Key Considerations When Evaluating ISRM Programs and Capabilities

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is president of IP Architects LLC. He has designed and implemented enterprisewide electronic business solutions, information security and risk management strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key global customers in a range of industries, including financial services, insurance, energy, government, hospitality, aerospace, health care, pharmaceuticals, media and entertainment, and IT. Pironti frequently provides briefings and acts as a trusted advisor to senior leaders of numerous organizations on information security and risk management and compliance topics and is also a member of a number of technical advisory boards for technology and services firms.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Traditionally, information security and risk management (ISRM) has often been perceived as a barrier to success and a disabling force within organizations and business leadership—instead of as a benefit and an enabling capability. This perception is typically a result of the traditional perception of technology: providing security first and using fear, uncertainty and doubt to invoke the need for security within organizations. However, a mature ISRM program and capability is an enabler to the organization and, in many cases, considered a strategic advantage in business activities.

ISRM programs and capabilities have become vital elements within most organizations as they realize the value of their data and information infrastructures. These capabilities have quickly matured beyond foundational requirements and now need to be managed and matured to ensure alignment with business expectations and activities. The accurate and continual evaluation of these programs and capabilities by examiners is critical to their success and to understanding their benefits and challenges to the organizations and constituencies they serve.

EVALUATION METHODS

There are numerous methods and practices that can be used to evaluate the ISRM program and capabilities of an organization, including surveys, interviews, artifact and evidence reviews, benchmarking, capability maturity modeling, and capability alignment with industry-recognized and industry-leading functional inventories. Independently, each of these provides value to the evaluator and the business, but by themselves, they do not provide a comprehensive perspective to all interested parties. It is often optimal to combine these capabilities and use them together to ensure that an accurate and complete view.

Using a customized version of the Capability Maturity Model (CMM) (**figure 1**) to evaluate ISRM programs and capabilities is often the most effective, comprehensive and widely recognized method. While originally developed for the software industry, CMM can be easily adapted for ISRM program and capability analysis. By adding an incrementing scale within the individual layers of the traditional CMM model, an evaluator can provide details about the maturity of an organization and capabilities that are often requested by organizational leadership and stakeholders. The incrementing scale should represent three distinct segments: .1 through .3 represent capabilities that are in their initial state of maturity, .4 through .6 represent stabilized maturity, and .7 through .9 represent progression toward the next level of maturity.

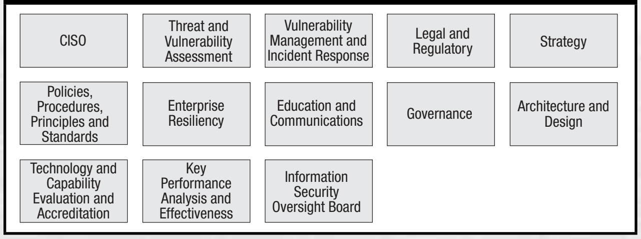
Figure 1—ISRM Capability Maturity Model

Maturity Level	General Description
5	Optimal, optimizing, business-aligned
4	Managed, controlled, predictable
3	Proactive, defined, implemented
2	Repeatable, reactive, best effort
1	Initial, undefined, *ad hoc*
0	Intent, not identified

Increment Range	Increment Description
.7-.9	Progressing
.4-.6	Stablized
.1-.3	Initial

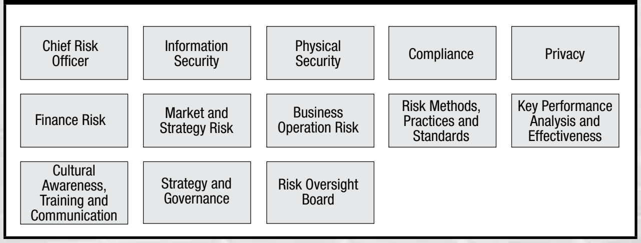
A leading way to evaluate ISRM programs and capabilities is to utilize functional inventories as a baseline for the evaluation of functions and a review of the governance models that are being used. In the case of ISRM, two functional inventories are applicable: the information security program (**figure 2**) and the information risk management program (**figure 3**). These inventories include the services and capabilities that should be evident within an organization if it has implemented comprehensive programs and capabilities.

Figure 2—Information Security Program Functional Inventory



CISO	Threat and Vulnerability Assessment	Vulnerability Management and Incident Response	Legal and Regulatory	Strategy
Policies, Procedures, Principles and Standards	Enterprise Resiliency	Education and Communications	Governance	Architecture and Design
Technology and Capability Evaluation and Accreditation	Key Performance Analysis and Effectiveness	Information Security Oversight Board		

Figure 3—Information Risk Management Program Functional Inventory



Chief Risk Officer	Information Security	Physical Security	Compliance	Privacy
Finance Risk	Market and Strategy Risk	Business Operation Risk	Risk Methods, Practices and Standards	Key Performance Analysis and Effectiveness
Cultural Awareness, Training and Communication	Strategy and Governance	Risk Oversight Board		

Once the functional inventories that are going to be used are identified, it is important to evaluate the strategy that the organization has developed for the ISRM program and capabilities to ensure that it is aligned with business expectations and requirements.

