RISK

# GETTING STARTED WITH RISK MANAGEMENT

ISACA®

# CONTENTS

# ABSTRACT

Although most enterprises have some sort of risk management, it often lacks the depth and specificity required by the business environments and risk landscapes in which they operate. The main drivers for risk management include improving enterprise decision-making, aligning resources to focus on risk with the greatest potential impact and ensuring value creation by maintaining risk within acceptable tolerances and appetites. This white paper illustrates how to structure risk management activities so that they fit the unique operating landscape of your enterprise.

# Introduction

Most enterprises have some form of risk management. Often, however, it is *ad hoc*, compliance based and reactive, primarily intended to address the latest threat in the news; in this context, risk management activities can reflect uncoordinated, arbitrary measures that fail to analyze risk and determine whether it warrants action. As a result, enterprises lack a systematic and coherent approach to risk management and may fail to achieve the greatest potential business or mission impact.

*COBIT® 5 for Risk*[1] presents two perspectives on how to use COBIT 5 in a risk context—risk function and risk management:

- **Risk function** perspective focuses on building and sustaining risk activities within an enterprise.
- **Risk management** perspective focuses on core risk governance and management processes for optimizing risk management.

The purpose of this white paper is to facilitate discussion on the risk management perspective, setting the context for risk management as a discipline that requires practitioners to consider their unique operating environments and risk landscapes when designing risk management processes. The white paper provides a practical, high-level view for an enterprise to understand risk management activities and other considerations that may be important to implementing and formalizing risk management processes. While the paper presents illustrative examples, it is not meant to be prescriptive or complete, though its guidance is applicable to any type of enterprise—commercial or noncommercial, public or private and small, medium or large.

This white paper describes how core risk processes are informed by the risk function perspective and the risk management perspective. **Figure 1** shows how the two perspectives use the COBIT 5 enablers to build and sustain a risk function and help mitigate risk.

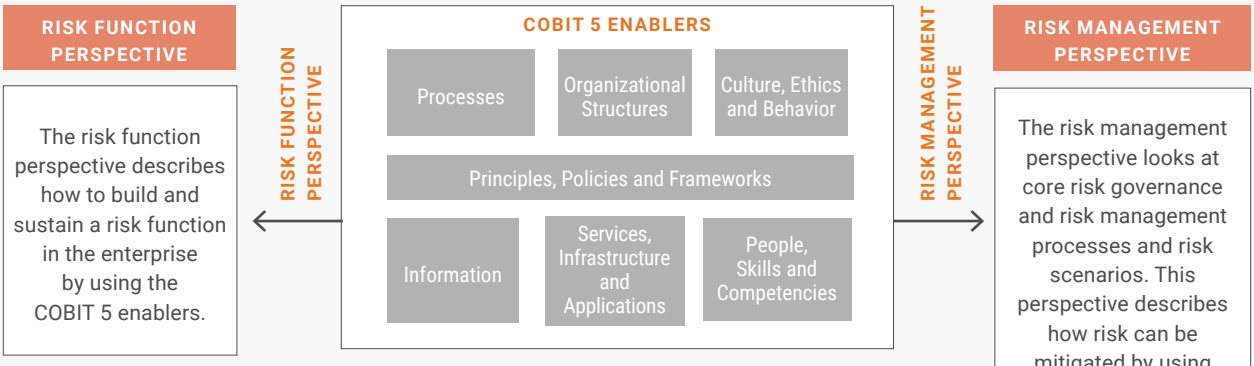


**FIGURE 1:** Two Perspectives on Risk

Source: ISACA, *COBIT® 5 for Risk*, USA, 2013, pg. 19, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

1 ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

## Risk Management and Its Benefits

To understand the practical aspects of risk management as a discipline, one first needs to understand the term risk. One dictionary definition of risk is:

> *A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.*[2]

Although the word risk is often associated with avoiding hazards or negative impact from an event or circumstance, that is not the only definition. ISACA uses the International Organization for Standardization (ISO) definition of risk, which combines "the probability of an event and its consequence."[3]

Enterprises exist to produce products and deliver services and generally have strategies, goals and objectives to achieve as part of their mission. In formulating a business or operational strategy, an enterprise often decides explicitly to accept some level of risk to achieve its objectives.[4] Risk management is an organizational discipline that identifies, analyzes and addresses risk whenever it carries the potential to jeopardize the enterprise's stated goals and objectives; combined with strategic planning, risk management ensures that risk remains commensurate with the enterprise's risk appetite and tolerance.

