Developing an Information Security and Risk Management Strategy

John P. Pironti, CISA, CISM, CGEIT, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC. He has designed and implemented enterprisewide electronic business solutions, information security and risk management programs, business resiliency capabilities, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, energy, government, hospitality, aerospace, media and entertainment, and information technology on a global scale. Pironti is a published author and writer, highly quoted and often interviewed by global media, and a frequent speaker on electronic business and security topics at domestic and international industry conference

An information security and risk management (ISRM) strategy provides an organization with a road map for information and information infrastructure protection with goals and objectives that ensure capabilities provided are aligned to business goals and the organization's risk profile. Traditionally, ISRM has been treated as an IT function and included in an organization's IT strategic planning. As ISRM has evolved into a more critical element of business support activities, it now requires its own independent strategy to ensure its ability to appropriately support business goals and to mature and evolve effectively.

A multiphased approach to developing an ISRM strategy is often most effective and provides recognizable results and value to an organization.

PHASE I—BUSINESS AWARENESS

The first phase includes the following:

- Understand the organization's current business conditions.
- Consider the organization's risk profile and appetite.

Current Business Conditions

When developing an ISRM strategy, it is important to understand the organization's current business conditions, as they will dictate the ability of the organization to execute the strategy that has been defined. If an organization does not have the staff, budget or interest in a robust or expansive ISRM capability, the strategy must reflect this situation. In many cases, organizations will implement effective capabilities only if those capabilities will reduce their capital and operational expenses or increase their value in the marketplace.

Quick tip:

- An organization's financial status is a key indicator of its current business condition:
  - If conservative, delay implementation of enhanced capabilities and focus on minimum requirements.
  - If growth, derive business value from implementation of robust capabilities.

Risk Profile

One of the vital and often misunderstood data points that must be considered when developing an ISRM strategy is the organization's risk profile and appetite. The goal of an ISRM strategy should be to complement business goals while maintaining a responsible level of risk management and security for the organization's information infrastructure and data. ISRM is one component of an overall enterprise risk management (ERM) capability, and as such, it should align itself with the goals and doctrines of ERM whenever possible.

Quick tip:

- ERM defines the organization's risk profile. Aligning with ERM allows business leadership to be confident that the ISRM strategy is business-enabling, not disabling.

When developing the ISRM strategy, it is important to understand the current and projected budget availability for the term of the strategy. One common mistake is to develop a strategy based on assumption of a future budget request rather than working within the guidelines of projected budget availability. This is not to say that the strategy must fall in line with the current projected budget, but it does allow for the alignment of financial guidelines and helps to ensure that the strategy can be viable and credible when presented to leadership for approval and endorsement. If a strategy is developed without the endorsement of the chief financial officer, it most likely will be rejected before its salient points are even discussed.

Quick tips:
- ISRM budgets are typically 7-10 percent of the overall IT budget without compliance activities and 10-13 percent when inclusive of compliance activities.
- If scope of the ISRM strategy extends beyond IT, budget requirements need to account for this.

PHASE II—STRATEGY DEFINITION

The second phase includes the following:
- Include a prescriptive annual plan followed by a rolling three-year plan.
- Clearly identify the point of arrival for capabilities based on management guidance and input.
- Ensure the availability and capability of necessary staff for the strategy execution.
- Gain an understanding of the organization's culture to ensure an appropriate plan for ISRM adoption.

Annual vs. Rolling Three-year Plan

In most cases, strategic planning follows a prescriptive annual plan followed by a higher-level, rolling three-year plan. The idea behind this is to allow for the determination of specific goals and objectives that can and should be met on an annual basis while accounting for the fact that ISRM is an ongoing activity. This also allows the organization to understand its current state of capability as well as its projected needs and requirements for the future. The rolling plan is adjusted annually to accommodate changes in business activities and conditions, while the annual plan stays consistent for the period within which it operates.

Quick tips:
- The typical time window for implementation of an ISRM strategy and program is 30-36 months (when all capabilities are in place and operating as business as usual).
- Capital and operational expenses are highest in year one, stabilize in year two and typically grow organically by year three.

