RIMS the risk management society

ISACA

# BRIDGING THE DIGITAL RISK GAP

## HOW COLLABORATION BETWEEN IT AND RISK MANAGEMENT CAN ENHANCE VALUE CREATION



# BRIDGING THE DIGITAL RISK GAP

## HOW COLLABORATION BETWEEN IT AND RISK MANAGEMENT CAN ENHANCE VALUE CREATION


### CONTRIBUTING AUTHORS

**Julie Cain**, CISSP, CISA, CRISC, GCEIT, CIPT
Senior Strategic Advisor, Information and Technology Risk Management
Education Testing Service (ETS)

**Grace Crickette**, ARM, CGEIT, CCEP-I, CSSA, SHRM-SCP, SPHR
Vice Chancellor for Administrative Affairs and Ethics Officer
University of Wisconsin-Whitewater

**Tom Easthope**, PMP
Director, Enterprise Risk Management
Microsoft

**Carol Fox**, ARM
Vice President, Strategic Initiatives
RIMS

**Paul W. Phillips, III**, CISA, CISM
Technical Research Manager
ISACA International

**James C. Samans**, CISA, CRISC, CISM, CBCP, CPP, CIPT, CISSP-ISSEP, PMP
Director, Information Systems Security
American Institutes for Research

**Evan Wheeler**, CRISC, CISSP
Vice President, Risk Management and Chief Information Security Officer
Edelman Financial Engines

### EXPERT REVIEWER

**Jack Freund, Ph.D.**, CISA, CRISC, CISM, CIPP/US, CIPT, CISSP, FIP
Director, Risk Science
RiskLens

### SUBJECT MATTER EXPERTS

**Tony Martin-Vegue**, CISM, CISSP, CEH, MCP, MSCE
Director, Information Security Risk
Informatica

**Alex Zadrozny**, CISA
Vice President, IT Risk and Controls
Bank of America Merrill Lynch

### EDITOR

**Morgan O'Rourke**
RIMS

### ART DIRECTOR

**Joe Zwielich**
RIMS


RIMS® *the* risk management society

**About RIMS**

As the preeminent organization dedicated to promoting the profession of risk management, RIMS, *the* risk management society®, is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world. Founded in 1950, RIMS is committed to advancing risk management capabilities for organizational success, bringing networking, professional development and education opportunities to its membership of more than 10,000 risk management professionals who are located in more than 60 countries. For more information on RIMS, visit www.RIMS.org.

ISACA®

**About ISACA**

Now in its 50th year, ISACA® is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips practitioners with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged practitioners—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China. For more information, visit www.isaca.org.

# INTRODUCTION

Technology has long been integral to the success of any organization, but as the range of business applications and the pace of innovation have increased, so has the risk. As a result, it is vital that risk management and information technology professionals communicate with each other on a regular basis to ensure the risk associated with the use of technology is properly managed, the enterprise assets are protected, and the value of technological investments is maximized. But all too often, it seems like the two groups are speaking a different language—that is, if they even speak at all.

ISACA® and RIMS have set out to bridge this gap by developing a joint report to help all parties collaborate and communicate more effectively so they can collectively bring more value to their organizations. This primer will help enhance the abilities of risk management and information technology professionals to speak the same language as they endeavor to incorporate the benefits and uncertainties associated with data and technology into the organization's overall strategy in order to create value and counterbalance unwanted risks and outcomes.

Integrating IT and risk management professionals in an overall digital strategy team can add value through coordinated decision making that is:

- Transparent, nimble and timely
- Inclusive and representative of enterprise needs
- Clearly defined in roles, accountability and decision-making authority
- Forward-looking in its risk assessment and benefit analyses (and not primarily resource based)
- Aligned to broader mission and strategy objectives
- Based on a disciplined design approach
- Open to interdependent thinking over functional thinking

To aid in common understanding, in addition to definitions of respective terminology that can found in Appendix B, a few basic definitions may be helpful to start. The terms "information security," "cybersecurity" and "IT security" are often used interchangeably, but they actually have different meanings.

In this report, we use the term **"information security"** to define the people, processes and technology involved in protecting data (information) in any form—whether digital or on paper—through its creation, storage, transmission, exchange and destruction. Information security is part of an organization's overall risk management approach and includes every operational and functional area along the entire value chain. At times, organizations view information security as an IT problem, but in truth everyone throughout an enterprise has a role to play in defining and managing the people, processes, technology and data the organization wishes to use and protect.

Included within the information security area is **"cybersecurity,"** a term used to describe the technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Cybersecurity deals specifically with the digital information an organization must protect from threats or other disruptions.

**"IT security"** describes a function, as well as a method of implementing policies, procedures and systems to defend the confidentiality, integrity and availability of any digital information used, transmitted or stored throughout the organization's environment. The term also applies to specific physical controls, hardware and software solutions used by IT departments to harden and manage the technology operations of the business.

Finally, we introduce the term **"cyber value chain"** to describe the digital and human processes and activities that cumulatively add discrete and new value for an organization and its customers.

*Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.*

# PART 1
## IT AND RISK MANAGEMENT WORLDS COLLIDE

Once limited to the realm of digital assets (such as networks and servers), the information technology (IT) function has increasingly evolved from managing hard assets as a shared service to serving as the backbone of the worldwide economy. As such, digital enterprise strategy—the IT architecture and governance of an organization—has become a strategic imperative.

Risk management has evolved as well from protecting the balance sheet through mitigation controls and insurance purchases to informing strategic and operational decisions and enhancing the viability of organizations within their respective ecosystems.

In the past, these worlds existed in separate environments, but a number of factors are now bringing them together.

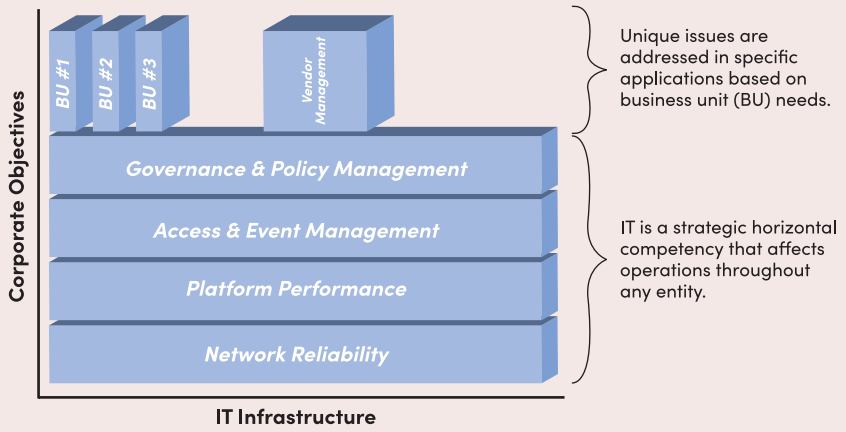
### The Changing Digital Risk Landscape

Digital enterprise strategy and execution—the IT infrastructure of governance and policy management, access and event management, network reliability and platform performance—are emerging as an essential horizontal competency to support business objectives through specific applications and vendor ecosystems by creating a new "Digital Risk Landscape" (see sidebar). As such, the IT and IT security functions are evolving from a protection/response posture to an engineering organization that is increasingly focused on what an enterprise needs to do to run the business, whatever that business happens to be.

As companies continue to transform digitally and cybersecurity becomes an increasingly critical capability, IT-related risk no longer is the sole purview of technical experts. Cybersecurity risks and opportunities are now a core component of a business risk portfolio. More organizations are undertaking digital transformation in their products or services and enterprise risk management is evolving to embrace these transformational aspects.

Because of expanding digital risk landscapes, risk management capabilities are also evolving as a corresponding horizontal competency. Lack of, or poorly thought out, digital enterprise strategies can torpedo an organization's mission and overall objectives. Likewise, failed implementations that do not deliver expected value to the organization—whether due to scope creep, budget overages or unrealistic expectations—can damage the viability of organizations as much as security risks related to data breaches and expropriation of intellectual property.

### THE DIGITAL RISK LANDSCAPE




© 2019 RISK & INSURANCE MANAGEMENT SOCIETY. ALL RIGHTS RESERVED.

***What is a Platform?*** "A platform enables an exchange of information, goods/services, money, attention, etc. between the producer and consumer," wrote strategist Sangeet Paul Choudary in a blog post titled "Platform Metrics" on his Pipes to Platforms website. All platforms are information-enabled businesses. Without the transfer of information to connect supply and demand and spark the interaction, the business is broken.

