Building a Comprehensive IT Risk Management Program
White Paper: Enterprise Security

Building a Comprehensive IT Risk Management Program

Contents

Executive summary .................................................................4
Introduction .................................................................4
Defining effective IT risk management ..........................................5
IT risk areas .................................................................5
Program approach to IT risk management .........................................6
IT risk management program model ..........................................7
Culture .................................................................8
Governance .............................................................12
Control areas and policies ...................................................14
Program office ............................................................18
IT risk register ............................................................20
Project management .........................................................21
Conclusion .............................................................22
Executive summary
The need for effective IT risk management has become significantly more important as organizations have become more dependent on their IT systems for their livelihood and success. While many organizations feel they have a solid grasp on their IT risk concerns, too often their IT risk management efforts have serious gaps and vulnerabilities due to a failure to take a holistic approach to IT risk.

Effective IT risk management requires a comprehensive approach that addresses all four areas of IT risk: security, availability, performance, and compliance. It requires an IT risk management program that follows a proven model that takes into account an organization’s unique culture and attitudes toward risk. An effective model for building an IT risk management program should outline best practices for organizing program governance, defining control areas and policies, establishing a IT risk management program office, creating a comprehensive IT risk register, and executing successful project management that achieves the desired risk objectives of both business and IT. When organizations rely on such models to build their own IT risk management programs, they not only put themselves in a much stronger position to mitigate their risks, they also enjoy the added benefit of increased operational efficiencies, improved quality of service, and reduced IT infrastructure costs.

Introduction
Information technology plays a dominant role in most organizations’ day-to-day business operations. It has become widely and deeply interconnected with routine and mission-critical business activities alike. Some industry experts say that organizations’ heavy and growing reliance on IT has led to many companies having IT account for more than 50 percent of their total capital expenditures. In some industries, such as financial services and online retail, virtually the entire business may be transacted using IT systems and networks.

As enterprises increase their dependence on IT for effective business operations, they also need to increase their awareness of the risks inherent to their entire IT and business ecosystem. International headlines expose many of the risks that plague enterprise IT: increased and more concerted cybercrime threats, computer failures shutting down stock exchange trading, computer performance degradation impacting productivity and sales, and heavy fines imposed due to lack of regulatory compliance. While the business side of an enterprise might not care about the intricacies of the technology that drives its business, it needs to understand that unmanaged risks can have and do have a direct and significantly negative impact on business.
Fortunately, more and more businesses have begun to understand the need for effective IT risk management. IT risk management has become a top priority for many enterprises worldwide. No longer does IT risk solely have the interest of IT managers and directors; it now has the attention of senior-level executives and board members as well. They realize that the days have passed when they can just assume that technology will just do its job. Both the technology and business sides of the enterprise must work together to address the challenges associated with IT risk management.

Defining effective IT risk management

Even though IT risk management has become a top priority in many boardrooms around the world, in most cases there exists a serious disconnect between IT risk management execution and IT risk management effectiveness. This disconnect arises primarily from basic misperceptions as to what effective IT risk management entails and how to address this far-reaching and complex area of the business.

IT risk areas

Many organizations that take IT risk seriously still fall significantly short of effective IT risk management because they have a narrow view in regard to what constitutes IT risk. For example, some organizations invest tremendous effort and capital on securing their IT systems, assuming they have successfully addressed all of their IT risk factors. While securing IT infrastructure is an important part of IT risk management, it represents only one aspect of IT risk management. IT risk falls into four main categories that all need to be managed and mitigated:

• **Security**—Protect against unauthorized access, alteration, or use of information; data leakage; data privacy; fraud; identity theft; financial theft; and damage to reputation, brand, and assets. It includes combating broad external threats (i.e., viruses and malware) and targeted attacks to specific applications, specific users, specific information, and specific systems that a business relies on every day.

• **Availability**—Protect against customer abandonment and lost sales; reduced customer, partner, and employee confidence; and reduced employee productivity resulting from downtime of business-critical systems and processes. It means ensuring business continuity by keeping systems up and available. It includes the need to mitigate the risk of application failure, data loss, and data corruption. In cases of a disaster, it requires being able to rapidly recover business processes or data that have become inaccessible in the timeframe needed by the business.
• **Performance**—Accommodate volume and performance requirements for access to business-critical processes—even during peak times—to ensure the highest levels of user productivity, and client and customer loyalty, as well as prevent lost sales and reduced client satisfaction due to prolonged or unsatisfactory access times.