Point of Arrival

When developing an ISRM strategy, it is important to clearly identify the point of arrival for capabilities based on management guidance and input. The point of arrival is simply a definition of the desired state of capability that the organization would like to have in place once the strategy has been executed. The best way to determine the point of arrival is to work with the leadership team to understand their goals regarding ISRM.

Often leadership teams have different perspectives on the point of arrival, dependent upon the audience to whom they are speaking. Leaders want to project a feeling of trust and safety to external parties, including clients and partners, and may state that they will do everything they can to ensure the safety of information infrastructure and data. Alternatively, these same leaders frequently communicate to internal audiences that they would like the organization to be as good or slightly better then its peers and competitors in its industry. This can often lead it down the path of "security by compliance"—meeting regulatory requirements and adhering to industry standards but not necessarily providing comprehensive ISRM capabilities for the organization.

Quick tips:
- Present multiple points of arrival for review and selection by the organization's leadership team.
- Develop key performance indicators (KPIs) based on the selected point of arrival to monitor value and effectiveness.

Staff Availability

A key element of any ISRM strategy is the level of staffing that will be available for strategy execution. It is important to correctly size the strategy based on current or expected staffing capabilities to ensure that the defined capabilities and objectives can be met. Many organizations find themselves in situations in which they have many objectives but do not have the staff available to achieve them. This is typically a primary concern during the initial foundational implementation phase in which staff requirements can be triple that of those required during the operational and maturity phases.

Quick tips:
- Identify staff availability for implementation and operation of strategy during the development process.
- Staff identified as having part-time availability (50 percent or less) should be projected to be available only for limited time (30 percent or less) to ensure effective implementation of strategy with available resources.

Cultural Awareness

Understanding the culture of an organization is important when developing an ISRM strategy, and a key element is adoption. Adoption of strategy will not occur quickly or effectively if the members of the organization who are impacted by the strategy do not support the implementation. If an organization has a culture that is based on open exchange of ideas and freethinking, the use of consensus activities and open discussion of the strategy will be most effective. In contrast, an organization in which the culture is based on directives from leadership and expected alignment to those directives will not benefit from open discussion and consensus. Instead, specific guidance and messaging from senior leadership will be necessary to drive adoption of the strategy.

PHASE III—STRATEGY DEVELOPMENT

The third phase includes the following:

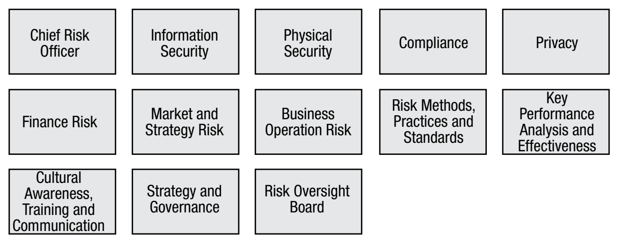
- Define the governance model and functional inventory of capabilities and services.
- Consider whether the ISRM strategy will include operational components or will act as a consultative element within the organization.
- Determine the reporting structure for ISRM.
- Consider the staff and competency requirements necessary to successfully implement and operate the ISRM strategy.
- Consider the risks of sourcing and ensure appropriate oversight by internal staff.

Models and Frameworks

When developing an ISRM strategy, it is important to define the governance model and functional inventory of capabilities and services that will be provided by the organization. A modular format is preferable, allowing the organization to add, delete or modify functions as business conditions and requirements change. Each function that is defined will also have KPIs with thresholds that allow the organization to understand whether the individual function, as well as the overall organization, is operating within acceptable tolerances.

ISRM is often broken into two functional models or inventories due to the distinction between the concepts of risk and security. An information risk management framework (see **figure 1**) will include multiple functions that are oriented toward identifying information risks across the entire spectrum of the organization, including operational, market, compliance, strategy, credit, fraud and other risk considerations. This framework frequently also includes information security as a component, since it is typically the enforcement element that allows the organization to implement its risk mitigation capabilities to ensure alignment with its risk profile and tolerance levels.