Explicitly defining risk appetite and understanding tolerances for different types of risk are important components of risk management. Risk appetite is the amount of risk that an enterprise is willing to accept to meet its strategic objectives. Risk appetite can be expressed in qualitative or quantitative terms. For example, an enterprise wants to expand its current service-desk call center to better serve its customers and must allocate US $10 million to fund the project, buy equipment, hire staff and provide training. The business has a defined and stated risk appetite of $10 million to achieve this objective. Risk tolerances reflect the thresholds or guardrails that help management determine when identified risk exceeds the risk appetite. In the call center example, the enterprise should determine the variation from risk appetite that it will accept before taking action; there may be tolerances, or acceptable variations, for example, with regards to staffing, dates for delivery of technology equipment or availability of facilities to house the call center. The risk tolerances may be expressed as a statement, such as, "The project budget is US $10 million; however, the acceptable range of spending is $8 million to $12 million." If the project is completed successfully for $12 million or less, then the risk has been managed within defined tolerances. An effective risk management process enables the enterprise to make better-informed decisions about accepting risk to create value and managing risk to minimize negative impact on organizational objectives.

Risk management is not merely a function or a department, nor is it only limited to internal controls. Risk management comprises the activities and culture that an enterprise undertakes to create and preserve value when meeting its strategic objectives. Many frameworks, techniques or methods may be used by an enterprise to establish and maintain the capability for

2 BusinessDictionary, "risk," 2017, *www.businessdictionary.com/definition/risk.html*

3 International Organization for Standardization (ISO), "Risk management – Vocabulary," ISO Guide 73:2009, November 2009 (reviewed and confirmed, 2016), *www.iso.org/standard/44651.html*

4 While this discussion focuses primarily on resources and activities to minimize business impact from a realized risk, the upside view of risk must also be considered when thinking about a risk management approach.

managing risk in a way that is efficient and effective. Whether risk is administered holistically (as in enterprise risk management) or managed as a single type or category (such as compliance or cybersecurity), the underlying principles of the risk management process apply. This white paper presents some common risk management approaches as illustrative examples, to help enterprises set the context for risk management.

Enterprise risk management (ERM) is defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as:

> *a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*[5]

The ERM view is most closely associated with the three-lines-of-defense (3LoD) model[6] that has become a common industry practice for managing risk in the financial sector. The 3LoD model is not limited to enterprise risk management and can be used for all risk types under management.

Operational risk management (ORM) focuses on day-to-day, front-line activities and associated risk related to operating the business or meeting its mission. The Basel Committee on Banking and Supervision defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."[7] The ORM principles of the US Army suggest the following actions:[8]

- Accept risk when benefits outweigh the costs.
- Accept no unnecessary risk.
- Anticipate and manage risk by planning.
- Make risk decisions at the right level.

*COBIT® 5 for Risk* defines information technology (IT) risk as business risk—specifically, business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.[9] To clarify and define IT risk requires discussion of information security risk and cybersecurity risk. Generally, information security is the protection of information by maintaining the confidentiality, integrity and availability of the assets in which that information lives. Other aspects of information security relate to nonrepudiation, privacy or sensitivity. Cybersecurity is related to IT, because technology is often the vector through which a cyberrisk is realized. Enterprises often distinguish information security from cybersecurity as distinct types of risk and spend a lot of time and resources identifying and justifying actions to prevent or avoid them. To understand these categories of risk, it is important to realize that any risk has the potential to become realized, if it is not identified, analyzed and managed well. IT, cybersecurity and information security risk does not have one source or category; rather, it reflects a combination of interrelated risk, which includes specific and unique characteristics, such as specialized types of technology, threat actors, user errors, attack vectors, control failures or software vulnerabilities.