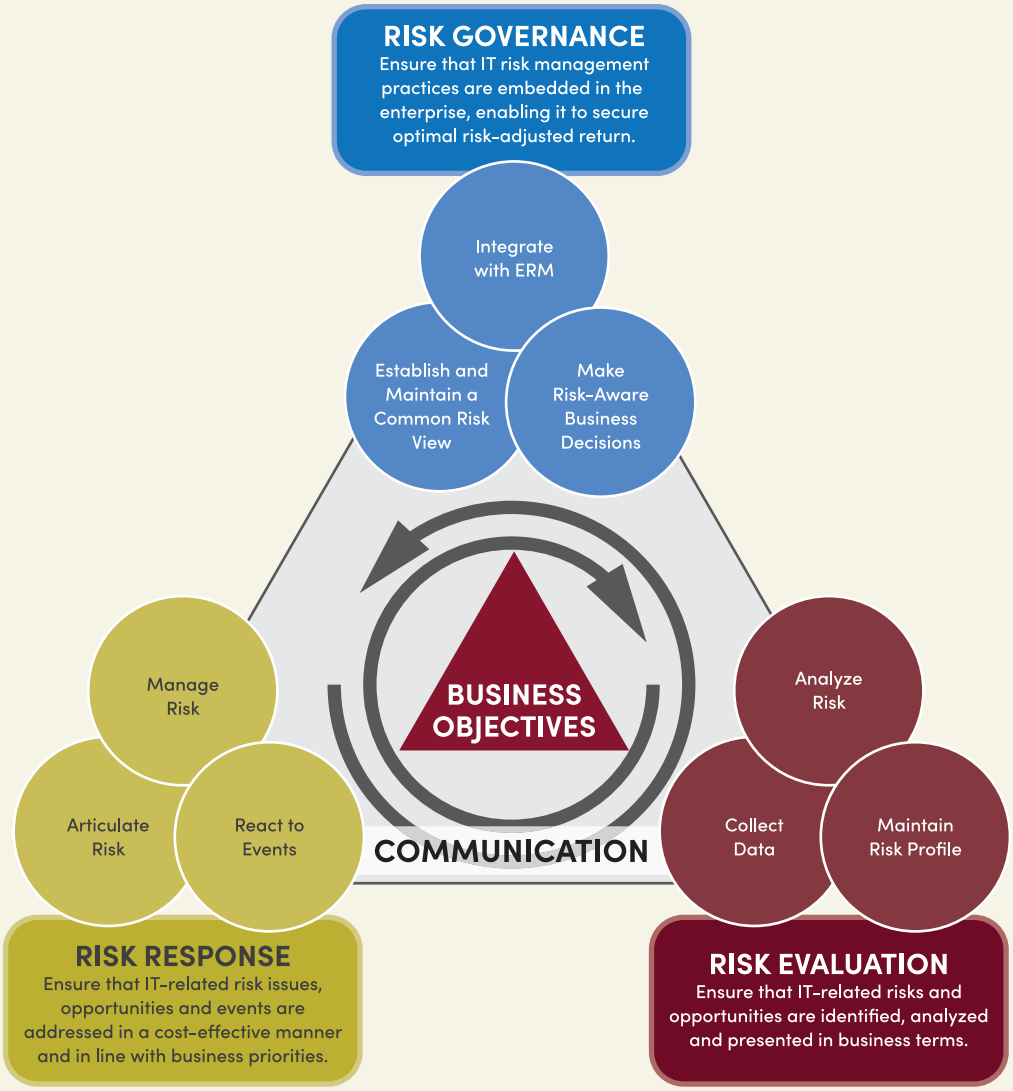
***What is a Network?*** The simplest description of a network is the infrastructure—the telephony (whether through cabling or wireless)—that carries information from place to place. The goal of the network is to transfer the information packet containing the information to be transferred (along with routing instructions) from the source to the destination with minimum failure. Routing is the process of selecting the best path on a network. In an IT environment, the term telephony may refer to computer hardware (such as servers, whether located onsite or in the cloud), software and computer network systems. In this context, the technology is specifically referred to as internet telephony, or Voice over Internet Protocol (VoIP).

***What is Access & Event Management?*** Identity and access management is, in computer security, the security and business discipline that enables the right individuals to access the right resources at the right times and for the right reasons. Event management has been described as managing "logs." According to the National Institute of Standards and Technology's (NIST) *Guide to Computer Security Log Management,* "A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security."

***What is Governance & Policy Management?*** According to ISACA's COBIT® framework, a governance system is made up of organizational structures; principles, policies and procedures; information; culture, ethics and behavior; people, skills and competencies; and services, infrastructure and applications. Policies may also be integrated with other policy documents, such as privacy, human resource and corporate ethics.


Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

**FIGURE 1 | RISK IT FRAMEWORK**




© 2009 ISACA. ALL RIGHTS RESERVED.

ISACA's Risk IT Framework acknowledges and integrates the two realms by embedding IT practices within enterprise risk management, enabling it to secure optimal risk-adjusted return (**figure 1**).

In the framework, risk management processes are grouped into three domains—risk governance, risk evaluation and risk response. The interplay of these domains guides risk management activities, information flow between processes and performance management in the context of overall business objectives. By using the framework, enterprises can make appropriate risk-aware decisions as the framework addresses many issues that enterprises face today, notably their need for:

- An accurate view of significant current and near-future IT-related risk throughout the extended enterprise, along with measurements of success in addressing the risk
- End-to-end guidance on how to manage IT-related risk, beyond both purely technical control measures and security
- Understanding how to capitalize on an investment made to an existing IT internal control system to manage IT-related risk
- Understanding how effective IT risk management enables business process efficiency, improves quality and reduces waste and costs
- Integrating overall risk and compliance structures within the enterprise when assessing and managing IT risk
- A common framework or language to facilitate communication and understanding among business, IT, risk and audit management
- Promotion of risk responsibility and its acceptance throughout the enterprise
- A complete risk profile to better understand the enterprise's full exposure, so as to better utilize company resources

The Risk IT Framework positions IT risk as a component of the overall risk universe of the

Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

enterprise, alongside strategic risk, operational risk, compliance risk, credit risk, market risk and others. IT risk, however, is not an isolated category—it often influences all the other risks in the enterprise. For example, strategic risk can have an IT component, especially when IT is the key enabler of new business initiatives. The same applies to credit risk, especially when poor IT security can lead to a lower credit rating. For this reason, the preferred depiction of IT risk is not within a hierarchic dependency on one of the other risk categories, but as a horizontal risk category applying to all other individual risk categories. Viewing IT risk holistically through an enterprise lens helps organizations clearly see its broader operational impact, which in turn can spur improvements in decision making, collaboration and accountability.

## New Regulatory Requirements

Other factors that help bring IT and risk management together include regulatory requirements and privacy concerns. The regulatory risk environment that is part of an organization's ecosystem requires a collaborative effort among all business units, including IT and risk management professionals, to identify, analyze and address compliance and business obligations. While a cross-enterprise approach may address corporate data requirements like those promulgated under Sarbanes-Oxley, business services that deal with customer, consumer and personal information present a more challenging regulatory environment, as they may be subject to multiple requirements under the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) standards, and the Gramm-Leach Bliley Act. Added to this already complex environment are jurisdictional regulatory requirements, such as the EU's General Data Protection Regulation (GDPR), India's Personal Data Protection Act and California's Consumer Privacy Act.

Organizations collecting data should take care to understand the applicability of privacy and data protection laws that may exist across jurisdictions. Some regulations apply based on physical presence of data within national borders, while others may apply requirements based on the identities of those whose information is collected. Breach reporting requirements also vary, and legislation in some jurisdictions allows for the imposition of financial penalties far in excess of those seen in prior decades. Information linked to an individual, commonly called personally identifiable information (PII), may bring particular risk to an organization that collects it, especially if the data remain unmanaged or improperly safeguarded.

## The Value of Common Understanding

The colliding worlds of IT and risk management professionals can lead to a constructive and symbiotic relationship through enterprise risk management practices. The common mission and focus of IT and risk management professionals—to support the achievement of an organization's objectives—are evident in the following enterprise-focused definitions published by ISACA and RIMS respectively:

ISACA defines *enterprise governance* as a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, that risk is managed appropriately, and verifying that the enterprise's resources are used responsibly.