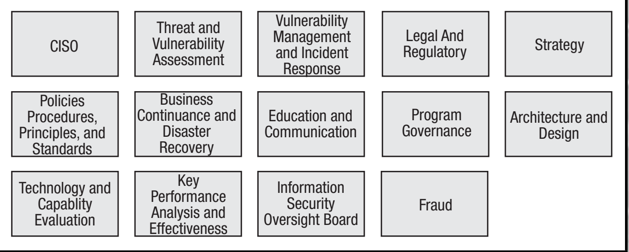
Figure 1—Information Risk Management Functional Inventory



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		

Information security should have its own inventory of capabilities and functions for the enforcement component of the ISRM strategy (see **figure 2**). These functions will include elements such as threat and vulnerability assessment, vulnerability management, business resiliency, architecture and design, and others. The KPIs defined for information security will measure the organization's ability to maintain the risk tolerance levels established by the risk management functions.

Figure 2—Information Security Functional Inventory



CISO	Threat and Vulnerability Assessment	Vulnerability Management and Incident Response	Legal And Regulatory	Strategy
Policies Procedures, Principles, and Standards	Business Continuance and Disaster Recovery	Education and Communication	Program Governance	Architecture and Design
Technology and Capablity Evaluation	Key Performance Analysis and Effectiveness	Information Security Oversight Board	Fraud	

Operational Components

It is essential to consider whether the ISRM strategy will include operational components as part of its activities or whether it will act as a consultative element within the organization. The benefits of having direct management and oversight of operational components are the ability to control the complete life cycle of capability from strategy to architecture and design, to implementation and operation. While this sounds attractive in theory, it is often recommended to exclude operational components from the

ISRM strategy and instead provide advisory and consultative capabilities to support the business operations.

Quick tip:

- The manner in which ISRM functions and their supporting governance structure are presented to an organization is key to driving acceptance and enabling success. Presenting the IRSM strategy as business-aligned advisory and consultative capabilities that are focused on risk management, instead of authoritative and technical capabilities that are focused on security to business audiences, will change the perception of ISRM from an organization that prevents success to one that enables it.

Reporting Structure

Many organizations view ISRM and risk management as an IT capability, reporting to the chief information officer (CIO) or chief technology officer (CTO). However, the ISRM scope of responsibility now frequently extends beyond technology to a focus on business processes and data. If this holds true, the ISRM group will likely be more effective as part of ERM and reporting to the chief risk officer (CRO).

Competency Models

Another consideration is the staff and competency requirements that will be necessary to successfully implement and operate the ISRM strategy. Competency models are documents that identify not only the job descriptions of specific positions, but also the relevant organizational and industry knowledge and skills that will be required. When developing an ISRM strategy, it is important to provide solutions, requiring competencies that are readily available within the organization or can be recruited for with minimal effort. If the strategy calls for skills and knowledge that are new to the organization, a ramp-up period must be established and timing for achievement of the point of arrival should be extended to account for the on-boarding period.

Sourcing Plans

Sourcing is an important consideration for an ISRM strategy. Many organizations fail to realize that they cannot transfer risk to a third-party organization even though they can utilize third parties to provide ISRM capabilities. Sourcing can be an effective tool to accelerate the implementation of capabilities as well as to provide operational capabilities, but third parties cannot assume the risks of the organization. The organization will always be responsible because they are the entity through which business is transacted and are required to provide appropriate levels of information security and risk management.

Third-party consulting resources can be helpful in accelerating the implementation or maturing specific functions. However, consulting must be used sparingly and must be overseen by internal staff to ensure that the requisite knowledge provided by the consulting firm is retained by the organization. Key functions that are provided to the organization should not be delivered exclusively by third-party consulting resources. Whenever possible, organizations should not utilize third parties to ensure consistency of services, since consulting resources are often the first to be removed in the case of budget reduction or declining business conditions.

Quick tips:

- Managed security services (MSS) providers can provide effective monitoring and management of ISRM technology capabilities after the organization has defined operating parameters.
- MSS providers can provide valuable insights and threat intelligence based on knowledge and data gathered by working with a large number of clients and the providers' focus on enhancement of products and services.

