Key Elements of an Information Risk Profile

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC. Pironti has designed and implemented enterprisewide electronic business solutions, information security and risk management and information technology strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key customers in numerous industries. He 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.

Information risk has become a top-of-mind issue for many business leaders and information risk management security (IRMS) professionals. Largely driven by a misunderstanding of each other's activities and motives, these two groups have historically had challenges interacting with each other. That is, business leaders recognize and embrace the need to take risk and often incent their constituents to take it as well in order to achieve business goals; conversely, IRMS professionals are charged with minimizing risk and ensuring their organization's information infrastructure and associated data assets are properly protected. The best way for these parties to reduce friction and meet their individual requirements is to mutually develop and maintain an information risk profile that they both can use to guide their respective activities.

An information risk profile documents the types, amounts and priority of information risk that an organization finds acceptable and unacceptable. This profile is developed collaboratively with numerous stakeholders throughout the organization, including business leaders, data and process owners, enterprise risk management, internal and external audit, legal, compliance, privacy, and IRMS.

ESTABLISHMENT OF DUE CARE

In the legal community due care can be defined as the effort made by an ordinarily prudent or reasonable party to avoid harm to another by taking circumstances into account.[1] When applied to IRMS, due care is often considered a technical compliance consideration and standards such as the Payment Card Industry Data Security Standards (PCI DSS) or National Institute of Standards and Technology (NIST) guidelines are often referenced. While these standards can be effective at providing broad guidance, an organization must develop its own view of due care and its own capability to implement and maintain skills to support this view. An information risk profile can be an invaluable tool to assist leaders and decision makers in establishing this guidance and effectively communicating their information and data risk appetite and expectations.

ALLOWING DECISION MAKERS TO MAKE DECISIONS

Typically, friction exists between decision makers and IRMS professionals due to their misperceptions of each other. Business leaders and decision makers often view IRMS requirements and professionals as obstacles in their path to success. At the same time, IRMS professionals often view business leaders and decision makers as individuals who are not informed enough to understand the value of their activities and the associated requirements. The detailing and documenting of the organization's information risk appetite and expectations remove the often-ubiquitous subjective assumptions that IRMS professionals use to guide their actions and activities.

IRMS professionals who effectively leverage the information risk profile now have a solid foundational tool. They can reference the information risk profile that was developed and endorsed by the organization's business leaders and decision makers. If IRMS professionals are effective in demonstrating their guidance and the actions align with the profile, the business leaders and decision makers are compelled to seriously consider them and either adjust the organization's information risk profile to accommodate the requests or modify their requirements to be in alignment. This creates an opportunity for IRMS professionals to engage in consultative and collaborative activities. Together, they can develop a plan that provides a positive outcome and meets requirements while still aligning with the organization's information risk management expectations.

LINKAGE TO ERM ACTIVITIES

Enterprise risk management (ERM) is an evolving and important concept within many

FORUM

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.

Go directly to the article:

organizations and includes information risk management as one of its functions. The use of an information risk profile is often an effective way for traditional security professionals to integrate with this concept. The profile provides important insights and guidelines associated with information risk identification and management. The ERM function can then leverage this information as it calculates overall enterprise risk and develops control objectives and management practices to effectively monitor and manage it. The structure of the profile provides a framework that easily and logically organizes data for the organization to leverage as needed.

INFORMATION RISK PROFILE STRUCTURE

An organization's information risk profile should be structured and formatted in a fashion that quickly demonstrates its value and intent to the organization, is easily understood and applicable to the organization as a whole, and is viewed as useful and beneficial to its leaders and stakeholders. The following can be useful in meeting these goals.

Guiding Principles and Strategic Directives

An organization's information risk profile should include guiding principles aligned with both its strategic directives and the supporting activities of its IRMS program and capabilities. This information should be listed early in the profile to allow the reader to understand its context and intent. Common guiding principles include the following:

- Ensure availability of key business processes including associated data and capabilities.
- Provide accurate identification and evaluation of threats, vulnerabilities and their associated risk to allow business leaders and process owners to make informed risk management decisions.
- Ensure that appropriate risk-mitigating controls are implemented and functioning properly and align with the organization's established risk tolerances.
- Ensure that funding and resources are allocated efficiently to ensure the highest level of information risk mitigation.

Information Risk Profile Development

Transparency is a key aspect to the success and adoption of an information risk profile. The risk profile's accuracy and credibility may be called into question if the methods, practices, source materials and intelligence—as well as individuals involved in its development—are not provided as part of the document. This information can be referenced as part of an appendix to the document and include links to the materials themselves.

Business-state Representation of Information Risk

The information risk profile should include a current-state analysis of identified information risk factors that have a reasonably high probability of occurrence and would represent a material impact to business operations if realized. The descriptions of risk should be brief and expressed in language that is recognized and understood by both business- and technology-oriented personnel.