Although cybersecurity and information security risk are hot topics currently—as many events in recent headlines

5 Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrating with Strategy and Performance*, USA, 2017, *https://www.coso.org/Pages/ERM-Framework-Purchase.aspx*

6 Institute of Internal Auditors (IIA), *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control*, January 2013, *https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf*

7 Basel Committee on Banking and Supervision, "Sound Practices for the Management and Supervision of Operational Risk," February 2003, *www.bis.org/publ/bcbs96.pdf*

8 Geren, Pete; George W. Casey, Jr.; *Statement on the Posture of the United States Army 2009*, "Information Papers – Risk Management," *www.army.mil/aps/09/information_papers/risk_management.html*

9 *Op cit* ISACA

suggest—risk often relates to other factors, such as the actions of people. For the purposes of this white paper, the risk management process steps of identification and analysis are generally performed in the same manner, regardless of the source or category of risk. (For example, practices to identify specific components of cybersecurity risk differ from those designed to identify other types of risk; but the initial, generic risk management steps of identification and analysis follow the same process regardless, for all risk types.) Conversely, risk response and treatment may need to be individualized for a specific type of risk, because some risk, such as cybersecurity, can materialize very quickly.

These definitions provide the context in which enterprises apply four common risk dispositions—accept, avoid, mitigate or transfer—to achieve objectives and mitigate risk with the greatest potential impact on objectives (should the risk materialize). Enterprises must manage common and unique risk, depending on their industry, competitors, geography and markets. Whether an enterprise uses the terms ERM, ORM, IT risk management, information security or cyberrisk management, practices should align and integrate in such a way that risk can be viewed horizontally and vertically, while being managed at the appropriate level in the enterprise to ensure that its strategy and mission are achieved (see **figure 2**).

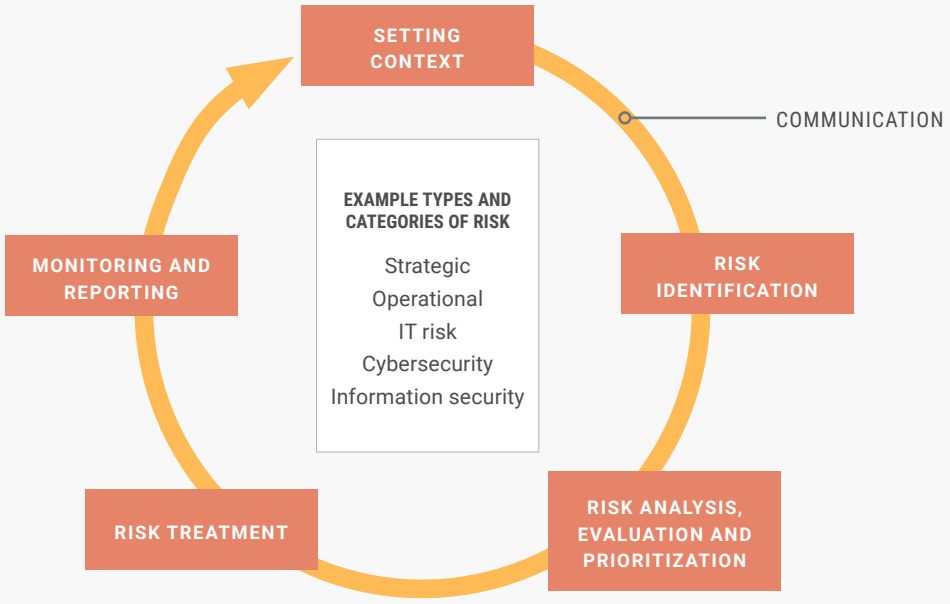


**FIGURE 2:** Risk Types and Categories in the Risk Management Process

# Implementing a Risk Management Process

Commitment from the highest level of enterprise leadership (including the C-suite, board of directors, senior leadership council, etc.) is necessary to ensure a successful implementation of risk management. Because risk management activities span different parts of the enterprise, some harmonization or integration of different risk management activities may be needed before proceeding. This section describes a step-by-step approach for implementing a risk management process. The steps and materials presented here reflect illustrative examples and are not meant to be prescriptive or complete. Leaders should carefully determine the elements that are required and best fit the unique culture and operating rhythm of their enterprise.