• **Compliance**—Avoid regulatory fines and penalties, breach of client confidentiality, litigation time and expense, executive productivity, and damage to business reputation by ensuring compliance with government and industry regulations, as well as industry-accepted best practices and policies for business operations.

Successful IT risk management requires businesses to take a step back from the narrow focused approaches common to most organizations, and then take a comprehensive look at all of the risks that exist in their environment and prioritize those risks according to the unique needs of their business. Failing to address IT risk management in a holistic manner can leave an organization seriously exposed and vulnerable to a wide array of threats to their business.

**Program approach to IT risk management**

Another risk management trap that many organizations fall into is taking a tactical or “risk de jour” approach to IT risk management. When a new strain of threats dominates the headlines, it not only raises executive awareness of a potential risk, but it also can have the effect that too much emphasis is placed on managing that specific risk. This can lead to spending priorities being inappropriately influenced by publicity, depleting or distracting from spending on other, sometimes latent, IT risks. Effective risk management requires an organization to first understand all of its overall risks, and then to align its overall spending in the appropriate areas.

This “risk de jour” approach is also very tactical in nature. Rather than having a well-thought-out risk mitigation strategy, organizations spin off individual projects to react to each newly discovered threat. The danger of this reactive stance is that when unforeseen disastrous events occur, organizations are not prepared to adequately deal with them, often resulting in more damage to the enterprise. Proactive approaches put enterprises in a better position to mitigate and protect themselves against these risks.

Another failing of a tactical or project management approach is that these projects often operate in isolation, not only from each other, but also from the different groups in the organization that should have a stake in their success. Often this creates a misalignment between the needs of the business and IT in terms of risk management. Also, projects are often managed at a local level or by a specific IT group with little or no enterprise oversight, leading to inefficiencies, threat gaps, and an unclear picture of the organization’s true risk landscape. Furthermore, by their very nature, projects have a beginning and an end, while IT risk management needs to be an ongoing effort.
Rather than taking a tactical approach, an organization needs to create a comprehensive IT risk management strategy that addresses the unique needs of its business and IT infrastructure. It must take an enterprise-wide approach that refines its people, processes, and systems in a manner that enables it to achieve the organization's preferred balance of IT costs and risks to improve the company's overall performance. At the heart of this approach, an organization needs to establish a holistic IT risk management program with the responsibility for the creation, implementation, and ongoing management of the enterprise's IT risk management strategy.

**IT risk management program model**

The establishment of an IT risk management program facilitates an organization's ability to understand the different types of risks that can affect its business, as well as prioritize those risks and effectively manage them in a holistic and comprehensive manner. Such a program provides the necessary vehicle to bring together the proper stakeholders from the different levels of the enterprise's IT and business operations to enable the proper alignment of IT and business needs in regard to IT risk management and the overall operational effectiveness of the IT organization.

As a growing number of organizations task their CIOs to create an IT risk management program, questions often arise: “What should the program look like?” “What and who does it involve?” “What does it do?” and “What should be its primary concerns?”

In answer to these questions, organizations need to examine the following six areas as they model or create their own IT risk management programs:

- Culture
- Governance
- Control areas and policies
- Program office
- IT risk register
- Project management
Assessing where an organization stands in relation to these areas, as discussed later in this paper, can provide it with insights on how to model its own IT risk management program. While this model represents the ideal, every business and IT environment has different IT risk needs and exposures that will determine to what degree they should and can follow the components covered by this model. As an ideal, it should be viewed as a guide and reference to help an organization build an effective IT risk management program that is the most appropriate for its unique risk posture and culture.

Culture

Every business has a different culture and a different attitude with regard to IT risk. In some industries, such as banking, risk plays an integral role in day-to-day operations. Banks profit by addressing financial risk in a very structured, methodical, and systematic manner, relying heavily on mathematical models. On the other hand, other industries are very risk averse and endeavor simply to “remove” as much risk as possible from their business.

Some organizations might be heavily concerned with regulatory compliance, while for others it might be barely a worry. A majority of organizations might cite business continuity as critical to their livelihood, but each will likely have a different tolerance for business disruptions or differing views on how long systems can be inaccessible before they have a significant impact on business.
Enterprises with customer-facing Web sites might demand the highest levels of performance and accessibility from their hosting centers, while for other businesses Web performance is just a minor concern.