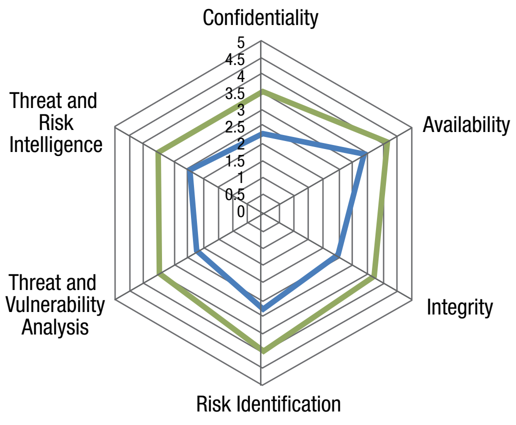
The current-state representation should also include the organization's IRM views, expectations and requirements. This should include identification and analysis of the opinions of business leaders and stakeholders and their views on information risk and security, a description of current business conditions, current threat and vulnerability analysis outcomes, and expectations of external parties (i.e., customers, partners, vendors, regulators). This can also assist in the development of future-state objectives and requirements.

Future-state Objectives and Requirements

The future-state objectives and requirements identify the ideal state of information risk management for the organization and general information risk appetite and tolerance. This includes key IRMS-related initiatives that are in progress or are soon to be initiated; their associated timelines for completion; and a brief summary of the initiative's owners, key dependencies, and expected level of information risk reduction at milestone points and at completion.

An effective way of evaluating and communicating the future-state objectives and requirements is to use a capability maturity model (CMM) approach. An assessment of key functions and capabilities for the current and future states using CMM can help an organization easily identify areas of required focus and investment for functions, capabilities and services that are required. Using a radar chart format (**figure 1**) to represent these data is an effective way of communicating the information and is easily understood by a broad audience.

Figure 1—CMM Radar Chart



Data Classification Levels and Designations
5—Confidential—restricted
4—Confidential—customer-or compliance-related
3—Proprietary
2—Internal use only
1—Public

Key Business Processes and Capabilities

Organizations often have numerous business processes and limited resources and bandwidth to protect them. It is important to identify the organization's key business processes and capabilities within the information risk profile—those that, if impacted negatively, could cause a material impact to the operations of the business. Often they can be separated into business support functions (i.e., payroll and benefits, messaging and communications, finance) and production (i.e., revenue generating, regulated, contractually required).

An easy but often overlooked source for a listing of these processes and capabilities is an organization's business continuity and/or disaster recovery plans. These plans typically include not only the key business processes, but also rank their level of importance to the organization. They also provide valuable insights into the recovery time and recovery point objectives that are often considered in risk calculations.

Key Data Elements

Key data elements that are identified and defined in the risk profile often include intellectual property, transaction data, financial data, nonpublic personal information, customer data, human resources information and other sensitive data assets. Defining the key data elements ensures users that the information risk profile provides a data dictionary that offers a clear understanding of the data element as well as its value to the organization.

Identification of Data Owners and Stakeholders

All data and information within an organization should be associated with a data owner and one or more stakeholders. Identifying and evaluating ownership attributes is important because the owners and stakeholders are responsible for their information risk management decisions. This activity can also assist in the identification of dependencies that can affect the risk appetite for data assets, especially in situations where they are required for one or more critical business functions or processes.

Identification of Business Value

The value of information is often misunderstood and based on subjective perceptions of data owners or evaluators instead of meaningful analysis and calculation. A basic principle of information risk management is that the cost to protect information should not exceed its value. To assess the value of information, it is often easier to identify, communicate and monitor the value of processes, rather than data assets. Processes can be attached to activities of the organization, such as revenue generation, core and general operations, and achievement of strategic business goals. The information risk profile does not need to quantify the exact value of data assets, but does need to establish a general representation of value to allow for the definition of appropriate levels of classification and control.

Data Classification Schema

To simplify information management, it is important to classify data into easily understood containers (see **figure 2**) associated with control objectives and requirements that identify data-handling requirements. This classification schema should be as simple as possible in order for it to be useful to the information risk profile and general activities of the organization.

The information risk profile should include the organization's data classification schema and a summary of the control requirements and objectives associated with it. It is recommended that data classification schemas contain between three and five levels of definition that contain progressively stronger and more comprehensive control objectives and requirements as they ascend.

Figure 2—Data Classification

Level	Designation
5	Confidential—restricted
4	Confidential—customer- or compliance-related
3	Proprietary
2	Internal use only
1	Public

Risk Levels and Categories

Risk levels and categories provide a framework that can be used to organize and communicate information risk in an easily recognizable format. Risk levels provide a scale to represent the level of material business impact that would result if a risk were to be realized. The categories help to define the type of impact that would likely materialize. To be useful, the levels and categories should be simple and easily understood.