RIMS defines *enterprise risk management* as a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

These concepts are related and compatible. Collaboration between IT and risk management professionals facilitates strategic alignment of resources and promotes the creation of value across an enterprise. Good strategic alignment implies a virtuous circle. IT and risk management professionals can leverage their knowledge and resources to better inform decision makers on how business strategies and objectives can benefit from IT capabilities, and spur investment in new technology.




Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

# PART 2
## INTEGRATING RISK MANAGEMENT INTO THE TECHNOLOGY LIFE CYCLE

Collaboration between IT and risk management professionals can add value to an organization in a number of ways, including through:

- Coordinated procurement and contract review, resulting in more favorable terms and conditions, service level agreements (SLAs), and coverage terms
- Better incident response that enhances reputational protection
- Improved information protection through records and data management training
- Better assurance that controls are operating as intended through validation from multiple sources

In order to achieve optimal value, however, risk management should be a part of technology implementation from a project's outset and throughout its life cycle. By understanding the technology life cycle, IT and risk management professionals can identify the best opportunities for collaboration.

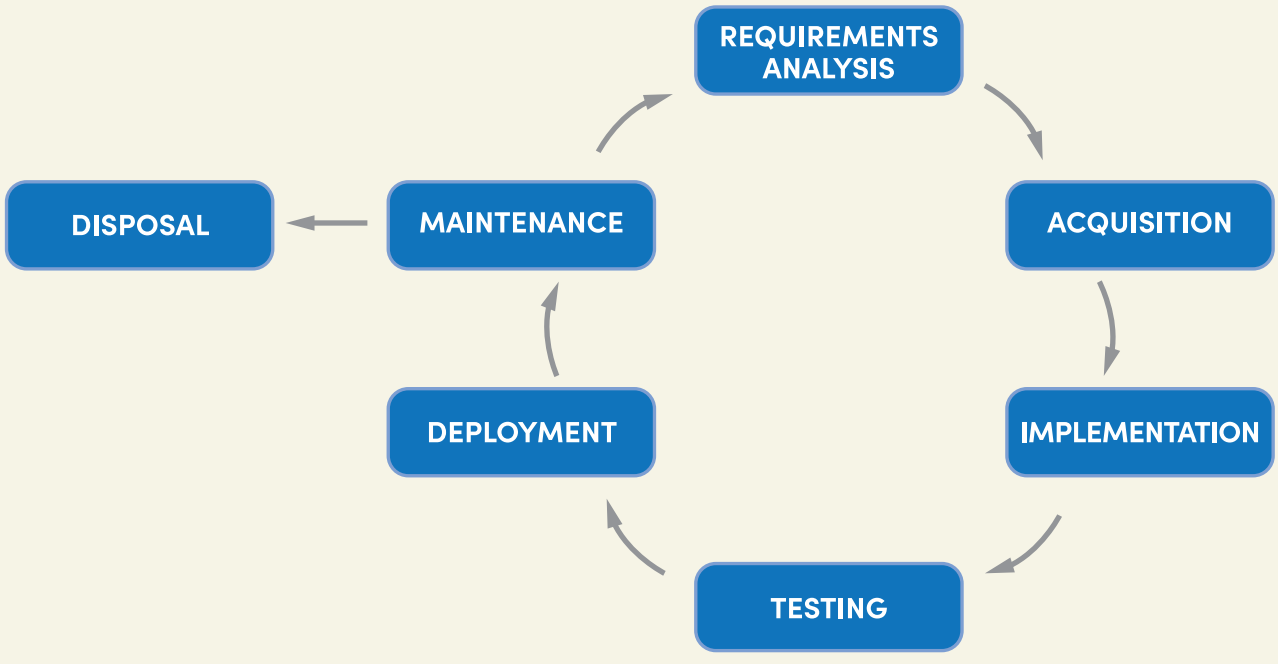
In general, technology follows a predictable life cycle (**figure 2**). The first step is requirements analysis, which progresses from a high-level concept to a formal definition tailored to an organizational mission or line of business. It is during the definition of requirements that an organization can most easily influence the course of the technology life cycle, because including or rejecting a requirement has little immediate cost. In particular, security requirements identified during the planning phase generally can be implemented with minimal effort, while adding security requirements during implementation can add considerable expense.

With requirements defined, the life cycle of technology then proceeds to acquisition, which may take the form of design and development, or identification of an existing product capable of fulfilling the requirements. The end state of this second step is to have technology that is ready for productive use.

Implementation is the third phase of the technology life cycle. This is the point at which the enterprise integrates the acquired capabilities into its processes, and the capabilities begin to play a role in value creation. The complexity of this step depends directly on the extent to which the requirements defined in the first step align with the processes that the technology means to support. Shortcomings in chosen solutions tend to become evident with the implementation of the acquired capabilities. At this stage, the cost of adapting to shortcomings can be considerable, imposing costs that may delay or impede value creation. Agile development methodologies prioritize getting technology into the hands of end users on an iterative basis, before a project is complete, allowing greater opportunities for mid-course corrective action. IT professionals increasingly realize that organizations are unable to envision their needs fully, even when substantial effort goes into the process of defining requirements.

Technology put into practice then undergoes testing, the fourth stage of the life cycle. Once implementation and testing are complete, deployment of the technology moves to full production, where it operates for its intended purposes and promotes value creation, and the life cycle proceeds to a maintenance phase. This phase continues in production, with upgrades included in the process of maintenance until such time as the technology is found to be irreconcilably deficient—the point at which continued upgrades are either technologically infeasible or fail to justify their cost relative to the benefits that they deliver. At this point,

**FIGURE 2 | TECHNOLOGY LIFE CYCLE**




Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

requirements analysis begins again to identify successor technology, whose implementation leads to the disposal of the technology that it replaces.

## The Role of IT Security

The requirements analysis phase is driven by the critical role that technology plays in facilitating value creation. But the potential consequences of risk (the effect of uncertainty on objectives) can result in impediments to or destruction of intended value, which contradicts the rationale for putting technology into practice in the first place. IT security solutions counterbalance this potential negative effect.

Security does not exist to *eliminate* risk, because security is not in itself a value-creating process. The role of security is to *manage* risk by balancing the cost of controls with a level of risk that is acceptable to an organization, so that value creation can proceed without undue impediment. Even where risk elimination is technically possible, that solution may not address the needs of the organization.

The function of IT security manages risk as part of its overall responsibilities, and effective technology implementation depends on identification of risk. Organizations have an array of tools and techniques available to identify risk as it relates to their particular lines of business and value creation, including brainstorming, the use of scenarios, consultations with subject-matter experts (SMEs) and evaluation of similar environments. Analysis follows identification, and may be qualitative, quantitative or semi-quantitative, and yields a basis on which to rank and classify specific areas of risk.

Affecting risk means modifying one or more of the components from which risk might arise: threat, vulnerability and impact. The role of IT security is to put in place controls that reduce vulnerability (thereby reducing likelihood) and/or the impact of negative consequences, a modifying "treatment" with specific intent commonly known as risk mitigation. Controls may be deterrent in nature, aimed at reducing the willingness of a threat actor to initiate a threat event. In most cases, however, mitigation focuses on reducing susceptibility to a threat or reducing the negative impact of a successful threat event. Within this context, preventative controls focus on vulnerability, while corrective controls focus on impact. Detective controls serve as monitoring capabilities to enable effective response to particular events.

Organizations have other choices for managing the negative consequences of risk beyond mitigation. Risk found upon analysis to be within levels that an organization finds acceptable needs no other treatment. On the opposite extreme, however, potential losses may be so high that deploying mitigation controls to acceptable levels is infeasible. In such cases, an organization may decide to avoid the risk of loss completely by ending a line of operations that creates the exposure. Organizations that need to modify potential financial impact to an acceptable level may use risk-sharing arrangements. Contractual instruments, such as insurance or service level agreements, serve to transfer some of the direct financial impacts of risk to a third party. Any of these approaches to risk treatment may be suitable and sufficient to address risk in a given context without reliance on IT security.

Even so, IT security has a critical role in risk management. Relatively few areas of digital risk are acceptable without some modification, and it is rare for an organization to deem a level of risk so high as to warrant avoidance. Risk sharing provides potential monetary relief but does not transfer full legal liability nor the potential longer-term effects on organizational reputation. Mitigation through deployment and maintenance of security controls, however, is within the direct control of the organization. Within this option, organizations typically deploy controls with two targets in mind: data and access.

