of any ISRM program or capability within an organization. There are numerous external regulatory, legal and industry standards and internal policies with which organizations need to be compliant to meet their compliance goals. Ideally, compliance should be considered a starting point and not an end

point of ISRM capabilities. Unfortunately, many organizations have adopted an approach called “security by compliance,” which is not only a sign of immaturity, but also may make them vulnerable to a significant number of business-impacting threats and may expose them to a wide range of risks for which they may not properly account.

4. **How are metrics and measures utilized?** Metrics and measures are often used by organizations to evaluate the capabilities of their business units and functions. ISRM programs and capabilities have become more engrained within organizations as independent business functions and business units, instead of as elements within technology programs. The need for these programs and capabilities to demonstrate and monitor their business value to their constituencies, including the organizations that they serve, has become a critical consideration in organizations’ operating strategy. The metrics and measures associated with ISRM capabilities should demonstrate a focus on the value provided and the efficiency of their functional capabilities.

   Each key metric or measure (collections of multiple metrics and measures or are considered critical to the success of the organization) should also include thresholds with associated actions or activities. Metrics and measures without thresholds do not provide insights into the values they produce. Thresholds can be as simple as a notification or as complex as a trigger for a series of actions and activities that will be executed once met. The intended audiences that will be required to take an action or will be impacted by an action once the threshold is achieved should be able to easily understand the business need or justification for the action and understand the value provided to the organization.

5. **Does the program use an operational or consultative approach?** Information security and risk management programs can include operational components as part of their core capabilities or can operate in an advisory and consulting capacity to the organization. If operational components are included, there should be a clear definition of expectations of the operational responsibilities and how they differentiate from other operational capabilities within the organization. There also should be documented processes and procedures for sharing information related to operational effectiveness, requirements, intelligence and incident-response activities.

   If the approach is purely an advisory and consultative approach, the services that are provided to the organization should be clearly documented, as should the level of effort and interactions with the business that will be required for the services to be successful. Providing guidance and advice without operational responsibilities often allows an ISRM organization to be viewed positively from within the organization since it is limited in its ability to prevent the organization from implementing operational capabilities to which it may not agree.

If you would like to read more about key considerations when evaluating information security and risk management programs and capabilities, look for the article of the same name in the **volume 2, 2011, issue** of the ISACA Journal or attend one of the **ISACA Information Security and Risk Management conferences** later this year.

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