Risk management is not a new activity for many organizations. This is true because risk, by definition, presents a threat to value and, therefore, it is in the best interest of an organization to manage it. The processes for lowering loss exposures to acceptable levels is something well understood across many industries and fields, most notably in financial risk management for banking and insurance companies.

Despite the recognition and maturity of risk management at an enterprise level, the principles and methodologies of IT-specific risk management are much newer and have led to the birth of new models for operational risk mappings. Until recently, the complexities of the decisions that were required to be made and implemented within the IT domain tended to insulate it from the same level of business alignment routinely expected from other business units and from the other elements of the risk management family.

However, due in part to increasing regulatory expectations and requirements that, in turn, have resulted from an ever-increasing dependence on IT and exposure to IT-specific risk for critical business functions, the discipline has taken on new importance and prominence within the management portfolio of many organizations’ governance, risk and compliance (GRC) and security functions.

The security aspect is included, since “risk management provides the rationale and justification for virtually all information security initiatives.”1 In essence, information security as a knowledge domain and specialization exists primarily to manage risks to information and IT resources. Risk is, in fact, the proximate cause of IT security. The recognition and convergence between traditional risk management methodologies and IT security-based risk are increasing due to the potential for financial efficiency gains that may be realized from better prioritized remediation efforts and from the potential for well-informed risk decision making.

STANDARDS AND FRAMEWORKS
ISACA and the IT Governance Institute (ITGI) are currently developing Risk IT, an IT enterprise risk management (ERM) framework that should significantly assist management as well as auditors in the work of control assessment and remediation identification.2 This new framework aims “to fill the gap between generic risk management frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO)’s Enterprise Risk Management—Integrated Framework (ERM) and Australia/New Zealand AS/NZ 4360, and detailed (mostly security-related) IT risk management frameworks.”3 Risk IT is being developed to address all levels of IT risk, from the strategic to operational levels.

The COSO ERM integrated framework provides the following commentary regarding risk management: “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.”4 This approach indicates that business value is maximized when a balance between growth and risk management is achieved. To be clear, this kind of risk management is not merely concerned with avoidance, it helps enable the organization to take additional risk because the frequency and severity impact have been analyzed and are well understood and, therefore, can be accepted—if the return is sufficient. This is one of the hidden values that can be derived from a healthy IT risk management environment.

The US National Institute of Standards and Technology (NIST) defines IT risk management as “the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT environment.”5 This definition helps to provide an explanation from the classic business definition to the IT operational frame of reference.

Whatever framework or processes are used, the important concept in risk management is a...
structured and organized identification, analysis, evaluation and deployment, followed by an effective remediation and monitoring program.

ENTERPRISE RISK MANAGEMENT
IT risk management is one component of broader ERM. ERM is an approach to managing key business risks and opportunities to maximize shareholder value. Within the scope of IT, risk management tends to focus on pure risk or what is often referred to as “hazard risk”—the kind of loss exposure that comes into existence as a result of the threat of accidental loss to technology assets.

The number and variety of risks that affect or are a direct result of IT activities are extensive and cover a wide range of risk sources. The risks can be organized into categories and together the full list helps to describe the risk profile of the organization.

Although no risk model can offer a complete picture, tables and classifications can help provide focus on key risks and facilitate completeness. Symantec, for example, categorizes IT risk elements into four groupings: security risk, availability risk, performance risk and compliance risk, as shown in figure 1.

However, it is possible to use the more generic confidentiality, integrity and availability classifications as well, since all IT risk can ultimately be distilled into those core constituents.

GOALS OF IT RISK MANAGEMENT
The primary intent of any risk management exercise is to, first, reduce the cost of risk related to an organization’s activities and, second, to reduce negative impacts related to the uncertainty of outcomes. Put another way by NIST, “minimizing negative impact on an organization and the need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems.” These two purposes have measurable return on investment and deliver value on many levels, including:
- Ensuring optimal allocation of resources within an organization
- At the highest level, making the organization a safer investment and thereby commanding a correspondingly higher shareholder value

Preloss Objectives
Prior to any losses, the goal of a risk management program is to ensure an economy of operations. That is to say, the cost of controls (and the risk program itself) should not exceed the total potential savings. This is achieved through the application of prudent and appropriate controls where cost and benefit are favorable or intersect. In addition, a preloss goal is to deliver “tolerable uncertainty,” which means providing assurance about the scope of what is possible and how each potential outcome may be treated. By understanding the full breadth of risk possibilities and depth of impact, suitable decisions to reduce or even add risk can be made.