These risk postures, combined with the varying attitudes toward risk of individuals within the organization, form the basis of the organization’s IT risk management culture. Understanding the risk culture means understanding how the business operates, what is considered acceptable and unacceptable risk, how certain risks affect business operations, and the prevailing attitudes of executive management toward IT risk.

Before an organization can create an IT risk management program that makes sense for its unique situation, there needs to be a clear understanding of its own risk attitudes and culture. Without this understanding, organizations may find it difficult to obtain the needed levels of executive sponsorship and could invest their IT risk management budget inappropriately.

The risk culture itself can also determine the effectiveness of an IT risk management program. The elements of the culture that can have a direct impact on the success of an IT risk management program include:

- Visibility and execution
- Awareness and communication
- Ownership and participation
- Incentives and penalties

Visibility and execution

One of the keys to understanding an organization’s risk culture is first determining the overall visibility of IT risks within the company. To what extent is IT risk a topic of concern within the organization? How often are IT risks discussed among board members, and do projects that target IT risk typically receive funding or support from an executive level? If an IT risk is discovered, is there a defined methodology to address that risk?

Unfortunately, in some organizations there is little or no visibility of IT risk at the executive level. Likewise, they often lack a standard approach to managing IT risk. If they uncover a risk, they spend some time and money to address it, but it’s typically a very reactive approach.

One of the keys of a successful IT risk management program is establishing the appropriate levels of visibility for IT risk among executives and board members. When business and IT operate in alignment with regard to IT risk management, it not only becomes easier to identify how IT assets and operations support business activities, but it also clarifies what areas of IT risk have the greatest potential business impact and what areas will have the lowest impact. This clarification helps prioritize and justify the needed investments to mitigate against potential risks.
Aligning business and IT risk concerns also has the potential to close risk gaps that could leave an organization critically exposed to a wide variety of internal and external risks. It eliminates duplication of effort and over-investment, which in turn wastes resources and creates unnecessary IT complexity and cost.

When executive management gives IT risk the proper attention, it creates an environment where the business side and the IT side of the organization can come together to create a comprehensive IT risk management program and a plan that is appropriate for the needs of the company. Such an aligned program not only lays the foundation for an effective strategy for mitigating IT risk, but it also can guide system design and decision-making that results in higher operational efficiency, greater capacity for innovation, lower IT costs, and reduced IT complexity.

**Awareness and communication**

Making IT risk visible at the executive level, as well as bringing business and IT interests in alignment, starts with communicating and raising awareness of IT risk concerns. How to best communicate these concerns will vary from company to company, but there should at least be a formal process in place for communicating throughout the organization the details of existing IT risks. Ideally, this communication process should be able to inform all stakeholders in a proactive manner about all IT risk initiatives, as well as the benefit and value that these initiatives bring to the business.

The communication vehicle may take many forms, including IT risk education programs. Such education programs could be on an informal ad hoc basis to train specific stakeholders, or they could be more formal and fully structured programs that educate all stakeholders on an ongoing basis. The use of “Risk Dashboard” technologies can also assist greatly in the area of awareness and communication.

**Ownership and participation**

Even if IT risk concerns are effectively communicated and executives are aware of the impact that these risks can have on the business, unless someone at an executive level takes responsibility for IT risk management efforts, those efforts may struggle to succeed. Lack of executive ownership for IT risk management typically signals that there is no real executive interest in the program.

At a minimum, IT risk management should have board-level sponsorship, even if that means related efforts are only periodically reported on. Preferably, such issues should be reported on a regular basis and a board-level executive should be formally accountable for the IT risk management program. Ownership of the IT risk management program at an executive level enables it to operate as a dedicated, centralized function that manages and coordinates all IT risk management initiatives.
Executive ownership gives the program the priority status needed to obtain and assign the required resources for IT risk mitigation initiatives. It makes it easier to establish a formal means for acquiring needed funds and resources, rather than only being able to get resources on an ad hoc basis as they become available.