EVALUATING ISRM STRATEGY

It is important to assess whether an organization has developed and implemented a formal strategy for the ISRM program and associated capabilities, and that it has been documented and approved within the organization. A comprehensive strategy will include, at minimum, the following key elements:

- Comprehension and acknowledgment 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

Strategy is an important component to evaluate. It must be carefully considered and executed to align with business requirements and expectations.

BUSINESS ALIGNMENT AND ACCEPTANCE

The alignment of ISRM capabilities with business requirements and activities is vital to the ISRM program's success. Polling and interviewing business stakeholders and leaders about their perceptions and interactions with the ISRM organization and its functions are the leading methods for assessing business alignment. The business and other interested parties, such as external stakeholders and regulatory oversight groups (if applicable), should not only be aware of the capabilities that are provided, but also be able to derive value from the knowledge and services that are furnished. A key indicator of the lack of business alignment is the business or any interested party being unhappy with or unaware of the capabilities or services that are provided or available.

An additional consideration when evaluating business alignment is the ability of the ISRM program or capabilities to assist in the enhancement of business activities and financial position. ISRM can be used as a valuable asset to increase the confidence of current and prospective customers and partners when they are deciding to begin or enhance a business relationship with an organization. A key indicator of the existence of this capability can be found in the sales and marketing approaches of the organization. Including ISRM concepts and capabilities in messaging or communication activities shows confidence in these capabilities and acknowledges their strategic value potential.

A key indicator of business acceptance is the time in the development cycle of products and services at which ISRM programs and capabilities are engaged. Often, organizations that utilize ISRM capabilities early in their development activities find that they are able to reduce costs (often by as much as 30 percent) and increase efficiency in those capabilities. This is because the organizations integrate ISRM concepts and requirements in the design phase, not toward the end of development activities when the need to add these capabilities results in costly reengineering and adjustments.

Another key indicator of ISRM business acceptance is the number of policy exception requests that are applied for by the business and then granted by the ISRM organization. It is typical to see an increased or higher-than-normal number of exception requests (compared to existing policies) when new policies are introduced. Exceptions that are requested based on the need for more time to comply with the policies are not as critical as those that are requested as an attempt by the business to evade or avoid complying with policies. More important than the number of requests is the number of approvals that are granted for the requests. A large number of requests and approvals is a key indicator that the policies are not aligned with the business needs or capabilities.

GOVERNANCE

To function at optimal efficiency and capability, ISRM programs and capabilities require a governance plan and structure to be in place and functioning. The governance model should include the functional inventory that is utilized and an operating plan for each function. This plan should include staff and resource requirements, budget tracking, maturity and stabilization plans, a mapping to strategic business goals and requirements, and evidence of business alignment. The governance model should also clearly define the minimal and optimal operating requirements for each function and show evidence of tracking activities that demonstrate that the leadership of both the ISRM program and the business has accurate and meaningful insights into the health and performance of the program and of the services and capabilities that are provided by the program.

The reporting structure of the ISRM program is key to its ability to be effective and successful within an organization. Many ISRM programs were created as part of technology organizations and are reported on to the chief information officer (CIO). This can be an effective structure for initial capabilities, but it is often not ideal or appropriate for mature organizations. The goal of ISRM should be to protect information and the information infrastructure, which includes technology, but it should not focus on this alone. When reviewing ISRM capabilities, areas should be noted in which a conflict of interest may arise due to ISRM leadership's interaction with members of technology leadership who may not understand or support the full scope of the capabilities and requirements.

Once the governance structure has been evaluated, the next key area of evaluation should be the threat, vulnerability and risk assessment methods and practices that are used by the ISRM program to appropriately identify, evaluate and report on the key areas of risk and concern on which the business should focus at any given time.

THREAT, VULNERABILITY AND RISK ASSESSMENT METHODS

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 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

A clear distinction must exist between threat and vulnerability analysis and risk management activities within the organization. Information security professionals often mischaracterize situations that are threats and vulnerabilities as risks because the professionals recognize the technical impact without appropriately understanding or incorporating the business impact into their assertions. In most cases, information security programs and the professionals who work in them do not have the full insights of the business leadership in regard to business strategy, importance rankings of business processes and capabilities, and business intelligence to properly identify and rank risks. However, the information they provide about threats, including probability and business impact insights, is essential to the accuracy and value of risk assessments and rankings.