Risk management should answer six questions:

1. What are we in business to do? [Mission, strategy and objectives]
2. To what risk are we exposed? What has changed in our environment, objectives or mission? [Risk identification]
3. What risk is most important? [Analysis, evaluation and prioritization]
4. What are we going to do about the high priority risk and others that require action? [Risk response and treatment]
5. Did our risk actions produce the desired outcomes? [Monitor, review and report]
6. Is the risk management process embedded in the business and operating as intended? [Periodic review]

**Figure 3** shows an example of a risk management process.

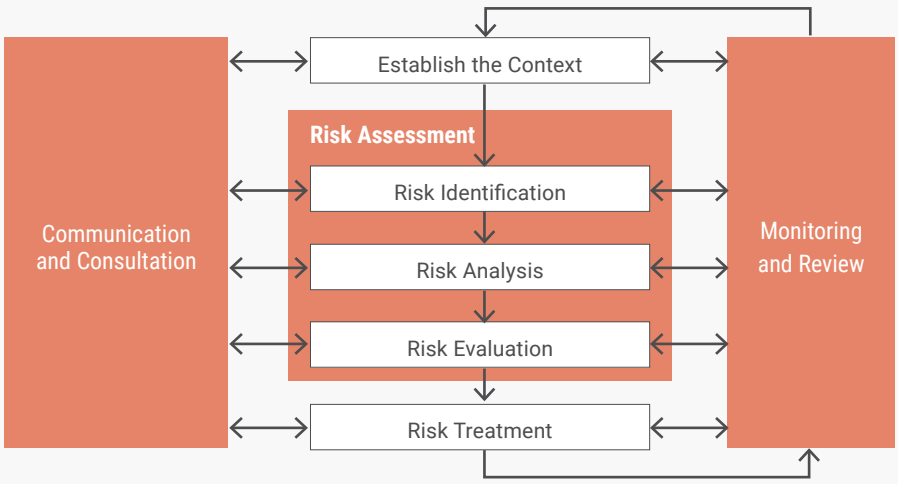


**FIGURE 3:** International Organization for Standardization (ISO) 31000 Risk Management Process

Source: ©ISO. This material is reproduced from ISO 31000:2009[10] with permission of the American National Standards Institute (ANSI) on behalf of ISO. All rights reserved.

10 International Organization for Standardization (ISO), "Risk management – Principles and guidelines," ISO 31000:2009, November 2009, *https://www.iso.org/standard/43170.html*

A discussion of currently practiced risk management is not complete unless inherent risk, current risk and residual risk are addressed. Inherent risk, also called gross risk or natural risk, reflects risk present in a process or activity without any controls in place. Residual risk reflects risk that remains after the risk treatment or risk response has been applied. Current risk is the actual risk today, given current risk responses inherited or applied. Unless the technology, system or process is in the very early design phase, it is unlikely that there are no controls in place in enterprises with a sustained focus on compliance with standards, regulations or the adoption of control catalogs.

COBIT 5 uses the term risk to mean current risk (see **figure 4**) and that view is reflected in this white paper. Implementing a set of prescribed controls or compliance regulations will generally protect an enterprise from most risk in the environment and can be put into effect without the benefit of a comprehensive risk assessment or embedded risk management process. It is easier to report on gaps in controls, security incidents or phishing attempts as risk events because they have already happened and can be measured. Reporting on the uncertainty of what might or might not happen is a discipline that takes an investment of education, time and resources to report to management in a way that improves decision making and does not rely solely on reporting the difference between the inherent and residual risk.

As a discipline, the audit and assurance roles are focused on the inspection, verification or conformance to a set of practices or controls to ensure that guidance is being followed, records are accurate and effectiveness targets are being met. Moving from a controls-based approach to a risk-based approach takes a forward-looking view of uncertainty. A risk-based approach is best paired with a strategic view of the enterprise to understand which potential uncertainties, or risk, have the highest potential to prevent the enterprise from meeting its intended targets, objectives and mission. In the absence of a mature risk management program and process, the enterprise can be generally effective in preventing realized risk with a robust compliance or controls program. However, to ensure that the enterprise is managing the risk that has the most relevance to the enterprise, thoughtful risk identification, risk analysis, risk management and risk monitoring processes must be defined, implemented and measured for effectiveness.