PHASE IV—METRICS AND BENCHMARKING

The fourth phase includes the following:

- Ensure alignment with industry standards and guidelines.
- Use a capability maturity model (CMM) assessment methodology.
- Use KPIs to measure the effectiveness of the functions and capabilities developed through the ISRM strategy.

Industry Standard Alignment

Alignment with one or more industry standards or guidelines can be beneficial to an ISRM strategy. There are multiple standards that can and should be considered, including CobiT, International Organization for Standardization (ISO) 27000 series and US National Institute of Standards and Technology (NIST) 800 series. However, it is important to remember that no single standard is appropriate for every organization, nor should strategy be based on only one option.

A current industry-leading practice is to identify functions and capabilities provided by the ISRM group and map them to industry standards and guidelines. This approach allows the organization to identify whether it is providing all of the functions and capabilities included within the standards and guidelines with which it chooses to align, as well as to identify levels of capabilities and competencies in these areas. Mapping ISRM capabilities to industry standards can also be very helpful in meeting compliance goals and requirements, since many of these (including typical vendor/partner compliance requirements) are based on the same standards and guidelines.

CMM Modeling and Benchmarking

Two key questions a management team will regularly ask about the organization's ISRM capabilities are: How capable are we? How will we know when we have reached our point of arrival? One of the most effective ways of assessing this is to use a CMM assessment methodology (see **figure 3**). A CMM methodology provides a simple yet effective scale that the organization can use to understand quickly which of its capabilities are functioning adequately and which need improvement to increase efficiency, reduce cost of operation and increase value to the organization.

Once the CMM assessment has been completed, the use of benchmarking data from other similar organizations based on the same CMM methodology will allow the organization to understand its level of capability and effectiveness compared to its peers and competitors (see **figure 4**). These data are vital in the development of an effective ISRM strategy because they provide valuable inputs into the governance approach, budget assessments, and development of goals and metrics. These data can be gathered through multiple sources, including consulting and analyst firms that actively collect and maintain data stores of this type.

