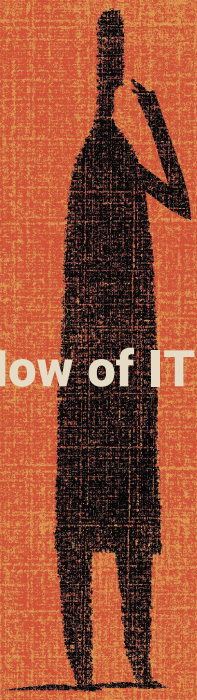
The Why and How of IT Risk Management



BY STEVEN L. SCHAFER

Risk is the effect of uncertainty on objectives. Risk management is a discipline for systematically calling out those things that can go wrong (or unexpectedly right) and then deciding what, if anything, to do with that information.

All organizations engage in risk management to some degree. Buying insurance, doing a background check on a potential employee, and conducting a security assessment are all examples of risk-management activities. The question is whether to formalize the risk-management function. The potential benefits from the extra effort to elevate risk management within an organization include: improving overall management, financial performance, regulatory compliance, governance, and internal controls; enhancing the reputation of the organization; and reducing losses.[1]

While developing and implementing a risk-management program may not be part of the official job description for the position of finance officer, he or she should promote a structured approach to managing risk. Risks usually have a financial component, which makes them directly relevant and important to the responsibilities of the IT financial manager.

Risk management is a discipline for systematically calling out those things that can go wrong (or unexpectedly right) and then deciding what, if anything, to do with that information.

INITIAL STEPS

Some preliminary work will set the stage for an effective IT risk-management program. This includes gathering strategic plans and objectives, inventorying existing risk-management activities, and understanding the organization's risk appetite. It's important to document this information to inform future efforts.

Step 1: Choose a Risk Management Framework. Like the columns and beams that hold a building together, a risk management framework offers the conceptual infrastructure for creating and carrying out risk-management activities. Using an established framework provides easy access to information, publications, and a community of experts regarding processes. An established framework also increases the legitimacy of the risk management initiative within an organization. Three frameworks that merit consideration are: "COBIT 5 for Risk," COSO's "Enterprise Risk Management," and ISO 31000 "Risk Management Principles and Guidelines."

As a practical matter, be prepared to borrow from all three, following the advice to adapt, not adopt. Integrating a framework with existing practices is essential; so is an iterative approach that builds on past efforts in manageable, incremental steps.

Step 2: Gather Strategic Plans and Objectives. An organization's strategic plan and the objectives it strives to achieve provide the context for its risk-management program. A solid understanding of strategic direction is essential to effective risk management. If a formal strategy does not exist, other documents might reflect goals and objectives. Places to look include annual reports, lists of major initiatives, budget documents, and even performance goals for employees. Statutes and ordinances for public agencies typically include a statement of purpose with a list of goals.

Step 3: Inventory Existing Risk-Management Activities. Taking stock of existing risk-management efforts within an organization avoids duplication and builds on existing support for risk management. This should include both the IT department and the whole enterprise. Places to look in the broader enterprise include the finance department, which understands and promotes internal controls to prevent fraud and accounting errors; the legal department, which is sensitive to potential legal issues; and the group that oversees the insurance program.

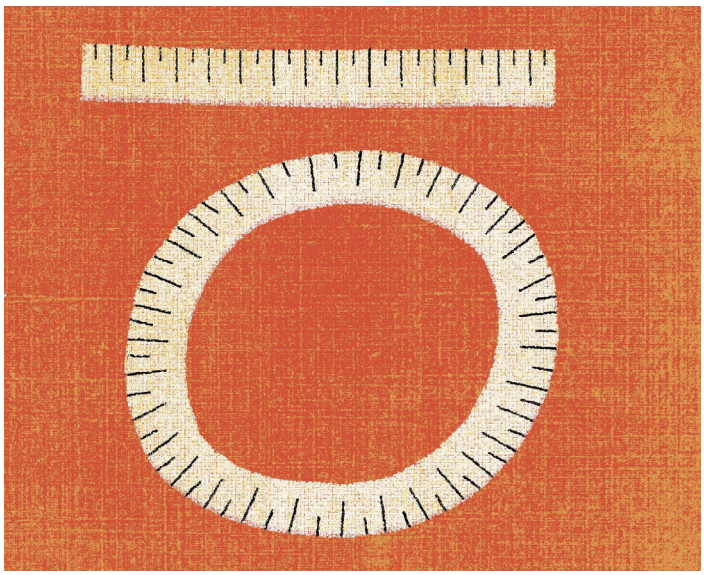
Most IT groups follow practices that fall into the general category of risk management. Back-up routines, redundant systems, disaster recovery, and business continuity planning all address the risk of being dependent on technology and the opportunity of using technology to mitigate the impact of a disaster on business operations. Change-management routines protect against unplanned downtime stemming from modifications introduced in the technical environment by multiple entities within the organization. Personnel practices such as background checks, non-compete clauses,