**FIGURE 4:** Interrelationship of Inherent, Current and Residual Risk

Source: ISACA, *COBIT® 5 for Risk*, USA, 2013, pg. 18, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

## Mission, Strategy and Objectives: Setting the Context

The enterprise mission, strategy and objectives are the basis for understanding the risk landscape in which the enterprise operates. Whether an enterprise is public or private, for profit or nonprofit, government or military, it has a mission to deliver value to stakeholders and customers. In most enterprises, information about the mission, business and objectives is usually documented and readily available. For large enterprises, the information may exist for each organizational unit, line of business or division. Understanding risk to the enterprise in the context of the mission, strategy and objectives is the first step in making sure that activities add value to the overall risk management process. This is known as setting the context for risk management. The foundational concepts of setting the context require the enterprise to maintain clear traceability between the mission and assets through which the mission is achieved and services and products are delivered. To accomplish the mission, assets—such as people, information, technology, raw materials and service providers—are essential. Clearly tracing a path from the mission, products, and services that the enterprise delivers to the underlying assets that support delivery aids in fostering the ownership and personal responsibility needed to effectively manage risk.

Action items:

1. Determine if risk appetite is established. Establishing and maintaining risk appetite and risk tolerance statements support appropriate risk taking within the predetermined limits (tolerances).
2. Communicate the risk vision to all enterprise employees and explain each employee's individual responsibilities with respect to risk management.
3. Identify the high-value services and products that fulfill the enterprise mission, strategy and objectives. This provides some prioritization to the risk management activities by placing focus on the critical assets.
4. From the high-value services and products, understand (identify and document) the critical assets that are required to deliver the service or product. The critical assets include technology, information, people, suppliers, vendors, facilities or any other resource that is required for successful service or product delivery.

## Risk Identification

Risk management focuses on supporting the enterprise strategy and objectives. Risk identification seeks to improve confidence by understanding any risk that impedes the enterprise's ability to meet its objectives. The risk identification process usually starts with brainstorming potential threats (e.g., cyberthreats), or any other areas of concern. Often, what keeps people awake at night turn out to be factors that contribute to risk rather than the risk itself. For example, people worry about unpatched systems and often miscategorize them as risk. An enterprise ultimately cares about the loss-event scenarios that would have an impact on its ability to meet its mission. Initial identification can take many forms, including interviews, brainstorming activities, web self-reporting or surveys.

Risk scenario analysis can be an important component of risk identification. *Risk Scenarios: Using COBIT® 5 for Risk* provides additional guidance for enterprises that are new to scenario analysis.[11] A risk scenario describes a possible event that—if and when it occurs—has an uncertain impact on the achievement of enterprise objectives. Scenario analysis can assist in the identification of key risk exposures and potentially severe events (especially emerging risk) with a potential for enterprise impact. When risk scenario analysis is conducted in an open and transparent environment, it can provide insights about events that are probable, but not realized previously. When getting started with scenario analysis, scoping the discussion to one business line or one critical system can be helpful, so that the participants are not overwhelmed.

11 ISACA, *Risk Scenarios: Using COBIT® 5 for Risk*, USA, 2014, www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Risk-Scenarios-Using-COBIT-5-for-Risk.aspx?cid=pr_1104761&appeal=pr

Another technique that is helpful for risk identification is the definition and use of a risk taxonomy. A risk taxonomy provides a scheme for classifying sources and categories of risk. The path from a cyberthreat or area of concern to a risk requires that the statement of risk be decomposed into components that are actionable. A risk taxonomy provides a common language for discussing and communicating risk to stakeholders.

Action items:

1. Establish techniques for the identification of risk. Candidate techniques include:
   - Scenario analysis
   - Risk taxonomy
   - Risk and control self-assessments (RCSA)
   - Interviews
   - Brainstorming
   - Identifying realized risk that has occurred in similar enterprises
   - Strength, weakness, opportunity and threat (SWOT) analyses
   - Business impact analyses (BIA)
2. Vulnerabilities and threats should be considered as inputs to the risk identification process, but not as a shortcut for conducting a robust identification and analysis of risk. Identified vulnerabilities may be one area of concern but do not constitute risk until other factors, such as the value of related assets and the threat landscape, are considered as part of the analysis in the next step. One example of a technology vulnerability is a security exposure that results from a product weakness that its designer did not intend to introduce. Vulnerabilities from areas other than technology, such as those from the actions of people, should also be considered as part of the evaluation and analysis step.
3. Decompose the areas of concerns and threats into a statement of risk, making sure to capture the circumstances, conditions or situation that causes the concern, and an impact statement that describes the outcome of the realized risk. An example statement of risk is, "Disclosure of confidential customer information to unauthorized persons results in increased cost of incident cleanup, reputation damage and loss of 20 percent of customer revenue."
4. Review the risk statements in the current list of identified risk (which may be documented in a risk register). If the risk is not current or in the form of actionable risk statements, reformulate it in the statement-impact format. Make sure the risk register does not contain only findings from previous audits or a list of vulnerabilities; for example, control deficiencies or a list of the results from a vulnerability scan are not risk. Although these may be sources of risk, they are not a complete catalog of risk. There are likely other sources of risk that could prove detrimental to the achievement of objectives if they are not identified and managed.

## Analysis, Evaluation and Prioritization

Many different methods and techniques exist for assessing and analyzing risk; each begins with the identification of risk. After areas of concern (potential future or emerging risk) are identified, they are typically sent to a centralized group for further assessment and analysis. Larger enterprises often have a project or program management office (PMO). The PMO is a good central intake point that can look horizontally across projects and programs for a more comprehensive view of risk. The centralized group should have a standard evaluation process for deciding whether the identified area of concern needs more detailed analysis and the type of analysis (quantitative or qualitative) that is needed. If an enterprise is just getting started with risk management, a centralized function may not exist. In the beginning

stages of risk management, clearly defining roles and responsibilities for prioritization is more important than the structure used. This standard evaluation process can be a quick checklist or questionnaire that includes risk factors, such as:

- Type of information created or used in the business process, e.g., personally identifiable information (PII), intellectual property (IP) or export-controlled information
- Type of authentication required to access the information
- Number of data records stored or transmitted by the system

Risk analysis and assessment are core approaches to bring realism, insight, engagement and improved structure to the complex management of enterprise risk and, especially, IT risk. Risk analysis estimates the frequency and magnitude of a given risk scenario. Risk assessment identifies and evaluates risk, its potential impact on the enterprise and the likelihood (probability) that a particular event will occur. Risk assessment is slightly broader than risk analysis and includes the activities of ranking or prioritizing the identified risk according to defined enterprise risk thresholds, grouping like risk types together for mitigation and documenting existing controls.

Action items:

1. Develop a set of enterprise criteria to rate and rank risk. Criteria can be qualitative and quantitative depending on the maturity of the risk program, available tools and resources, and the use of risk appetite or risk tolerance statements, if they exist.
2. A common industry practice for enterprises just getting started with risk management is to rank and rate the top five-to-10 risk scenarios across ERM, ORM, IT or cybersecurity on an impact-and-likelihood matrix, which is also known as a heat map or a stoplight chart. As an enterprise evolves its analysis capabilities, this kind of visualization may still be used, but should be substantiated by quantitative analytics, which support the decisions used to rate risk in alignment with risk appetites and risk thresholds.
3. Risk is usually assigned a disposition of accept, avoid, mitigate or transfer, with candidate actions for each disposition. For risk that exceeds the stated thresholds or is deemed unacceptable, a risk response or treatment is the next step.

## Risk Response and Treatment

When risk is deemed unacceptable or out of tolerance based on the enterprise risk appetite, activities for risk response are selected. Generally, the main responses or treatments are: accept, avoid, mitigate and transfer.

- **Acceptance** is just that; the identified risk is within tolerance of the risk appetite and no further action is necessary. Although not generally a best practice, there may be some cases in which risk is accepted even if it is out of tolerance. This is more often the case when an enterprise does not have a set of risk tolerances that are embedded in the risk management process. Some items may not rise to the level of risk today but merit close monitoring for certain conditions that can elevate them to risk; for such items, one alternative is to create a watch list.
- **Avoidance** involves taking steps to remove a hazard or exposure, or to engage in an alternate activity that lowers the probability of risk occurrence.
- **Mitigation** is probably the most common response to identified risk, and many people in the risk industry are familiar with the different types of controls that are available as mitigating actions to bring the identified risk within tolerance and appetite.