When evaluating ISRM capabilities, a key area of focus should be the process utilized to identify and represent risk to the organization and key stakeholders. Risk assessment, ranking and reporting capabilities should utilize and follow a structured, consistent and repeatable approach. The ISRM capabilities of an organization can provide valuable insights into the enterprise risk management (ERM) capabilities of the organization, and are often better suited to perform information risk assessments and rankings for the enterprise. ERM often does not have the maturity or knowledge to properly incorporate information risk into their assessment, ranking and reporting. Consequently, the ISRM program and capabilities should work closely with the ERM organization and associated stakeholders to understand their needs and to assist them with their activities.

MODES OF OPERATION

ISRM programs and capabilities are unique within organizations because they have proactive and reactive responsibilities. It is important to assess the ability to effectively operate in both modes. Mature programs are often more focused on proactive capabilities such as threat and vulnerability analysis, vulnerability management, training and awareness, intelligence activities, and control maturity and enhancement. Reactive programs tend to be focused on compliance activities and on responding to incidents and threats as they are realized. If an organization is focused on reactive capabilities, it is often a key indicator of immaturity and a lack of organizational focus on ISRM programs and capabilities.

When evaluating ISRM programs and capabilities, it is important to identify their charter and what they are expected to protect or what problem they are trying to solve. Typically, there are two modes of operation that are utilized. The first is a primarily reactive and technologically focused approach. This model is often found in organizations that do not have mature capabilities and/or do not derive business value from ISRM. In this case, the organization typically does not adequately fund its ISRM program, relies on these capabilities only when it is negatively impacted by an information security incident, and utilizes them as response capabilities.

The second mode of operation, a data- and business-process-focused approach, is typically indicative of a more mature organization. In this mode, the organization perceives ISRM as providing business value, will leverage these capabilities in its revenue-generating business activities, and will embrace the guidance and functions that are provided as a benefit to the organization's success, rather than as a disabling roadblock. In this mode, technology is still incorporated in the activities of ISRM capabilities, but they are more focused on business processes and data in these activities. In most cases, technology becomes a supporting element and is used to enable controls instead of being the primary focus of the ISRM activities.

Either mode of operation can assist the organization in meeting its compliance goals (internal and external, if applicable). The extent to which this should be evaluated and scrutinized will be based on the organization's approach to compliance.

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. One consideration that must be made is the organization's approach to compliance. 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, it may also 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.

Security by compliance is often an indicator of an organization's distrust or frustration with its current ISRM capabilities. Compliance requirements have provided organizations a measure by which they believe they can gauge their needs for ISRM capabilities. Again, compliance should be considered a starting point and not an end point for ISRM programs, capabilities and requirements.

A key attribute of mature and effective ISRM programs and capabilities is their ability to meet internal and external compliance requirements and goals with minimal effort as a result of their business-as-usual activities. Compliance is not treated as a separate initiative or program, but instead as an integrated component of the organization's business activities. In many cases, proof of compliance will become a data-packaging and reporting activity, with a small amount of effort required to meet specific requirements or to develop reports that may not be part of the normal business operations of an organization.

A compliance strategy should also be part of any compliance-related activities. Complete compliance may not be desirable or achievable given an organization's current business conditions or activities. In this case, it is important that a strategy and road map exist that highlight and focus on the most critical compliance requirements first, and then address other requirements based on business impact and the level of effort required to achieve the requirements over a reasonable period of time.

Along with a strategy for compliance, training and awareness activities also need to be evaluated and considered for their effectiveness. Training and awareness are essential to the concept of cultural change and critical to the success of achieving the goals of business-as-usual activities.

TRAINING AND AWARENESS

Training and awareness activities for ISRM are essential to the success of any capability or program. Training and awareness should not be limited to annual training activities or one platform (electronic, lecture, broadcasts, etc.). When evaluating training and awareness activities, it is important to determine whether the organization has identified the learning styles of its stakeholders and constituency and whether it develops aligned materials.

Training and awareness activities should allow for interactive and bilateral opportunities for learning and communication. It is important that the intended audiences have the ability to ask questions, express concerns and/or suggest ideas. Electronic means such as an internal web site with frequently asked questions (FAQs), blog posts, social media capabilities, and direct contact options with ISRM leadership and staff demonstrate an organization's commitment to working with its constituency instead of being authoritative and omniscient in its approach.

One approach to evaluate the effectiveness of an ISRM program's training and awareness capabilities is to choose employees at random and poll them about their knowledge and impression of the program. The individuals who are chosen should represent a cross-section of the organization, including individual contributors, managers and organizational leaders, and should be asked the same questions. By correlating the data obtained from polling each of these groups, a clear understanding of the awareness of the ISRM program and its capabilities can be derived by its intended constituency and documented.