The preloss goal of providing legality is also an important component of the risk program as it relates not only to “duty of care” tort liability, but also to administrative laws and regulations related to technology, including the US Sarbanes-Oxley Act, Japan’s J- SOX, Payment Card Industry (PCI) Data Security Standards (DSS), the US Health Insurance Portability and Accountability Act (HIPAA), and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) and Bill 198 (also known as the “Canadian Sarbanes-Oxley” Act).

Postloss Objectives
After a loss, the goal of risk management is to ensure survival, followed by, and closely related to, continuity of operations. This objective includes technical and business elements that combine to ensure

<table>
<thead>
<tr>
<th>Figure 1—Symantec’s Four Elements of IT Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal and External Malicious Threats</strong></td>
</tr>
<tr>
<td>• Keep bad things out.</td>
</tr>
<tr>
<td>• Keep important things in.</td>
</tr>
<tr>
<td><strong>IT Policy and External Regulations</strong></td>
</tr>
<tr>
<td>• Ensure adequate controls.</td>
</tr>
<tr>
<td>• Automate evidence collection.</td>
</tr>
<tr>
<td><strong>Natural Disasters and System Failures</strong></td>
</tr>
<tr>
<td>• Keep systems up.</td>
</tr>
<tr>
<td>• Ensure rapid recovery.</td>
</tr>
<tr>
<td><strong>Application Performance and IT Performance</strong></td>
</tr>
<tr>
<td>• Optimize resources.</td>
</tr>
<tr>
<td>• Ensure correct configuration.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
</tr>
<tr>
<td><strong>Performance</strong></td>
</tr>
</tbody>
</table>
that critical functions can continue to operate under a variety of loss scenarios.

The risk management program provides a method for planning, organizing, leading and allocating resources to mitigate the effects of accidental loss. In brief, risk management is part of the due diligence owed by a public company or agency to its shareholders. So, at an organizational level, risk management is a governance dimension, and, therefore, support for risk management principles and processes is a clear demonstration of management’s care, as illustrated in figure 2.

Setting an effective strategic “tone at the top” helps ensure that risk management is “baked into” the organization and considered a part of every manager’s job—not an afterthought with output distributed in silos across myriad business units. The trickle down to IT operational management is a duty to help ensure that the types of controls, the cost of controls and the implementation of them are all appropriate for the resources or information that is being managed.

**TYPES OF ENTERPRISE IT RISK**

Financial risk management professionals like to group loss exposures into four kinds: property, liability, personnel and net income loss. For IT professionals, the spotlight tends to shine most brightly on the first kind of exposure, property—an exposure that establishes the possibility that an organization will sustain loss as a result of destruction, theft or loss of use. Translated into technology terms of reference, this would be the threat to confidentiality, integrity and/or availability within the application, information infrastructure and people resource pools.

Liability exposure is the potential loss resulting from a claim that an organization’s failure to the duty of care owed resulted in property damage or bodily injury to another party. In an increasingly regulated environment, the demands of due diligence have elevated the need for effective and demonstrable risk management processes, including those involving IT.

The threat of personnel loss is the risk to an organization that results from the death, disability, retirement or resignation of an individual that deprives the organization of specialized skill or knowledge that cannot easily be replaced. This risk can be a factor for IT because of the number of permutations and combinations of complex technology in each organization, and a resulting need for specialized skill sets to support specific infrastructure and applications.

**RISK ASSESSMENT**

The primary tools of an IT risk manager are risk assessment and analysis. This is because it is only through a thorough assessment process that a complete picture of IT risk can be drawn. Once this is complete, it can then provide the organization with the necessary information to make appropriate, properly prioritized and cost-effective risk management technique selections.

Of course, any successful risk assessment relies heavily on the completeness of the threat list. Compiling a complete list can be challenging and is commonly known as the problem of

---

**Figure 2—IT Governance Institute’s IT Governance Focus Areas**

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Source: ITGI, CoIT 4.1, 2007, figure 2
the “unknown unknowns.” Since we do not know about what we do not know yet, experience and analysis become valuable assets during this stage of risk management. In many cases, using expertise beyond the boundaries of the organization can provide additional benefits as a result of objectivity and potentially broader exposure experience.

RISK MATRIX
A risk matrix focuses on the dimensions of loss frequency and loss severity. Sometimes these are called likelihood and impact, respectively. The subjective, or qualitative, approach to this relationship is well understood in the risk management profession and is illustrated in the Prouty approach shown in figure 3.