- **Transfer** is often underutilized and misunderstood as a risk response, especially for cybersecurity risk. Risk transfer involves shifting risk from one party to another through a contract. It is most often accomplished using an insurance policy, but a noninsurance agreement may also be used for risk transfer. Responsibility for the risk cannot be transferred, but options like insurance, a liability waiver with a client or an indemnification agreement with a supplier can help manage any impact from realized risk.

Action items:

1. Assign dispositions to all risk. Dispositions may simply be recorded in a spreadsheet alongside a list of risk conditions or in a more formal risk register in a software application or tool. All risk should be documented so it is not overlooked or forgotten as environmental, business and risk conditions change.
2. Periodically revisit areas of concern, watch items and identified risk as conditions change. If the enterprise has a threat intelligence or other function that monitors the external environment for emerging risk, the information from that function can be used here.
3. For risk that is to be mitigated, designate a person with the responsibility to develop and implement (or delegate) the necessary activities to take action on the risk. Usually, this person is known as the risk owner and has access to knowledge, skills, resources and abilities to commit to a course of action that mitigates the identified risk. In practice, this may look like a responsible, accountable, consulted, informed (RACI) chart (see **figure 5**).
4. Activities implemented to address the risk are generally reflected in a plan. This plan may be called a risk mitigation plan, a risk project, a plan of action and milestones, or some other specific enterprise name that is meaningful.
5. Risk that may be too costly to mitigate with controls might benefit from a contingency or other plan that seeks to minimize or reduce impact if the risk is realized.

## Monitor and Report on Risk Under Management

Reporting on risk activities ensures a continuous feedback loop to management, senior leaders, risk committees and boards of directors or other executive bodies. As the risk management activities progress, analysis should be performed to understand the root causes of any realized risk with the intent of deriving key risk indicators. Key risk indicators provide a leading metric that can be tracked over time to better understand the conditions that contribute to realized risk.

Effective risk management requires periodic monitoring until the risk treatment plan is completed. Periodically reevaluate conditions that might elevate any watch item or vulnerability to a full-fledged risk.

Action items:

1. Monitor the status of identified risk, risk treatment plans and measures of the risk management process. In some enterprises, the project management function can be leveraged to embed the risk management processes into daily business routines.
2. Periodically revisit areas of concern, watch items and identified risk as conditions change. Update the risk register as needed.
3. Report the progress of risk management activities to all relevant stakeholders. Candidate stakeholders are:
   - Process and system owners
   - Audit and risk committees
   - Governance boards
   - External regulators (if an enterprise is subject to such regulation)

| Key Management Practice | Board | Chief executive officer | Chief financial officer | Chief operating officer | Business executives | Business process owners | Strategy executive committee | Steering committee (programs/projects) | Project management office | Value management office | Chief risk officer | Chief information security officer | Architecture board | Enterprise risk committee | Head human resources | Compliance | Audit | Chief information officer | Head architect | Head development | Head IT operations | Head IT administration | Service manager | Information security manager | Business continuity manager | Privacy officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| APO12.01 Collect data. | | I | | | | R | | | R | | R | R | | I | | C | C | A | R | R | R | R | R | R | R | R |
| APO12.02 Analyze risk. | | I | | | | R | | | C | | R | C | | I | | R | R | A | C | C | C | C | C | C | C | C |
| APO12.03 Maintain a risk profile. | | I | | | | R | | | C | | A | C | | I | | R | R | R | C | C | C | C | C | C | C | C |
| APO12.04 Articulate risk. | | I | | | | R | | | C | | R | C | | I | | C | C | A | C | C | C | C | C | C | C | C |
| APO12.05 Define a risk management action portfolio. | | I | | | | R | | | C | | A | C | | I | | C | C | R | C | C | C | C | C | C | C | C |
| APO12.06 Respond to risk. | | I | | | | R | | | R | | R | R | | I | | C | C | A | R | R | R | R | R | R | R | R |

**FIGURE 5:** Example APO12 RACI Chart

Source: ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, pg. 108, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*

## Periodic Review and Improvement of the Risk Management Process

Risk managers should periodically review the steps of the risk management process in sufficient detail to identify improvements and efficiencies to make risk management part of the normal business rhythm and not an addon or optional activity that provides little business value. In enterprises with a more mature risk management capability, risk activities are structured within processes that are defined, planned and measured. Review may include definition and reporting of process metrics to help determine if risk management is operating as intended.