## Data and Risk Management

Information systems exist to store, transfer and process data used in value creation, which makes data a focal point of information risk. Although specific threats to data come in nearly infinite forms, all threats affect one or more of three data characteristics:

- **Confidentiality**, or keeping data from those who should not have it
- **Integrity**, or maintaining data so that it remains suitable for use
- **Availability**, or making data accessible to those who seek it

The relative importance of these three characteristics varies. Understanding the context of a specific organizational process is essential to assigning proper weight to each of the three, as they can work at cross-purposes. For instance, error-correction mechanisms promote integrity but may impede availability by introducing delays in processing. Whether that is necessary, tolerable or unacceptable depends entirely on the context, which in turn requires knowing what data are used and how—something that requires a strong data management program.

Organizations create two types of data. Intentional data are created to serve a purpose. Processes for and in support of value creation generally yield this type of data in the form of records, outputs and logs that become part of the IT security tracking system. Intentional data also include information that IT security might not be aware of such as data created by users to facilitate low-level processes that are not formally documented. Examples of this sort of data include working papers, personal notes and logs enabled by a user and stored locally. Regardless of how the data was created or by whom, all data that is critical for a business process to function must be documented by users and included in an enterprise-level information inventory.

The other form of data that can exist within organizations is accidental data. Incomplete or flawed processes can create data without anyone's knowledge. Accidental data may create confidentiality problems, as in the case of a partially decrypted file or sensitive document discarded in the trash instead of being shredded. Accidental data can also introduce integrity problems if mistaken for valid production data. Careful testing and the use of logs and other detective controls to ensure awareness of incomplete or failed processes can mitigate this risk.

## Access and Risk Management

Managing access to data is another way in which organizations are able to manage risk. Balancing confidentiality and availability means ensuring access to those who need it while denying access to unauthorized individuals. The first step in this process is unique **identification** where someone attempting to gain access announces who they are (e.g., "I am John Smith."). Next is **authentication**, which involves verifying that the identity provided in fact corresponds to the identity of the actual requestor.

The process of authentication involves one or more of three factors:

- **Something you know**, such as a user name and password


Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.



- **Something you have**, such as a mobile device or electronic token
- **Something you are**, such as a biometric like a fingerprint, or other physical characteristics

Depending on the circumstances, one authentication factor may be sufficient; however, the reliability of authentication significantly improves with the combination of two or more factors. For example, organizations commonly use multifactor authentication at a physical or logical perimeter for initial access, then accept a single factor where access may be restricted inside the perimeter.

The process of identification and authentication establishes (within particular ranges of mathematical probability) that a requestor is who the requestor claims to be. Whether that results in effective access management depends entirely on how an organization leverages identity to control access. One leading practice in access management is least privilege, or the idea that someone should have as much access as needed to accomplish assigned tasks, but have no access beyond that. When combined with segregation of duties, which is the intentional assignment of different people to roles that must work together to accomplish some high-risk activity (such as an electronic funds transfer or the movement of newly written software code into a production environment), least privilege is highly effective at managing access risk.

Organizations are able to apply a least privilege model of access only when there is clear definition of user roles. When more than one user needs access, role-based access control (RBAC) facilitates the implementation of least privilege, with privileges granted to roles rather than individual users. In practice, RBAC can be difficult to implement effectively, as many individual user accounts are granted permissions for convenience or due to improper role delineation. Organizations sometimes also blur the lines between roles in an effort to increase operational efficiency, infringing on segregation of duties. The result may be a level of risk that the organization would find unacceptable, cloaked by an assumption that a least-privilege role-based policy is working as intended.

## Challenges of Managing Digital Assets and Related Risk

Management of risk relies in part on knowing what needs protection, which may be more difficult when dealing with digital assets rather than traditional items of value. Data creation happens accidentally as well as intentionally, and the presence of intentional data may not be known beyond the scope of those who create the data. Where the data is truly ancillary, the data's ambiguity may not have adverse consequences. However, without inclusion in a proper enterprise-wide digital inventory, data valuation naturally defaults to the subjective judgment of those who are aware the data exist.

Digital assets can be difficult to value even when identified. One challenge arises from sheer scale: Prices for storing data are very low and continue to fall, so organizations tend to retain more data than in prior decades. Often, the rationale for doing so is not that the data has any clear value, but, rather, that the lack of value cannot be positively determined—a "retain by default" approach that follows directly from the low cost of storage and the increasing sense that data may have unrecognized value. The cost of security applied to protecting an asset should generally be based on its role in value creation and the consequences (or impact) of its loss, if not safeguarded. Where the value of data is unclear, the value of protection is equally ambiguous.

The environment of general connectivity that defines typical information systems makes protecting digital assets more challenging. Network perimeters may be well established. Even so, internal controls safeguarding data within these perimeters may be lacking. Data with known sensitivity get highest priority, relying on the implementation of role-base access control (RBAC) and other least-privilege mechanisms with potential shortcomings. Similarly, data known to need (or substantially benefit from) protections of integrity or the guarantee of availability become a priority over unidentified data. As data proliferate, the majority tends to remain largely unmanaged, theoretically available to any user able to locate the data. Under these conditions, the practical safeguard against unauthorized access is often obscurity.

Organizations have begun to accept that the sheer volume of data makes broad-based protection relatively ineffective and are increasingly adopting a "citadel" model. In this model, high-value data reside in well-designed "walled-off" protective parts of the network, while other data goes unmanaged within the protections afforded by perimeter controls. The model is not substantially different in principle from the old reality, but there is an important difference in practice. Whereas the old model afforded varying levels of protection on the basis of inadequate or imprecise implementation, the citadel approach places considerable emphasis on knowing what data is being afforded strong protections and why. As a result, security controls link more closely with value creation, justifying risk mitigation efforts and expense.

Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

## Assurance of Controls

Organizations generally utilize three levels of defense: operations, risk management/compliance and audit. Once designed, built or directed through technology life cycle requirements, production staff implement and operate controls as they have primary responsibility for their successful use. System administrators, embedded in the value-creation process, are responsible for monitoring, upgrades and maintenance.

Compliance is a management function that exists in parallel to operations, encompassing activities such as quality compliance and independent validation. On a recurring basis, compliance staff work with production staff to verify the proper functioning of controls through techniques such as log review and the use of automated tools. In most cases, access to logs should be limited to compliance teams, with production staff not permitted to change or delete log entries. Ideally, failure of logging would generate an alert that triggers a timely investigation.

While production staff is strictly focused on creating value, compliance staff is focused on creating value in ways that meet security standards. This focus provides compliance staff with a greater likelihood of identifying variations in performance of controls that remain consistent with value creation goals but fail to meet security goals. Timely identification of such variations alerts management to take actions to manage risk effectively within tolerable levels. Compliance functions also facilitate reporting within organizations, helping key stakeholders in their understanding of deviations from acceptable risk targets.

The third level of defense is audit. Auditors typically operate independently of production and compliance teams for the benefit of those involved in enterprise governance, such as the board of directors. Auditors not only assess whether controls are operating effectively and efficiently, but also how well the monitoring capabilities and processes of the first two lines of defense are being carried out—the auditor "watches the watchmen." This function is most effective when auditors are dedicated to their task and do not assist in risk mitigation activities.

Those assigned to operations generally perform most "hands on" activity associated with controls. Compliance teams may have direct access to logs and monitoring tools but typically do not change system settings or modify controls themselves. Auditors, typically not integrated in operations, may request that production or compliance staff provide the evidence that they need for their work, such as extracted logs or answers to interview questions. This separation is intentional, since each successive layer of defense is most effective when it is distinct and focused on its intended role.

## Day-to-Day Risk Management

With controls properly designed and implemented throughout information systems, risk management on a day-to-day basis becomes a function of monitoring and reporting. Every detective control serves as a risk indicator, tracking some value that corresponds to a potential area of risk. Some controls monitor areas whose influence over value creation is substantial; these controls are highly correlated to outcomes and may serve as key risk indicators (KRIs), metrics whose performance provide a level of assurance that operations are proceeding within tolerable expectations or that risk may be exceeding acceptable levels.

In addition to detection, monitoring also extends to the maintenance of preventative controls and verification that corrective controls are working as intended. Production and compliance staff typically work together on a recurring basis to carry out these tasks.