and confidentiality statements shore up some of an organization's vulnerabilities stemming from the people it employs. Project management uses project charters to protect against scope creep and careful tracking of progress to flag potential problems early. Security officers are now common in IT organizations to focus more attention on cybersecurity. Testing saves time and resources by revealing problems when they are easier to fix and before they disrupt operations. Training helps maximize value by giving people the knowledge they need to make effective use of systems and procedures.

Step 4: Understanding and Communicating Risk Appetite. Risk appetite is "the amount of risk an entity is prepared to accept when trying to achieve its objectives."[2] Risk appetite reflects the enterprise's capacity to absorb loss (e.g., financial loss or reputational damage) and management's predisposition towards risk taking (which ranges from cautious to aggressive). Articulating and communicating risk appetite helps everyone in the organization know what types of consequences are acceptable.

An organization can ask itself questions in the following areas:[3]

- *Corporate values* — What risks will the organization not accept?
- *Strategy* — What risks does the organization need to take?
- *Stakeholders* — What risks are stakeholders willing to bear, and to what level?
- C*apacity* — What potential consequences can the entity afford, within its resources?



Below are examples of risk appetite statements for a public agency:

- *Reputation and public trust* — Reputation and public trust are all-important. The agency will avoid any situation that could compromise its reputation or violate public trust.
- *Regulatory compliance* — This incorporates a broad range of edicts, including state statutes, federal grant requirements, auditing standards, budget limits, personnel rules, and procurement rules. Non-compliance can have serious consequences and undercut public trust. For these reasons, the agency will always strive to follow regulatory requirements. Violations — whether inadvertent or through conflicts with other mandates — will be documented openly.
- *Financial loss* — The agency will manage its finances carefully. Services must be self-sustaining. A temporary loss in any particular area may be acceptable as part of a clear strategy to develop a new shared service. Chronic loses must be dealt with promptly.
- *Goals* — The agency will aggressively pursue opportunities to achieve its vision and mission and the governor's directives.

CREATE AN IT RISK-MANAGEMENT CHARTER

A project charter assigns authority, articulates responsibilities, and defines scope, among other things. In risk-management terms, the project charter reduces uncertainty about authority, responsibility, and scope.

The exact content of the project charter should reflect the needs of the organization and the situation. An outline might include the following sections:

- Introduction
- Purpose, objectives and scope (delineation of what is in scope and out of scope)
- Governance (authority, communication, and changes to the charter)
- Approach, timeline, and deliverables
- Organization and staffing (organizational structure, roles and responsibilities)
- Budget
- Assumptions

The section on approach should designate the risk-management framework that will be used. Deliverables might include an inventory of existing IT risk-management activities, a report on the IT organization's risk appetite and culture, methodology for identifying and evaluating risks, the initial risk assessment, and the initial risk plan.

Developing the project charter and then obtaining its endorsement can help win support for the risk-management effort. Discussion leading to adoption of the project charter may provide information and perspectives that will be helpful. In addition, giving the organization's leadership an opportunity to set the direction gives them control, which increases trust and cooperation.

> While developing and implementing a risk-management program may not be part of the finance officer's official job description, he or she should promote a structured approach to managing risk.

Tailoring the content of the project charter to the needs of the organization is an opportunity to demonstrate that the organization is risk aware. What are the sources of uncertainty (positive or negative) surrounding the risk management effort? Answers to this question become potential topics to address in the project charter. Although the project charter should not become the first iteration of the risk assessment or risk action plan, it could identify specific risk topics that require investigation.