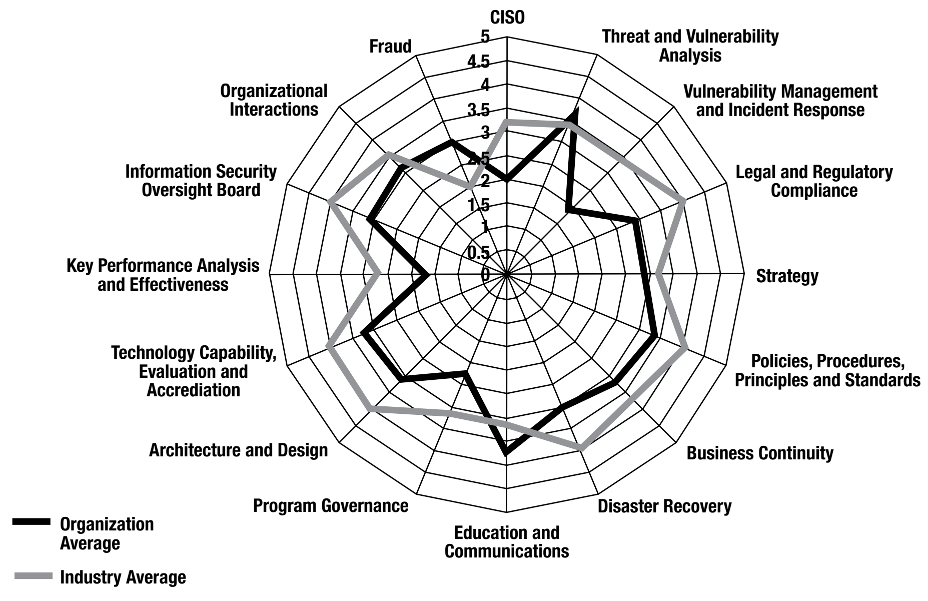
Figure 3—ISRM CMM Scale

Maturity Level	General Description	Control Summary	Key Features
5	Optimal, optimizing and business-aligned	• Included in audit and assessment cycles • Control metrics measured and monitored • Developed and utilized process metrics • Complete control quality feedback loop	• Tracked control information and status • Aligned with business processes • Very low associated residual risk level • Meeting or exceeding business requirements
4	Managed, controlled and predictable	• Controls audited and tested for compliance • Defined metrics and thresholds • Standards in place and followed • Operates within recognized processes • Training and awareness complete	• Efficiently operated within formal processes • Embedded in IT processes • Business requirements considered • Low associated residual risk level • Good/excellent effectiveness
3	Proactive, defined and implemented	• Owners trained to operate control • Evenly implemented and monitored • Documented in control catalog • Documented standards • Regular assessment of control	• Good/excellent efficiency • Becoming embedded in IT processes • Widely known and published status of control • Moderate associated residual risk • Effectiveness in an acceptable range
2	Repeatable, reactive and best effort	• Ownership assigned to role, person or process • Implemented inconsistently across organization • Documented via policies and guidelines • Haphazard assessment and/or audit	• Mediocre/fair efficiency • Status usually known by a few • Moderate to high associated residual risk • Effectiveness based on individual effort/expertise
1	Initial, undefined and *ad hoc*	• Not officially assigned to role, person or process • Partially implemented • Not well documented • Not monitored or assessed	• Poor efficiency • Questionable ownership • Vague status • High associated residual risk • Generally unknown effectiveness
0	Intent and not identified	• Control not implemented • Unknown presence of control	• Control not officially in place • Unidentified requirements • Associated risk level assumed to be very high

Key Performance Indicators

KPIs should be used to measure the effectiveness of the functions and capabilities that are developed through the ISRM strategy. When developing KPIs, it is important to identify the business value that is intended to be gained with function or capability, and then define objective criteria that can be used to assess this value. Subjective KPIs can be open to interpretation by the audience evaluating the metric; therefore, objective KPIs should be utilized whenever possible. Typically, KPIs associated with a dollar value, benefit or business impact statements are the most effective and interesting to leadership and stakeholder audiences.

Figure 4—Benchmark Diagram



> **Quick tips:**
> - Successful KPIs require thresholds to establish acceptable and unacceptable limits.
> - KPIs should be aligned with point-of-arrival guidelines and annual organizational goals.

PHASE V—IMPLEMENTATION AND OPERATION

The fifth phase includes the following:

- Take global considerations into account.
- Determine how compliant the organization wants or needs to be.
- Determine consequences of not conforming to ISRM policies and requirements.
- Utilize an oversight board as part of the operational model for an ISRM strategy.
- Ensure that appropriate communication is occurring between the ISRM group and supporting business functions.
- Ensure cultural awareness regarding how information protection activities are viewed within the organization by changing the focus from security to risk management.

Global Considerations

Global considerations cannot be neglected when developing an ISRM strategy. Many controls, capabilities, standards and guidelines that are appropriate for a specific geography may not be applicable in others. For instance, in the US, an appropriate and preferred measurement of employee awareness of ISRM capabilities is to present employees with materials, test them on their retention and recognition of the materials, and collectively store and report this information. However, in countries such as Germany, this is not an allowed practice and cannot be implemented due to human resource regulations.

> **Quick tips:**
> - Threats and risks can vary significantly based on geography. Physical threats tend to be less probable in developed nations and environments due to the intention to steal data instead of infrastructure.
> - Examine socioeconomic data for regions within which the organization operates to understand cultural and economic considerations that can impact strategy development.

Compliance and Risk

Compliance is currently the driving force behind many ISRM strategy development activities. One question that is often overlooked by organizations is: How compliant do they want or need to be to the regulations, standards and expectations of the third parties that evaluate them? Many organizations invest significant money and resources to obtain and maintain compliance to regulations and standards. A better approach often is to analyze the impact of not being compliant or becoming only partially compliant. In many cases, full compliance can be debilitating to business operations. If a regulation or standard does not have court precedence or defined and implemented consequence management, the impact of noncompliance may not be well understood. It may be in the organization's best interest to continue to develop capabilities in line with industry-leading and organizational best practices instead of focusing on external compliance requirements alone.