Threat-hunting activities, vulnerability assessments, and manual or automated reviews of logged data all contribute to the overall picture of risk within an organization on a daily basis. Combined with the results of periodic internal or external audits, those responsible for risk governance are able to develop and maintain an understanding of risk as it relates to organizations at the strategic level.

Organizations seeking to develop risk management and governance programs may find it beneficial to adopt formal standards such as the ISO 31000 series. Leveraging a flexible framework may be a useful way to ensure that the functions of effective risk management are present in a tailored program. The U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework and COBIT 2019 are both examples of frameworks that help align business and security considerations in a context of risk.

Managers and technical experts should also keep in mind that the risk environment in which an organization operates is dynamic and requires regular reevaluation. Activities such as identification, assessment and treatment of risk are ideally iterative to ensure that the risk management program remains relevant.




Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

Where KRIs indicate elevated levels of risk—or where other monitoring capabilities reveal an aggregate level of risk constituting similar cause for concern—an organization may experience an event that warrants a coordinated reaction. Risk events reaching established thresholds may trigger developed processes for incident response. Although commonly associated with active attempts at network intrusion or other cybersecurity events, incident response is not purely an IT phenomenon. It is fundamentally a sequence of corrective controls and associated procedures, and may extend to processes that reduce workforce, facility or organizational impacts, such as emergency evacuation or crisis management.

## Legacy and Industrial Systems

One situation that can arise in organizations is an inability to manage risk directly within a specific system. In certain industrial processes, for example, technology must operate on a nearly real-time basis in order to provide adequate safety (such as in a power plant). The need for unimpeded processing makes availability the highest priority, with integrity accorded a second-place role. Confidentiality necessarily balances against this business need within such a system, because the ability to prevent access is fundamentally at odds with nearly real-time processing under conditions of safety. However, managing the risk posed by accidental lockouts creates conditions that exacerbate the risk posed by malicious activity.

Industrial controls and older legacy systems also tend to be custom integrated, with upgrades considerably more difficult to perform than in contexts of office automation. As a result, industrial controls and other forms of legacy computing may not be able to accommodate modern preventive controls even when one takes processing speed out of the equation. The obvious solution to this situation is to replace the systems, but that may be cost prohibitive, especially when the systems play central roles in value creation.

In cases such as these, organizations may choose to deploy compensating controls, which exist outside of the systems that create the unacceptable risk but influence them in ways that bring the risk to an acceptable level. For instance, an unmodified industrial system might be placed on its own network segment, isolated from other traffic, with all access brokered through an internal security perimeter that provides strong authentication and ensures the confidentiality of the data by denying outside access. When considering the risk associated with any system, and especially industrial or legacy systems, it is important to take into account the effect of any compensating controls.

## Cross-Disciplinary Collaboration

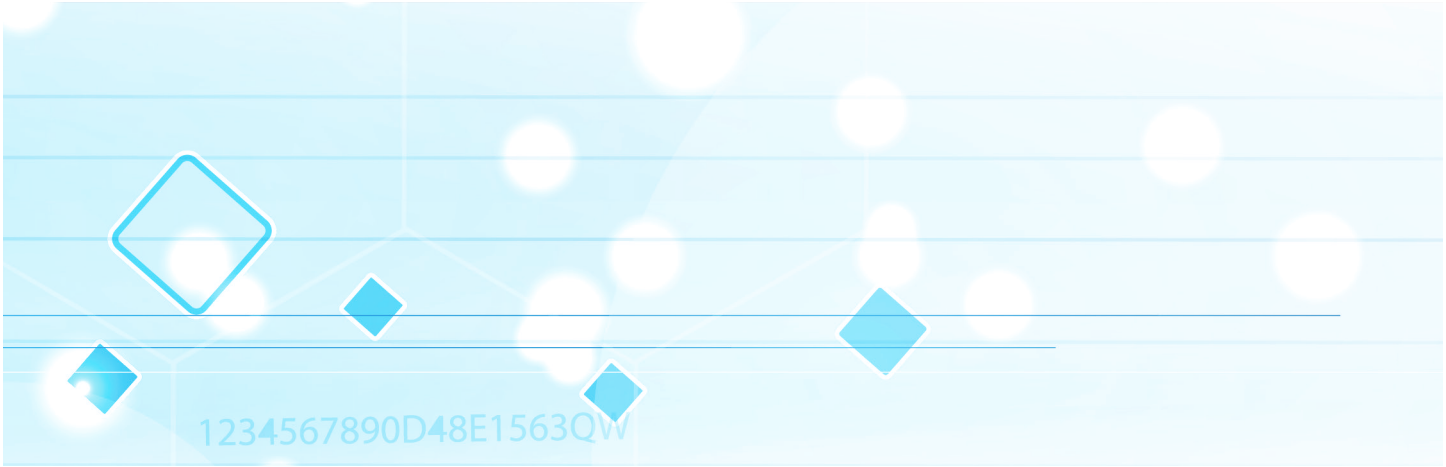
Risk management in a digital world necessarily places IT security and risk management professionals in a collaborative role. However, other functions also play important roles. Logical security controls established within networks and systems are vulnerable in environments where physical access is unrestricted, so risk management relies in part on the efforts of facilities managers and traditional security staff.

The compliance function tends to be broad-based and typically extends beyond IT functions such as contract adherence and code of conduct. Internal auditors provide assurance that systems and processes are operating as expected. As such, internal auditors generally are independent of IT security. External parties may be engaged in audits, particularly in industries that are subject to public regulation.

Organizations have alternatives to mitigation when it comes to managing risk, one of which is the transference of risk through third-party sharing agreements. Mechanisms such as service level agreements should undergo legal and risk management review. Consultations with attorneys are advisable in cases where incident response creates forensic evidence, particularly in cases where an organization is able to identify responsible threat actors and is weighing the merits of seeking criminal prosecution.

Typically, a corporate insurance and risk finance function manages risk sharing to protect the balance sheet by providing funding in the event of loss. Purchasing teams also play a role in obtaining any third-party technology or acquired services. In such cases, IT security staff may need to serve as SMEs to ensure that identified products and vendors meet security requirements, and risk management professionals may need to serve as SMEs in assessing the business risk and insurance requirements related to the third-party relationship.

Finally, there is the broad trend towards consolidation of strategic oversight of all risk management functions at the enterprise level. This move towards integration—whether in a formalized governance, risk and compliance (GRC) structure or organizationally through a chief risk officer—does not infringe on the specialized expertise of IT security. Rather, IT security and the other roles provide subject-matter expert support in terms of both planning and monitoring to deliver value to the organization as a whole.




Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

# PART 3
## INTEGRATING FRAMEWORKS, ROLES AND METHODS

IT and risk management professionals both employ various tools and strategies to help them manage risk. Although the methodologies used by the two groups differ, they are generally designed to achieve similar results. By integrating these frameworks, roles and methods, IT and risk management professionals can better coordinate their efforts to address threats and create value.

### Integrating Frameworks

There are several frameworks available to facilitate cybersecurity risk management. Many organizations choose to adopt the framework made available from the U.S. National Institute of Standards and Technology (NIST), because it is comprehensive, regularly updated, easily tailored and available at no cost. NIST's Cybersecurity Framework, which is designed to be voluntary and not regulatory, is a prioritized, flexible and cost-effective approach that helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

Its design specifically incorporates the framework into a comprehensive ERM program. Two important elements of the framework are: 1) the use of cyberrisk assessments in the larger organizational environment of mission, functions, reputation, assets and individuals to **Identify**, **Protect** and **Detect**, and 2) risk management strategies related to the organization's overall priorities, risk tolerances and assumptions for taking operational decisions that help an organization **Respond** and **Recover**.