IDENTIFY RISKS

Risk assessment is the heart of risk-management. According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO): "The focus here is to gain an understanding of — and agreement on — the organization's top risks and how they are managed. The starting point is to get a manageable list of what are collectively seen as the most significant risks."[4] Equally important is avoiding too much detail or too many risks early on that can impede progress on the boarder risk-management endeavor.

COSO suggests using a combination of techniques in identifying risk. These can include looking at past events, facilitated workshops, interviews, process flow analysis, expansion of routine business planning activities, and lists of risks published by other sources. Methods for risk identification can be tailored to different parts of the organization, but COSO advocates casting a wide net to understand the universe of risks that could impact the organization.[5]

One approach is to broach questions about risk during routine budget and rate-review sessions with managers of technical teams. The agenda for these sessions might include the following topics:

- Identifying the services that support mission-critical functions. What is the current status of efforts to protect against disruption? What scenarios represent the greatest threat to operations of mission-critical systems?
- Focusing on threats to availability. How long would it take to restore service in the event of either hardware failure or loss of the building?
- Identifying opportunities to expand services or customer base.
- Determining which investments should be included in the budget to address risks or pursue opportunities.

Past experience (from within an organization and from outside entities) provides valuable insights for identifying potential IT risks. Following are common categories of "war stories" to look for.

System Infrastructure. This includes the hardware and networks that deliver data and applications. Common weaknesses include hardware failure, compatibility issues, and problems with telecommunications providers for Internet access and data circuits. The problems are not always technical in nature. For example, telecommunications providers often have problems with billing and accurately applying payments to the correct account, and some have policies of automatically disconnecting service for non-payment, which can lead to sudden loss of service. Risk assessments should identify and prevent these types of problems.

Providers. An organization's "partnership" with providers can easily become one-sided. Risks to the customer include changes in the provider's ownership, responsiveness,

and quality of service. Depending too much on a single provider adds to the level of risk, but multiple providers can complicate the situation by playing the pass-the-blame game when things go wrong. Changes in licensing terms and conditions followed by software audits can become very expensive lessons in who to trust.

> An organization's strategic plan and the objectives it strives to achieve provide the context for its risk-management program.

Project Staffing. So much depends on the quality of staff assigned to a project. Good project management helps, but also be alert to poorly performing teams, where a lack of skills is the source of risk.

People. Don't overlook the importance of people in keeping all the automation running smoothly. Are certain systems or applications dependent on one employee? If that person is unavailable, can other people step in? Are procedures well documented? Employees can also cause security risks and accidental — or intentional — disclosure of sensitive information. Some years ago, a city's systems administrator shut down access to all of the city's servers as retribution for a perceived wrong, and no one else knew the passwords to the servers to undo the damage.

Processes. Procurement is a major source of fraud (second only to financial fraud), and IT is a major purchaser of hardware, software, and services. Failure to follow sound procurement practices can jeopardize the budget, quality, and reputation of the IT organization.

Buildings. The physical locations where people work or where servers live are often the easiest place to start a risk assessment because they are tangible and a traditional subject. Fire, flood, storms, and electrical outages are relatively easy to visualize and safe to discuss. But even here, risk assessments can become complex, especially for data centers. Keep looking for single points of failure, including subsystems that few people may understand. The risk assessment should systematically identify anything that would lead to a loss of power, loss of cooling, or other disruptions in service. Here are some examples:

- Springtime release of seed pods from cottonwood trees clogged rooftop filters on the chiller system at a data center and almost shut the system down.
- City water project almost caused a shutdown of a data center because circulation of chilled water within the building depended on external water pressure. Internal pumps lacked size for effective circulation of non-pressurized water.
- The backup generator is tested weekly, but never under full load.

Changes. New technologies, new applications, software upgrades, new security threats, staff turnover, and other changes are themselves sources of risk. Any change should raise red flags that prompt questions about risk, and structured change management processes must be part of the overall efforts to address risk.

Near Misses. Near misses deserve special attention. These are past events that brought no serious consequences even though the outcomes could have been major or even catastrophic. Don't allow near misses to create complacency. Instead, treat them as actual failures and learn from them. People tend to become numb to risk after experiencing several rolls of the dice when nothing bad happens. Overconfidence also explains the willingness of workers to follow flawed procedures — they have always done them that way with no problems.