The following are examples of information risk levels:

- **High**—Severe material compliance, legal and/or financial consequences; significant material impact on critical business processes and/or business operations; loss of customer trust and/or damage to brand reputation
- **Medium**—Significant material compliance, legal or financial consequences; substantial material impact on key business processes and/or business operations; weakened customer trust and/or brand reputation
- **Low**—Negligible to no material compliance, legal and/or financial consequences; minimal material impact on key business processes and/or operations; insignificant change in customer trust and/or brand reputation

The following are examples of information risk categories:

- **Confidentiality**—The disclosure of sensitive information to unauthorized individuals or systems
- **Integrity**—Impact to the accuracy and consistency of data and information
- **Availability**—Effect on the ability to access capabilities and associated data and information

By using this method of level setting and categorization, key business processes can then be presented in the form of a heat map (see **figure 3**) to visualize the associated information risk levels.

Figure 3—Current Information Risk Levels by Key Business Processes

Key Business Processes	Confidentiality	Integrity	Availability
Payroll and benefits	High	High	High
Credit and collections	High	High	High
Web presence	High	High	Medium
Billing and receivables	Medium	Medium	Medium
Supply chain management	Medium	Medium	Low
Messaging and communications	Medium	Low	Low
Procurement and payables	Low	Low	Low

MATERIAL BUSINESS IMPACT CONSIDERATIONS

Material business impact considerations are a vital element of any information risk profile. They provide the equivalent to pain charts—commonly used in health care environments. A pain chart typically uses a numerical or graphical scale and allows a health care provider to understand the level of pain and discomfort that a patient is experiencing in order to respond with the appropriate level of care. In the information risk profile, the material business impact considerations identify the impact an incident or loss has in terms that are easily understandable and recognizable by the organization. These considerations should span a number of categories including financial, productivity, availability, reputation, compliance, partner and supply chain, and customer. Here are some example material business impact considerations for an organization that has annual revenues of US $500 million:

- **Financial:** An immediate and unplanned loss equal to or greater than the following list would represent a material business impact to the organization:

Material Business Impact	Financial Loss Amount
Catastrophic	US $100,000,000 and above
Major	US $5,000,000 to $99,999,999
Moderate	US $1,000,000 to $4,999,999
Minor	US $100,000 to $999,999
Negligible	Less than US $100,000

- **Productivity:** An immediate and unplanned loss of employee productivity equal to or greater than the following list would represent a material business impact to the organization:

Material Business Impact Category	Employee Productivity Percent Loss
Catastrophic	85% and above
Major	40 - 84%
Moderate	20 - 39%
Minor	10 - 19%
Negligible	1 - 9%

- **Availability:** An immediate complete or partial lack of availability of one or more key business processes and associated information assets and supporting systems would represent a material business impact to the organization:

Material Business Impact Category	Time of Unavailability (Partial or Full)
Catastrophic	8 days and beyond
Major	73 hours - 7 days
Moderate	9 - 72 hours
Minor	2 - 8 hours
Negligible	Less than 2 hours

IDENTIFIED KEY INFORMATION RISK AND MITIGATION CAPABILITIES

The identification of known key information risk and mitigation capabilities provides a high-level perspective on the current information risk posture of the organization. These change and evolve over time and should be revisited as part of the annual update cycle for the information risk profile. The following are examples of key information risk:

- Limited visibility into information infrastructure and sensitive data assets
- Minimal governance and compliance enforcement for third-party processing, storage and use of sensitive data assets
- Lack of a trust-but-verify control structure to limit impact of insider threats
- Limited capability to perform and maintain threat and vulnerability analysis of key business processes and activities
- Lack of a risk-conscious and security-aware culture
- Limited IRMS considerations in product and application development life cycle and technology operations
- Negligible information risk intelligence gathering, processing and communication capabilities

Examples of identified risk mitigation capabilities include:

- Expectation of employee adherence to IRMS policies and standards
- Basic technological security controls (e.g., firewall, intrusion detection, data encryption, antivirus)
- Insurance coverage of US $20 million to mitigate incident response and recovery costs for damage to information systems and data
- Basic business resiliency capabilities maintained (command and control, incident response, business continuity, disaster recovery), reducing the impact if a risk is realized

Individually, these data points provide limited value to the organization. When they are assembled together, properly endorsed and kept current, they can provide a holistic view of the organization's perspective associated with information risk management.

ENDORSEMENT AND UPDATES

For the information risk profile to be meaningful to the organization, its leadership and stakeholders must agree upon and endorse it. It is important to identify in the document who endorsed the profile and when it was released. This can be done through a document change management control table. The information risk profile itself should be reviewed, at a minimum, on an annual basis or as business conditions change that have a potential impact on the information risk appetite of the organization.

CONCLUSION

An information risk profile is critical to the success of an organization's information risk management strategy and activities. It provides valuable insights into an organization's information risk appetite and expectations for information risk management. Information risk and security professionals and programs that effectively leverage this information in their actions and activities can be confident in their alignment with business requirements and expectations.

REFERENCES

National Institute of Science and Technology (NIST), Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," 2010

International Organization for Standardization (ISO), ISO 27005:2008, *Information technology—Security techniques—Information security risk management,* 2008

ISACA, COBIT® 5, USA, 2012

ISACA, Risk IT, USA, 2009

ENDNOTE

[1] US Legal Inc., definition of "Due Care," *www.uslegal.com*