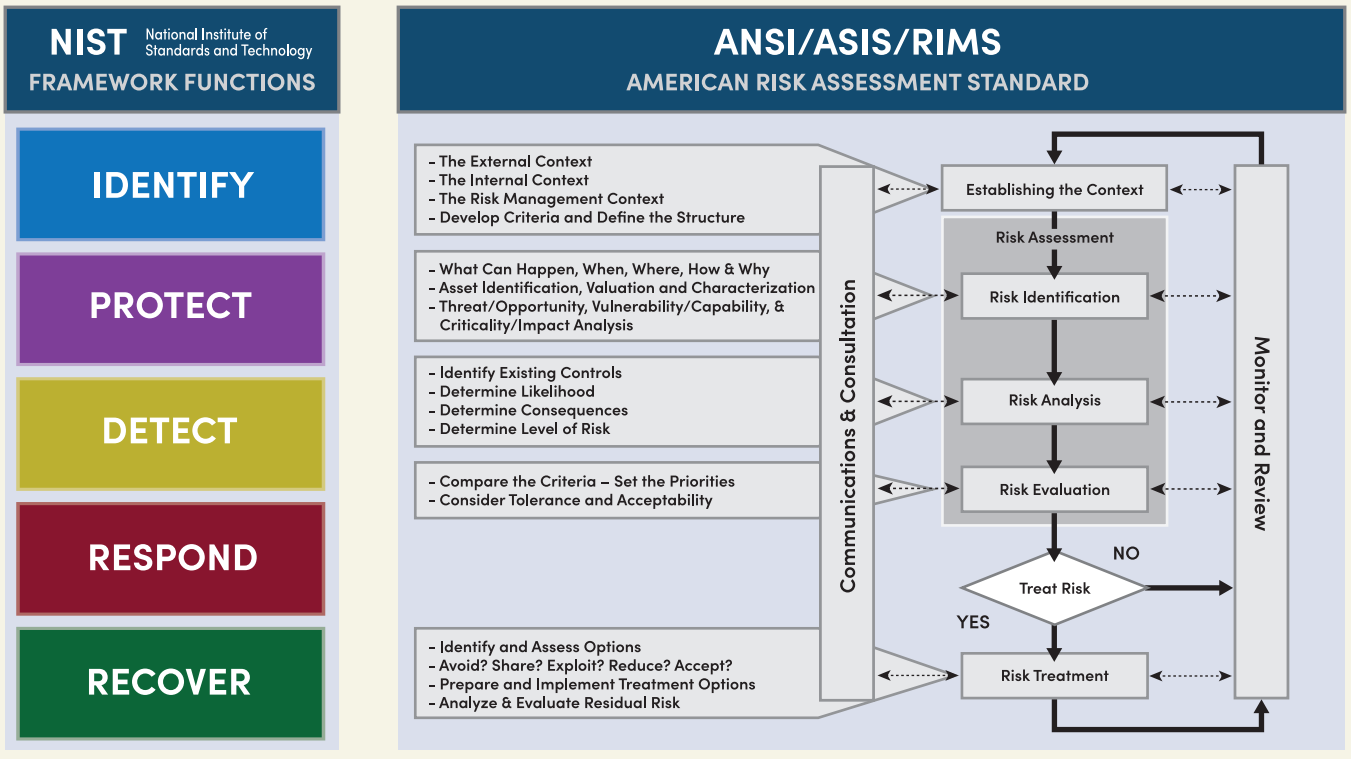
As an illustration of how closely the NIST Cybersecurity Framework integrates with enterprise risk management, the risk process from the American National Standards Institute (ANSI) risk assessment standard RA.1, developed jointly by the security industry professional association, ASIS International and RIMS, aligns with the NIST Framework functions (**figure 3**).

While both reflect high-level processes, the NIST Cybersecurity Framework is a more detailed prescription for specific action that has already integrated risk tolerance decisions into a set of policies and response thresholds that security professionals rely on to execute with minimal deliberation. The ANSI RA.1 standard complements this approach by providing a meaningful process for that deliberation.

Generally, practitioners from both professions start with a baseline of business objectives and the establishment of context to enable the application of risk-based decision making. Supporting executive decisions requires having a means to understand the what, when and how to accept risks.

The ANSI RA.1 standard considers identification, analysis and evaluation of business impact scenarios, while NIST's Protect element focuses on establishing policies, standards and protective mechanisms that complement the assessment process. NIST's Detect function focuses on monitoring the environment—including compliance with policies and standards, but also effectiveness of an organization's protective mechanisms.

**FIGURE 3** | ALIGNMENT OF NIST CYBERSECURITY FRAMEWORK AND THE ANSI/ASIS/RIMS RISK ASSESSMENT STANDARD





Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

Both follow a process that requires decision making regarding action post-evaluation. The ANSI RA.1 standard has more options such as sharing, avoiding, accepting, reducing and exploiting. The NIST framework assumes that defined thresholds for various responses already exist in accordance with an organization's tolerance.

Lastly, both are similar in that they reflect a closing element to a risk assessment process. They both include the preparation or communication with stakeholders. Despite this commonality, there are important differences—the ANSI RA.1 Standard references recording and reporting as a basis for programmatic review while NIST's Recover function reflects a specific communication regarding re-establishment of a normal operating environment.

## Integrating Roles

Successful organizations do not create a separate risk governance structure for their risk management practices. Rather, they integrate risk management into existing governance arrangements based on process, framework and technical design. As noted in the ISO 31000 standard on risk management, "The effectiveness of risk management will depend on its integration into the governance of the organization, including decision making. This requires support from stakeholders, particularly top management."

Accountability for managing risk, at times referenced as "risk ownership," is an important aspect of the technical design of risk governance. For example, there should be clear understanding of roles, responsibilities and accountability within the governance structure. Documentation of risk commitment that is either informal or formal (such as risk management policies, procedures, common vocabulary and standards) typically are included in an organization's overall governance arrangements.

Cyberrisk management falls naturally into both strategic and operational risks due to the ubiquitous use of technology. At times, strategic and operational risks become the oversight responsibility of the entire board, rather than delegated to a board committee.

Traditionally, organizations have assigned accountability through divisions defined by product line or function. As organizations become increasingly dependent on technology, IT infrastructures are moving beyond support services to become production functions and key enablers of value creation. This expanded role warrants and demands expanded accountability. Technology no longer pertains simply and solely to an IT department, and accordingly, should no longer be subject to the isolated decisions of one executive. Where technology drives the entire business, the entire business needs to care about technology.

Visualizing roles through a responsibility assignment matrix within the IT ecosystem recognizes the ubiquitous nature of technology, while acknowledging the cross-functional expertise needed for enterprise IT risk management. Using the four foundations of the IT infrastructure (governance and policies, access and event management, platform peformance, and network reliability), **figure 4** depicts the overarching leads and management elements within each foundational area.

Executive support for an ERM-based approach within the corporate culture determines the success of integration for an enterprise IT risk management approach, which is generally sponsored by a chief information officer (CIO) or chief information security officer (CISO). IT and risk management professionals may co-lead in engaging the various functional-area leads and in providing program support, proj-

**FIGURE 4 | ENTERPRISE IT RISK MANAGEMENT RESPONSIBILITY ASSIGNMENT MATRIX**




© 2019 RISK & INSURANCE MANAGEMENT SOCIETY. ALL RIGHTS RESERVED.

Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved. 

ect management, metrics and benefits, managing related accounting issues, and developing collaborative risk assessments and action plans.

Risk management activities within organizations committed to an integrated ERM-based approach go beyond regulatory compliance. An integrated program should include an accountable lead for governance and policies, typically led by someone in the legal department. In addition to internal policy development and regulatory compliance, this area may address issues such as physical security, vulnerability protection, and employee education and awareness. Specific IT areas may require separate IT leads for access and event management (identity and access management and reporting), platform performance (standards, encryption, data storage and securing systems and applications), and network reliability (firewalls, intrusion, wireless and IoT integration).

While IT and risk management professionals may start and end at different points in the regulatory risk framework, both sets of professionals are key enablers of value creation by leveraging their respective risk frameworks to ensure organizational objectives are met. On its face, this may seem duplicative; in practice, this integrated approach is complementary and reinforces desired organizational behaviors.