ANALYZE AND EVALUATE IT RISKS

Once risks have been identified, the organization needs to convert raw data into something that it can act on. Sometimes, just raising awareness of particular risks is sufficient — no special analysis is necessary because a course of action is clear. For example, the advantage of redundancy for mission-critical systems is typically obvious without extensive analysis. In other cases, more information is needed to understand the consequences of a risk, estimate its probability, and identify factors that would either mitigate the consequences or lower the likelihood of an event. This additional detail becomes valuable when comparing costs versus benefits or assigning priorities to multiple risks.

> Articulating and communicating risk appetite helps everyone in the organization know what types of consequences are acceptable.

Governments might want to do a preliminary analysis that screens risks based on the following courses of action:[6]

1. Decide to treat risks without further assessment.
2. Set aside insignificant risks that would not justify treatment.
3. Proceed with more detailed assessment.

Sorting risks into these categories can follow several iterations as information is gathered on risks in the third group that needs more research. The sorting process can be simple or sophisticated, depending on the needs and capacity of each entity.

Quantitative Methods. Psychological research has shown that people are bad at assessing the likelihood of events. Without specific training in calibrating assessments, people tend to be overconfident in the accuracy of their guesses regarding probabilities.

Quantification is feasible and should be the default approach in any evaluation of risks. Author Douglas Hubbard makes several key points regarding quantification,[7] noting that someone, somewhere has tackled whatever measurement problem you may have. As for data, he notes that you're likely to have more than you think and can acquire it more economically than you expect, and that the data you need is likely both smaller and different than it initially appears.

Simple Classification System. The ultimate purpose of analyzing and evaluating the list of IT risks is to sort them into three broad categories:[8]

- Immediate action ("quick wins").
- Further research ("business case to be made").
- Deferral ("costly responses to lower risks").

Especially for initial risk-management efforts, agreement on a short list of major risks represents significant progress, without the need for elaborate prioritization methodologies. A next step would be adopting a set of assessment criteria and applying them to the list of risks as a way of securing additional insight for sorting risks into broad categories.

Most of the time and effort involved in the risk assessment process should be reserved for conducting detailed studies of those risks that require a business case or careful analysis to guide management decisions. Examples might include documenting the single points of failure in the data center, understanding the potential interaction between multiple risks, and calculating the likely financial impact of specific events in order to build the business case for treatment.

CREATE A RISK RESPONSE/ACTION PLAN

Risk treatment options — which are not necessarily mutually exclusive — include:[9]

- Avoiding the risk by deciding avoid or discontinue the activity.
- Taking or increasing the risk in order to pursue an opportunity.
- Removing the source of risk.
- Changing the likelihood of the risk occurring.
- Changing the consequences of the risk, should it occur.
- Sharing the risk with another party (including contracts and risk financing).
- Making an informed decision to retain the risk.

Of course, the risk treatment chosen can itself introduce risks. "A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an inte-

gral part of the risk treatment plan to give assurance that the measures remain effective."[10] Monitoring the risk landscape is also important; this can be done by preparing key risk indicators as early warning signals of critical areas.[11] Capacity monitoring of servers and storage is a well known and widely practiced example, and this type of monitoring could be applied to other risks.

The purpose of the action plan is to summarize the methods, findings, and recommendations of the risk-management effort. Documentation serves as a communication tool, and adoption of the action plan confirms buy-in from the leadership of the organization. In addition, a listing of significant risks by organizational unit, type of impact, or type of risk (e.g., strategic, financial, operational, or compliance) helps with focusing responsibility and attention on addressing risks.

The risk action plan should include an overview of any in-depth studies of specific risks. The action plan should include a reporting process for tracking the status of risks and monitoring progress, gaps in risk processes, and adequacy of risk responses. Reports should be simple and tailored to the needs and practices of the organization.

Cyber Insurance. One topic for the risk action plan is whether or not to buy cyber insurance. Cyber insurance covers certain damages or related costs stemming from a data breach and the loss of personal identifiable information. Insurance typically covers crisis management (which may include advice and assistance as well as expenses for investigating an incident and remediating networks), notification (which covers the cost of notifying all individuals potentially impacted by the loss of data), credit monitoring for individuals affected, and loss of funds through theft or fines and penalties.