Action items:

1. Periodically revisit the mechanisms for each of the risk process steps to understand if the step is efficient and effective. For example, if an enterprise is using a risk and control self-assessment (RCSA) as a technique for risk identification, is it updated periodically as conditions change or emerging risk is discovered?
2. Is there a project or program management office that can be leveraged to make risk management a normal part of enterprise operations? Tracking progress of risk treatment activities against plans is a good way to get started with metrics.
3. Evaluate risk activities to ensure that the most important assets and services are in scope. Some enterprises start with high-value assets and then expand the scope as capability matures.
4. Integrate the planning of risk management activities with audit and compliance planning activities. Often, there is economy in collecting data once and using it to satisfy multiple information needs.
5. If the risk management activities rely on quantitative models, the models should be subject to the risk management process to ensure that they continue to perform as intended.

# Summary

The main drivers for risk management include the needs to improve decision making in enterprises, align risk management resources to address the risk with the greatest potential impact on the enterprise and ensure that value is created by maintaining risk within acceptable tolerances and appetites. Any enterprises can follow the guidance in this white paper to structure risk management activities into a process that fits its unique operational landscape.

# Acknowledgments

ISACA would like to recognize:

## Lead Developer

**Lisa Young**
CISA, CISM, CISSP, USA

## Expert Reviewers

**Ewan Johnston**
CISA, UK

**Jack Jones**
CISA, CRISC, CISM, CISSP, USA

**Michelle Valdez**
CISSP, USA

**Brandon L. Young**
CISA, GCIH, USA

## ISACA Board of Directors

**Theresa Grafenstine, Chair**
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte-Arlington, VA, USA

**Robert Clyde, Vice-Chair**
CISM
Clyde Consulting LLC, USA

**Brennan Baybeck**
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA, Director

**Zubin Chagpar**
CISA, CISM, PMP
Amazon Web Services, UK, Director

**Peter Christiaans**
CISA, CRISC, CISM, PMP
Deloitte Consulting LLP, USA, Director

**Hironori Goto**
CISA, CRISC, CISM, CGEIT, ABCP
Five-I, LLC, Japan, Director

**Mike Hughes**
CISA, CRISC, CGEIT
Haines Watts, UK, Director

**Leonard Ong**
CISA, CRISC, CISM, CGEIT, CPP, CFE, PMP, CIPM, CIPT, CISSP, ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA
Merck & Co., Inc., Singapore, Director

**R.V. Raghu**
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India, Director

**Jo Stewart-Rattray**
CISA, CRISC, CISM, CGEIT, FACS CP
BRM Holdich, Australia, Director

**Ted Wolff**
CISA
Vanguard, Inc., USA, Director

**Tichaona Zororo**
CISA, CRISC, CISM, CGEIT, COBIT 5 Certified Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa, Director

**Chris K. Dimitriadis, Ph.D.**
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
Intralot, S.A., Greece

**Robert E Stroud**
ISACA Board Chair, 2014-2015
CRISC, CGEIT
XebiaLabs, Inc., USA

**Tony Hayes**
ISACA Board Chair, 2013-2014
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA
Queensland Government, Australia

**Matt Loeb**
CGEIT, FASAE, CAE
ISACA, USA, Director

# About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its half-million engaged professionals in information and cyber security, 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 215 chapters and offices in both the United States and China.

## Disclaimer

ISACA has designed and created *Getting Started With Risk Management* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

### RESERVATION OF RIGHTS



ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

**Phone:** +1.847.660.5505

**Fax:** +1.847.253.1755

**Support:** support.isaca.org

**Web:** www.isaca.org

**Provide feedback:**
www.isaca.org/Getting-Started-With-Risk

**Participate in the ISACA Knowledge Center:**
www.isaca.org/knowledge-center

**Twitter:**
www.twitter.com/ISACANews

**LinkedIn:**
www.linkd.in/ISACAOfficial

**Facebook:**
www.facebook.com/ISACAHQ

**Instagram:**
www.instagram.com/isacanews/