Consequence Management

What happens when the intended group or organization does not conform to ISRM policies and requirements? Consequence management is the enforcement element for issues of noncompliance or nonalignment. It can range from a simple risk waiver that removes liability for actions from the ISRM group all the way to punitive actions against employees who choose not to align to ISRM directives.

Quick tips:

- A laddered approach to consequence management is often the most effective and accepted within organizations.
- Increased consequences should be based on risk and business impact to organization.

Oversight and Reporting

Utilizing an oversight board as part of the operational model for an ISRM strategy can ensure business alignment as well as remove the ability for dissenters to criticize the organization for a lack of business consciousness. An oversight board should be composed of key business leaders and stakeholders from the organization as well as business elements that are governed by requirements from the ISRM group.

Quick tips:

- Oversight boards should meet monthly or quarterly unless business conditions or incidents warrant more regular meetings.
- Key metrics and requests for approval of activities or materials should be presented at these meetings.

Organizational Interactions

Organizational interactions ensure that appropriate communication is occurring between the ISRM group and supporting business functions. Organizational interactions differ from training, communication and awareness capabilities in that they are reciprocal in nature instead of a projection from the ISRM group. It is important to identify supporting and benefiting organizational elements and to implement formal communication capabilities that can be monitored to ensure that all appropriate parties are communicating with each other to support the ISRM program activities and strategy.

These communications should be monitored and reported as part of the KPIs that are collected and reported to the oversight board. The goal here is to ensure that the organization's leadership is confident that ISRM activities and reporting are supported by credible data.

Quick tip:

- Use KPIs to monitor communications and report effectiveness of organizational interactions to the organization's leadership.

Communication and Awareness

Communication and awareness are vital portions of the ISRM strategy since a core capability of the organization is to communicate appropriately and to influence positive and proactive change. Communication considerations are based on the organization's culture and style. It is important to utilize multiple forms of communication and awareness as well as continual reinforcement when communicating change. Electronic media are appropriate for general communication, but human interaction is vital for key information to allow for bilateral conversation instead of one-way communication.

Cultural Change: Security vs. Risk Management

A fundamental consideration in ISRM is the cultural change regarding how information protection activities are viewed within the organization. As previously stated, information security is often seen as an obstacle to success instead of a benefit because many security professionals focus on technology and restrictions to provide protection, which often prevents business leaders from carrying out activities that they see as enhancements to the business. The word "security" has a negative connotation in the minds of many professionals, since they associate it with restriction and prevention. By utilizing the word “risk” in the title of the group and taking a risk management approach instead of a security-focused one, the opposite often occurs.

Risk is something business professionals are accustomed to managing on a regular basis. When they are presented with information from a risk perspective, business professionals are more likely to accept guidance and assistance from the ISRM group. Once the business leadership identifies the level of risk deemed acceptable for the organization or business activity, security can be utilized to develop, monitor and maintain controls that align to the defined risk profile. This allows the ISRM group to achieve its primary objectives: providing information security and risk management capabilities to the organization.

FINAL THOUGHTS

Without a defined and developed strategy, an organization’s ISRM capabilities will continue to be viewed negatively and will have limited benefits or positive impact. Developing an ISRM strategy is a critical element in the maturation of information security capabilities. If the goal of the ISRM group is to be business aligned, then its strategy must be developed with this goal in mind.

If an effective strategy is developed and implemented, ISRM will become a key benefit to the organization, and its value will be easily understood through the reduction of information security incidents as well as the effort and costs associated with information protection.

The true measure of success of a well-developed and implemented strategy can be found in the impressions and actions of the constituency that it serves. If they utilize ISRM capabilities during key decision-making activities and consult with the ISRM group on a regular basis, success can be achieved. If they continue to fear and avoid ISRM and its capabilities until it is absolutely necessary to engage, the strategy needs to be changed.