Correlating data and reporting the results to business leaders and stakeholders are activities that are often associated with metrics and measures. Organizational leaders often base their opinion of the business value provided and of the effectiveness of ISRM programs and capabilities on the metrics and measures that are provided to them.

METRICS AND MEASURES

Metrics and measures help professionals 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. These programs and capabilities need to demonstrate business value to their constituencies, including the organizations that they serve. The metrics and measures associated with ISRM capabilities should demonstrate a focus on the value provided by the individual functions and services that they offer, and on the maturity and efficiency of their functional capabilities.

One of the key performance indicators of the metrics and measures capabilities of an organization is the methods and practices that are utilized for development and operation. A consistent and repeatable methodology should be used for the creation of metrics and measures and for the data gathering, analysis, reporting and threshold assignment elements. If metrics and measures are changed frequently (less than one year would be atypical), the data that are collected and reported using them may not be accurate or representative of what is being measured.

Each key metric or measure (those that are 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 positive or negative meaning of the values that 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 that 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 appreciate the value provided to the organization.

Reporting may be the most valuable and important area to review closely when evaluating metrics capabilities. Reporting is the culmination of all of the metric and measurement activities, and is ultimately how the information will be presented to the organization. A key consideration of reporting is audience identification and alignment. In most cases, ISRM programs provide data to a variety of interested parties including senior leadership, business process owners, and technical and operations staff. The reporting of the metrics and measures should be tailored to each of these audiences in the presentation and format and by which data are included. One way to evaluate the reporting capabilities is to interview stakeholders who are recipients of the data for each identified audience type, gauge the value they believe they receive from the reports and identify how they use the reports in their business activities. If the reports are used for business activities or are reviewed only because the recipients perceive that they need to do so to meet an expectation of leadership, these reports need to be revisited to ensure that they provide consistent business value to the recipients.

OPERATIONAL VS. CONSULTATIVE APPROACH

ISRM programs can include operational components as part of their core capabilities, or they can operate in an advisory and consulting capacity. If operational components are included, there should be a clear definition of expectations of the operational responsibilities and how they differ from other operational capabilities within the organization. There should also be documented processes and procedures for sharing information about operational effectiveness, requirements, intelligence and incident-response activities.

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

INDUSTRY STANDARD ALIGNMENT

There are numerous ways in which an ISRM program can demonstrate its capabilities to interested parties and third-party examiners, but typically the most effective include a demonstration of the alignment of capabilities to industry regulations and/or standards. Industry standards tend to be accepted as industry-leading practices or, at a minimum, as a demonstration of minimal competency and capability. When evaluating ISRM capabilities, it is important to identify what, if any, standards with which an organization is attempting to align, and for what reason. If organizations are aligning purely for the purpose of meeting compliance guidelines, they may not understand or be receiving the benefits that are intended by the standards. If they are treating the standards as guidelines by which they are modeling their services and capabilities, this may be a sign of immaturity since they are reliant on the point of view of outsiders rather than the development of their own best practices.

Industry standards alignment does have many benefits for an ISRM program or capability. An indication of effective alignment will be a mapping of an organization's existing capabilities to those prescribed by the standards that the organization finds useful or beneficial to the business. This method demonstrates that the organization has a thorough understanding of the standards to which it is aligning, as well as an appreciation for the need to develop its own capabilities independently. Some of the key industry standards (or good practices) with which ISRM organizations and capabilities may elect to demonstrate alignment include:

- ISO 27001-27008 and 31000
- US National Institute for Science and Technology (NIST) 800 series of standards
- Payment Card Industry Data Security Standard (PCI DSS)
- COBIT

CONCLUSION

The business value and impact of ISRM programs and capabilities are rapidly being recognized within organizations. ISRM programs are no longer subservient to other capabilities and need to be evaluated and assessed on a regular basis to ensure that they continue to align with the needs and requirements of the organizations they serve. Effective evaluation will allow an organization and its leadership to understand how their ISRM capabilities align with their expectations and industry-leading practices, and where investment needs to be made to meet their needs and requirements.

REFERENCES AND FURTHER READING

Nolan, Richard L.; "Stages of Growth Model for IT Organizations," *Harvard Business Review*, 1973

Humphrey, Watts; *Managing the Software Process*, Addison Wesley, USA, 1989

Pironti, John; "Developing an Information Security and Risk Management Strategy," *ISACA Journal*, vol. 2, 2010

Pironti, John; "Key Elements of an Information Risk Management Program," *Information Systems Control Journal*, vol. 2, 2008

Pironti, John; "Key Elements of an Information Security Program," *Information Systems Control Journal*, vol. 1, 2005