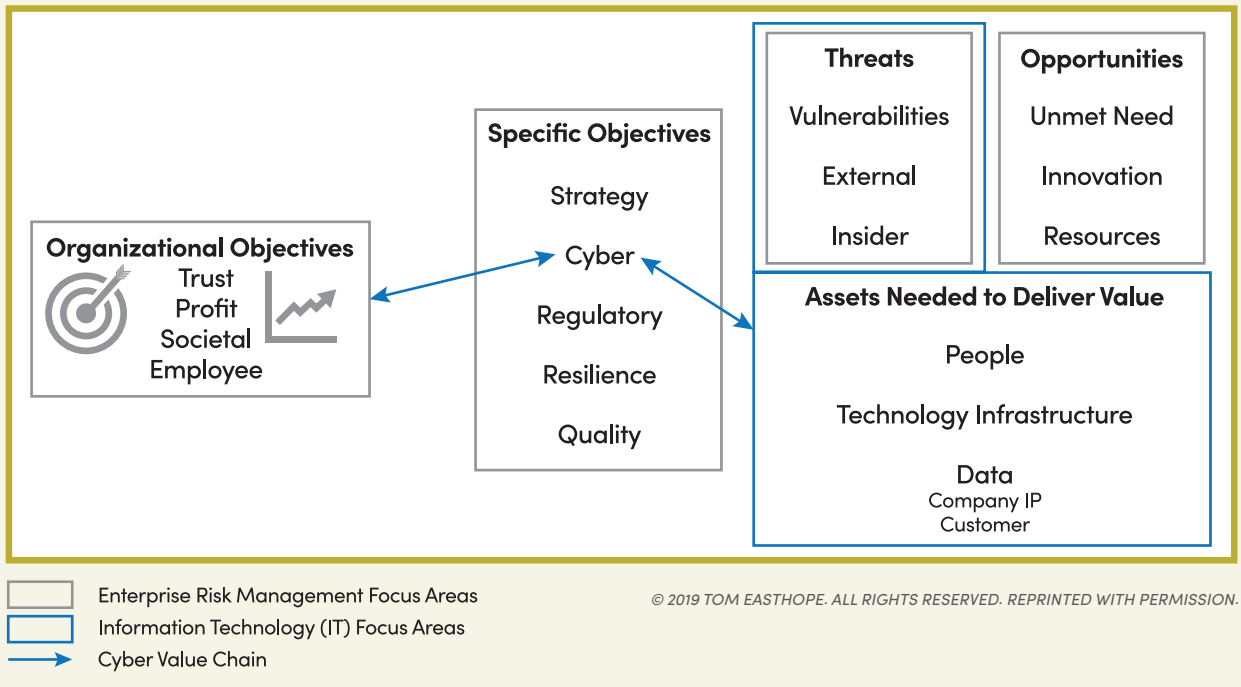
## Integrating Methods of Assessment

Collaboration and communications processes in IT security are similar to those used in enterprise risk management, but with different, though complementary, objectives and different terminology. IT security processes typically tend to support an asset-based, control-centric approach to risk reduction, while enterprise risk management processes generally support management of both downside and upside risk associated with uncertainty and volatility in achieving business objectives. Most organizations already have controls established against commonly and widely understood risk, such as business disruption, environmental and execution failure, among others. What tends to be missing is a set of common methods for assessment and conducting root cause analyses that tie control actions to both the risk appetite of the organization and to its strategic objectives.

**Figure 5** depicts the cyber value chain as a key part of ERM's focus on an enterprise's organizational and specific business objectives. From an assessment process perspective, information security typically identifies assets, then threats to those assets and the assets' vulnerability to those threats. ERM typically identifies overall organizational and business objectives—along with the integrated processes necessary to meet specific objectives—and seeks to reduce uncertainty in achieving those objectives, whether from threats or in uncovering and executing opportunities.

Rather than focus on asset profiling, ERM processes typically identify where, when, why and how business model, market, events, operations, third parties and other elements associated with business changes, issues and others—whether known or underreported—might prevent, degrade or support goals. In doing so, risk management professionals also analyze perceived uncertainties and opportunities through consistent, objective and pervasive assessment evaluation criteria, such as impacts, likelihood, assurance (effectiveness of controls) and other variables, such as speed to onset and time horizon, to determine potential consequences and the estimated risk level relevant to business objectives. For example, risk management professionals may use a value chain analysis to analyze internal firm activities in order to recognize which activities are the most valuable to the enterprise and which ones could be improved to provide competitive advantage. Through this business process mapping, untapped opportunities may be uncovered where an unmet market need can be addressed through innovation given sufficient

**FIGURE 5 | ASSET PROFILING VS. BUSINESS PROCESS MAP**




© 2019 TOM EASTHOPE. ALL RIGHTS RESERVED. REPRINTED WITH PERMISSION.


Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

resources. The same assets that may be profiled by IT in its assessment would also underpin new innovation and products to meet specific objectives.

Many other assessment methods used by IT and risk management professionals are similar on the surface, but actually have slightly different objectives. Integration efforts should consider the key differences between them in case adjustments need to be made to achieve desired outcomes. Some examples include:

- *Threat Modeling vs. Scenario Analysis.* Specific technical and process controls employed for IT security are often selected and prioritized following modeling of various potential internal and external threats to the confidentiality, integrity and availability of critical information and technology assets with focus on preventing or stopping the worst threats and/or limiting the impact of realized threats. ERM, which is focused on achieving business objectives, often employs scenario analysis—first, to identify threats and opportunities, then to identify and prioritize modification strategies, which narrow the range of uncertainty and volatility to bring an organization's exposure in line with its risk appetite/risk tolerance.
- *Incident/Vulnerability vs. Loss Events.* When a cybersecurity event occurs, resulting in potential or actual loss of confidentiality, integrity and/or availability of information or technology assets, IT security employs well-orchestrated collaboration and communication processes to address it. Often, this response involves key enterprise stakeholders who investigate, respond and contain the event, usually via technical mitigation activities. ERM focuses more broadly on quantifying risk, reducing financial impact to the organization, and identifying and managing cross-functional exposures—which, in turn, may trigger subsequent events such as legal, regulatory or contractual notification and reporting; payment of fees, fines or damages to impacted parties; and handling of claims.
- *Controls Assessment vs. Management Effectiveness.* While differences between these processes are minor, they are worth noting. Cyberprofessionals work at a more granular level, with established thresholds and tolerances for known scenarios. Their intended outcome is that controls work as designed. ERM, on the other hand, operates more broadly by looking at management's effectiveness in creating culture, intelligent decision making and prioritization. ERM also considers the potential to exploit a risk proactively for a positive outcome, while information security's control assessment is limited to the prevention of a negative outcome.

Overall, coordinating assessments of risk and capabilities through both IT and risk management lenses creates value by improving communication and bringing additional resources to the assessment processes. This allows organizations to improve performance by identifying a broader range of risks and potential mitigations, and ensures that operations are proceeding within acceptable risk tolerances. In addition, providing the organization's board with a collaborative risk assessment and coordinated action plans builds trust, resulting in additional funding for IT and other business investments. Leveraging the respective assessment techniques also leads to more informed underwriting—and thus improves pricing of insurance programs, terms of coverage, products and services.

## CONCLUSION

Many organizations struggle to align risk functions in support of common interests because of communication difficulties between the different functions. Lacking a common taxonomy, professionals in information security and risk management may not realize that they are performing substantially similar activities with different areas of focus. For instance, risk identification in an information security context typically begins with identification and valuation of information assets and proceeds from there to identifying possible threats and assessing vulnerabilities. In contrast, risk management professionals may use business processes as a starting point for identifying risk, beginning with delineation of objectives and then seeking to reduce the uncertainty associated with attaining them.

These are extremely similar practices. Preserving information assets is the primary objective of an organization's information security function, and the combination of threat and vulnerability defines uncertainty as a probability value. Risk management scenario analysis is closely related to cybersecurity threat modeling. Despite this commonality, people working in cybersecurity and risk management tend to regard one another's roles as unrelated. Developing clear, common language and mutual understanding can serve as a strong bridge to unite the cultures, bring risk management functions together and create significant value for organizations that make the effort.

Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

# APPENDIX A

## Mapping ISACA's Risk IT Framework and the RIMS Risk Maturity Model

ISACA's Risk IT Framework focuses on three domains: risk governance, risk evaluation and risk response. Each domain is comprised of three processes, which align well with the RIMS Risk Maturity Model's seven attributes.

### Three Domains in ISACA's Risk IT Framework

- **Risk governance** – The objective of this risk domain is to ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. The domain is made up of three processes:
  - > Integration with ERM
  - > Establishment and maintenance of a common risk view
  - > Making risk-aware business decisions
- **Risk evaluation** – The objective of this risk domain is to ensure that IT-related risks and opportunities are identified, analyzed and presented in business terms. The domain is made up of three processes:
  - > Analysis of risk
  - > Collection of data
  - > Maintenance of risk profile
- **Risk response** – The objective of this risk domain is to ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities. This domain is made up of three processes:
  - > Management of risk
  - > Articulation of risk
  - > Reaction to risk

### Seven Attributes of the RIMS Risk Maturity Model (RIMS RMM)

1. **ERM-based approach.** Gaining executive support within the corporate culture.
2. **ERM process management.** Integrating ERM into business processes.
3. **Risk appetite management.** Establishing accountability within leadership and policies to guide decision making.
4. **Root cause discipline.** Binding events to their process sources.
5. **Uncovering risks.** Performing risk assessments to document risks and opportunities.
6. **Performance management.** Executing organizational vision, mission and strategy through outcomes-based measurements.
7. **Business resiliency and sustainability.** Integrating ERM into operational planning and execution.