While these dimensions help direct the kind of control that is appropriate, to assign priority, the existence of a threat source, an attack vector or a vulnerability must be considered. If any of these factors is nonexistent, the risk is effectively reduced to zero, no matter how severe the impact might be. This is intuitively obvious, since a threat does not exist if there is no vulnerability to be exploited and/or no attack vector or source from which it can originate. The multiplicative properties of this relationship lend themselves to calculating IT risk by multiplying the values together to derive the IT risk factor.

That value can be used to calculate a relative loss exposure, and, by multiplying the factor by asset value, it is possible to attach a monetary value to each risk. This equation is often quoted in IT reference sources. “With few exceptions, whether related to financial, physical or technological resources, different types of risk can be calculated using the same universal formula. Risk can be defined by the following calculation: Risk = asset value X threat X vulnerability.”10

These values can be prioritized against each other and used along with the exposure elements in the frequency and severity matrix to guide potential responses. This prioritization and response category is a valuable resource, as it allows the organization to make remediation investments in the most cost-effective way possible. It also may identify risks that the organization can safely assume without the need for remediation.

THE VALUE OF RISK MANAGEMENT CONTROLS
To drive value from risk management, it is critical that a management program extend past simply assessing and analyzing, but also follow through with implementation and remediation plans to lower the risk profile for the organization. “Risk and control are virtually inseparable—like two sides of a coin—meaning that risks first must be identified and assessed and then managed and mitigated.”11

There are a number of accepted risk control techniques that can be used, including concepts such as avoidance, prevention and reduction.

Prevention addresses the frequency of occurrence, whereas reduction addresses the severity of a particular loss. As well as control techniques, risk financing techniques that include insurance, transfer and retention can be utilized. Any risk that is not controlled, avoided or financed must be retained. Acceptable retention levels are subject to the risk appetite of the organization and should be formally derived and approved. Sometimes retention can be the most economic risk financing available. In all cases, it is the technique of last resort—the final option for loss exposures that simply cannot be insured or transferred. Risk that is retained is sometimes called “residual risk,” and when it is accepted, it is considered to have been “assumed.”

RISK MANAGEMENT PROGRAM
As with other management programs, such as quality’s plan-do-check-act (PDCA)/Deming cycle of continual improvement, it is expected that the risk management program be monitored and revised through a process feedback loop. IT risk must be routinely evaluated as a result of the changing threat, vulnerability and exposure landscape.
In this way, the program can adequately respond to new loss potential that could have evolved or been added since the last review. It also allows for the reevaluation of mitigation strategies to determine if new controls or countermeasures may have become more desirable than those previously implemented, thereby improving business efficiencies while still controlling risk exposure. This is an often overlooked business efficiency gain resulting from a cyclical, program-based approach to IT risk management.

CONCLUSION
No organization could ever eliminate all risk and remain viable. That is a simple fact of business life. By their very nature, some risks must be lived with, and this is perfectly acceptable, especially as the likelihood/frequency and impact of a risk become smaller and smaller. The value in risk management comes from having the knowledge about those occurrence factors and the resulting impact. With that knowledge, it is possible to prioritize and control risk efficiently and effectively. However, without such knowledge, only reaction and uncertainty would result.

IT risk management is one facet of ERM that is concerned with protecting an organization’s information assets and systems. Risk management in its broadest sense is a cornerstone of overall corporate governance, since it ultimately helps drive shareholder value by providing investors assurance about the risks to their money. Therefore, IT risk management should be considered a program, rather than a periodic project focused on IT security controls. As a program, IT risk management may consider, on a continuous basis, the full range of risk responses and can include the ability to take on additional risk for higher returns as a result of risk-aware decision making.

While driving value from nonrevenue-generating activities can be a challenge, in the case of IT risk management, the hidden values will be uncovered as a result of a well-implemented program.

REFERENCES

ENDNOTES
2 For more information on the Risk IT framework, please see www.isaca.org
4 COSO, Enterprise Risk Management—Integrated Framework, USA, September 2004
7 Op cit, NIST, p. 4
8 Baranoff, E.; S. Harrington; G. Niehaus; “Risk Assessment,” AICPCU/IIA, 2005
9 Davis, Chris; Mike Schiller; Kevin Wheeler; IT Auditing, Using Controls to Protect Information Assets, McGraw-Hill, 2007, p. 351
10 Ibid.