Both the public sector and private entities face large potential losses from a data breach. For example, the Target Corporation data breach in December 2013 affected 40 million customers. This remains one of the largest thefts of credit card data, but it was not an isolated incident. A recent magazine article summarized 20 major breaches in 2014, including well-known names like Niemen Marcus, Home Depot, Jimmy Johns, and JP Morgan Chase.[12] A survey determined that the average financial impact to companies for one or more incidents was $9.4 million.[13]

In the public sector, a data breach at the South Carolina Department of Revenue is illustrative. In fall 2012, a cyberattack exposed 3.6 million social security numbers and 387,000 credit and debit card numbers. The state paid more than $12 million for credit monitoring, $5.6 million for stronger encryption, and $1.3 million to notify taxpayers.[14]

The decision to purchase or forego cyber insurance should include considerations about the potential magnitude of impact, vulnerability, and capacity to absorb loss and to respond. The cost of premiums is also a factor. According to one source, the typical premium is $15,000 to $20,000 for every $1 million in coverage.[15] The application process may also be a factor. Purchasing cyber insurance requires an "in-depth asset exploration and process control" that "itself acts as a risk management tool." For entities with decentralized IT environments and distributed management of applications and data, gathering the information required for underwriting may be prohibitive.

NEXT STEPS

Conducting ongoing communications and developing the next phase of the risk-management program are essential components of any risk-management framework. "Ongoing communication" means keeping the issue of risk management in front of top management.

The implementation of risk management is an evolutionary process that should follow an incremental approach of continuous improvement. Ideas for building momentum and strengthening an organization's risk culture and practices include:[16]

- A program of continuing enterprise risk-management education for executives.
- Policies and action plans to embed enterprise risk-management processes into the organization's functional units (e.g., procurement, IT, or supply chain units).

> Broach questions about risk during routine budget and rate-review sessions with managers of technical teams.

- Integration of risk-management processes into an organization's annual planning and budgeting processes.

These suggestions underscore the concept that communication must be baked into every aspect of risk-management, not just treated as one step in a sequence of several activities. Success is when communication regarding risk become multi-directional — top to bottom, bottom to top, and even sideways within the organization. Risk awareness should be an always-on condition, not just limited to activities of the formal risk-management program.

> Both the public sector and private entities face large potential losses from a data breach.

CONCLUSIONS

All organizations require some level of risk-management. Setting a successful course begins with gathering strategic plans and objectives, inventorying existing risk-management activities, and understanding the organization's risk appetite. Organizations then need to create an IT risk-management charter; identify, analyze, and evaluate risks; and create a risk response/action plan. Finally, it's necessary to keep the issue of risk-management in front of top management. While the finance officer might not be officially responsible for the organization's risk-management program, safeguarding government funds by managing risk is an important part of the job.

Notes

1. "Help: how to sell the concept of operational risk management in the organization," LinkedIn discussion, comment by Alex Dali, April 26, 2014.
2. The Risk IT Framework, RiskIT (based on COBIT), ISACA, 2009.
3. "Board oversight of risk: Defining risk appetite in plain English," PriceWaterhouseCoopers, May 2014.
4. Mark L. Frigo and Richard J. Anderson, Embracing Enterprise Risk Management: Practical Approaches for Getting Started, Committee of Sponsoring Organizations of the Treadway Commission, 2011.
5. "ERM Integrated Framework – Executive Summary," COSO, 2004.
6. Recommended by ISO 31010 — "Risk Assessment Techniques" — a companion document to ISO 31009 that focuses on the risk-assessment process.
7. Douglas Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* (Wiley, 2009).
8. See COBIT Risk IT, page 29, or ISO 31010, page 20.
9. International Standard ISO 31000, Risk Management — Principles and Guidelines, International Standards Organization, 2009.
10. Ibid.
11. COBIT Risk IT Framework.
12. Bill Hardekopf, "The Big Data Breaches of 2014," *Forbes*, January 13, 2015.
13. Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, Ponemon Institute, August 2013.
14. Adam Stone, "Cyberinsurance: Do You Need It?," GovTech.com, February 27, 2014.
15. Ibid.
16. Frigo and Anderson.

STEVEN L. SCHAFER was IT administrator for finance for the State of Nebraska. Since retiring in December 2014, he has conducted workshops on risk management and rate setting for the IT Financial Management Association. He is researching topics on government reform and is interested in ways that governments can make more effective use of data to improve operations and transparency.