## Crosswalk between ISACA's Risk IT Framework and the RIMS Risk Maturity Model

| Three Domains in the Risk IT Framework | Attributes of RIMS Risk Maturity Model (RMM) |
|---|---|
| Risk Governance | 1, 2, 3 |
| Risk Evaluation | 4, 5 |
| Risk Response | 6, 7 |


Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

# APPENDIX B

## Glossary of Risk Management Terminology (from *RIMS Strategic Risk Management Implementation Guide*)

**Base case** the set of reasons, arguments and supporting facts offered in justification of a chosen strategy. It refers to the expected strategic plans an organization will be taking, and what the future outcomes would be if planning assumptions materialize. The concept also may be referred to as a base case scenario.

**Control framework** a management structure that unifies isolated risk control approaches into a collectively motivated control environment in which all control functions are focused on achieving the organizational objectives.

**Core competency** a particular strength relative to other organizations that provides the fundamental basis for added value and strategic advantage.

**Deal killer risks** uncertainties that, if left unresolved, could undermine the entire objective or venture.

**Dynamic risks** risks that are known to exist, but may change over time.

**Economic buyer** the individual within an organization that is the ultimate purchaser of products or services for an organization. In most instances, the economic buyer is also the responsible decision maker, who may or may not have operational responsibility for the products or services purchased. For example, the corporate chief financial officer or treasurer may be the economic buyer of insurance, with the corporate risk manager being the "user buyer," defined as the individual responsible for the implementation of products or services purchased.

**Emerging risk** a novel manifestation of risk or type that has not been experienced previously.

**Emerging risk sensing** the range of activities carried out to identify and understand evolving sources of risk that could have a significant impact to the organization.

**Enterprise risk management (ERM)** a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio.

**Environmental scanning** a process of systematically exploring and interpreting a broad array of macro- and micro-surroundings to identify trend indicators to better understand the drivers of change and to gauge their potential future impact on the organization.

**Integrative thinking** the ability to hold two seemingly opposing ideas in one's mind at once, and then reach a synthesis that contains elements of both but improves on each to create a new approach or direction. Integrative thinkers do not accept either/or solutions.

**Key risk indicator (KRI)** a measure to indicate the potential presence, level or trend of a risk.

**Lagging indicators** measures that develop parallel or subsequent to a development or trend (e.g., the development of housing prices is a lagging indicator for the economy).

**Leading indicators** measures that develop in advance or in parallel to a development or trend (e.g., the number of orders for heavy equipment and raw supplies is a leading indicator for the economy).

**Opportunity** a favorable or advantageous combination of circumstances and/or a pertinent occasion or time that may improve an organization's position if acted upon.

**Path dependent risks** risks that arise when pursuing the wrong path or direction would involve wasting huge sums of money or time or both.

**Resilience** the capability and capacity of an organization to reorganize under change and deliver its mission continually, despite the impact of external or internally generated risks.

**Risk** an uncertain future outcome that can either improve or worsen an organization's position.

**Risk appetite** the total exposed amount that an organization wishes to undertake on the basis of risk-return trade-offs for one or more desired and expected outcomes. As such, risk appetite is inextricably linked with—and may vary according to—expected returns. Reflective of an organization's business strategy, risk strategies and stakeholder expectations, risk appetite generally is set and/or endorsed by the board of directors through discussions with management. Risk appetite statements may be expressed qualitatively and/or quantitatively and managed with respect to either an allocated individual initiative and/or in the aggregate.

**Risk attitude** the organizational or individual's perceived qualitative and quantitative value that may be gained in comparison to the related potential loss or losses. Attitudes toward risk may range along a continuum from risk taking to risk averse.

**Risk driver** a factor that has a strong influence on the eventual outcome or result, that is, on whether or not key objectives will be achieved.

**Risk fluencies** an individual's technical ability to conceptualize, converse and execute actions utilizing a specific risk management lexicon. If one assumes that the "language of risk" is one that requires conceptual and contextual mastery, the level to which risk a practitioner is "fluent" in the language will determine the practitioner's overall level of understanding and ability to deliver results. Risk fluencies may also refer to the overall understanding and use of the applied risk lexicon within the organization.

**Risk intelligence** the ability to weigh risks effectively, and involves classifying, characterizing and calculating threats and opportunities; perceiving relationships; learning quickly; storing, retrieving and acting upon relevant information; communicating effectively; and adjusting to new circumstances. Risk intelligence reinforces risk resilience.

**Risk tolerance** the amount of uncertainty an organization is willing to accept in the aggregate (or more narrowly within a certain business

Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.

# APPENDIX B

unit or for a specific risk category). Expressed in quantitative terms that can be monitored (such as volatility or deviation measures, for example), risk tolerance often is communicated in terms of acceptable/unacceptable outcomes or as limited levels of risk. Risk tolerance statements identify the specific minimum and maximum levels beyond which the organization is unwilling to accept variations from the expected outcome.

**Root cause analysis** a systematic approach for identifying and assessing risks whereby a defined risk is analyzed through questions such as "what can make this happen?"

**Scenario planning** a structured way for individuals or organizations to think about multiple plausible ways in which the future might unfold. The technique is used to inspire imagination and provoke "thinking the unthinkable," thereby increasing emerging risk sensing. Alternate definition from Art of the Long View, Peter Schwartz (1996): a tool for ordering one's perceptions about alternative future environments in which one's decisions might be played out. Alternately: a set of organized way for people to dream effectively about one's (or collectively an organization's) own future. This is a disciplined way of thinking more than a formal methodology.

**Stakeholder** any individual or organization that is directly or indirectly involved with or affected by an organization's decisions and activities

**Strategic risks** internal or external uncertainties, whether event or trend driven, that impact an organization's strategies and/or the implementation of its strategies.

**Strategic risk assessment** a systematic and continual process for assessing the strategic risks facing an organization.

**Strategic risk management (SRM)** a business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization's strategy and strategic execution.

**Strategy** a complete plan of action for whatever situations may arise in achieving an organization's goals within the established time. An organization's strategic plans will determine the actions the organization will take at any stage of the planning period as circumstances change.

**Value** created when an organization makes products or delivers services that people outside the organization find to be worthwhile, useful, convenient, effective or otherwise desirable or of some importance to the processor or user.

**Values** an organization's cultural beliefs and behaviors that form the foundation on which the organization performs its work and the way the people within the organization conduct themselves; sometimes referred to as core values.

**Volatility** the level and speed of change over time and against a norm or expected state. Antonym: stability.

## Glossary of IT Terminology *(from ISACA)*

**Compensating controls** are alternative technical or non-technical safeguards, put in place to mitigate risk(s) when a security measure is deemed too difficult or impractical to implement.

**Incident response** is the response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people or its ability to function productively. An incident response may include evacuating a facility, initiating a disaster recovery plan (DRP), performing damage assessment and/or other measures necessary to return the enterprise to a more stable status.

**Least privilege** is an information security principle. Least privilege reflects the practice of limiting the access rights of users to the bare minimum permissions they need to perform their work. A user (or an application, depending on the subject) will be granted permission to read, write or execute only those files or resources appropriate to legitimate purposes.

**Personally identifiable information (PII)** includes any information that could possibly identify a particular individual including any data that can be used to differentiate one person from another. Examples include a full name, Social Security number, driver's license number, bank account number, passport number and email address.

**Requirements analysis** is the process of identifying quantifiable and detailed user expectations for a new or modified product. It includes determining the needs necessary to meet a new or updated product or project. The process must take into account conflicting expectations of all stakeholders.

**Role-based access control (RBAC)** restricts access based on an employee's role within an organization. Typically used in very large organizations with many users to simplify the security administration process with hundreds of users and thousands of permissions.

**Segregation of duties** is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. Segregation/separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

**Software development life cycle (SDLC)** is a framework used to design, develop and test high-quality programs. It is a process followed by development teams, which consists of a detailed plan describing how to develop, maintain and replace specific software.


Copyright © 2019 Risk and Insurance Management Society, Inc. (RIMS) and ISACA. All rights reserved.