Another aspect of executive ownership is making sure that there is the appropriate level of participation in the program from all stakeholders. Achieving appropriate participation in the program begins with helping all stakeholders understand their responsibilities in terms of the different IT risk management initiatives. Proper participation also means that responsibilities of all stakeholders need to be coordinated, including any third-party stakeholders with IT risk management responsibility. For some organizations it might be sufficient to have some risk areas only loosely coordinated with various stakeholders. The optimum goal would be to have all IT risk management efforts tightly coordinated and integrated with all stakeholders.

**Incentives and penalties**

Incentives play a vital role in the success of any IT risk management program. Without the proper incentives in place, human nature dictates that few within the organization will feel the necessity to support or conform to any IT risk management initiatives. Effective incentives might come in the form of pay, with the incentives either being on the positive or negative ends of the remuneration scale. Whatever the incentives, they need to start with individuals clearly understanding the consequences of not supporting or conforming to IT risk initiatives. The communication of these consequences can be formalized within individuals’ job descriptions.

However, there not only needs to be an understanding of the consequences to the individual for non-conformance, but individuals also need to understand the consequences that their action or inaction can have on the business as a whole. Too often, few people in the organization fully realize the benefits or risks to the business that are associated with conformity to IT risk management practices. It’s a step in the right direction when at least senior management has a fundamental understanding of the risk and benefits of supporting the IT risk management program, but it’s far better when all stakeholders understand the business and individual consequences. Likewise, in terms of remuneration, providing incentive rewards to senior management is recommended, but providing incentive rewards to stakeholders at all levels, including third parties, is even better.
Governance

After gaining an understanding of its culture—through its assessment of its needs in terms of visibility, execution, awareness, ownership, participation, and incentives—an organization needs to look at how it can best govern its IT risk management program. To effectively deal with the ever-changing risk landscape, the overall governance of the program should have a formal, well-organized structure that can continue beyond the life of individual risk initiatives and projects. Governance needs to be ongoing to ensure that the program doesn’t cease to exist just because a certain project comes to a close. It needs to embrace a comprehensive view of risk management, addressing current risks while looking ahead to future risks.

Effective governance of the IT risk management program resides at multiple levels of responsibility. From the CIO to the backup administrator, everyone in the organization needs to share a common understanding of how their individual areas of responsibility relate to the IT risk management program.

When considering how to govern their IT risk management programs, organizations should look at the following areas of concern:

- Organization and stakeholders
- Objectives
- Scope
- Risk management strategy
- Reporting mechanisms

Organization and stakeholders

Businesses must determine what type of organizational structure is most appropriate to govern their IT risk management program. This could be a central governance committee or council comprising key individuals from various aspects of the business. Whether it’s a large or small governing body, it needs to have top-down authority and responsibility to clearly communicate, delegate, execute, and lead the program initiatives for the entire enterprise.

The governing body should communicate and meet on a regular basis with all stakeholders to ensure that business and IT concerns stay aligned, and to make sure the enterprise remains invested in the overall risk management strategy. Stakeholders should be individuals from all aspects of the business, and their responsibilities with regard to the program should be clearly defined. As needed, the governing body and the program’s stakeholders should have access to external IT risk management expertise to complement their abilities to perform their responsibilities.
The organization should also define and document its governance processes for the program to ensure conformance with IT risk initiatives from all parts of the business. Regular communication with all stakeholders and a formal definition of processes will help prevent different individuals within the organization from initiating their own risk mitigation projects without direction from the program’s governing body.

**Objectives**

The governance body needs to set objectives as they relate to IT risk management. These objectives need to be based on the culture of the organization and in line with its agreed-upon risk tolerance and risk posture. Objectives must be measurable to allow the organization to determine if its risk initiatives are being successful. Since the risk landscape changes regularly, these objectives need to be reviewed on a regular basis by the governance body to ensure that they still appropriately reflect the needs of the business and IT infrastructure. For example, an objective for one organization might be to ensure a specific level of uninterrupted availability of certain key services, while another organization might have an objective that requires any new virus definitions to be deployed to all systems in the organization within a specified timeframe.

**Scope**

Defining the scope of the IT risk management program helps ensure that everybody understands what parts of the business and IT infrastructure the program touches. While some organizations might simply define the program’s scope on an ad hoc basis as certain events occur, it’s more effective to formally define the full scope of the IT risk management program and publish that scope definition to all stakeholders.

Also, if the scope is defined in a comprehensive manner, rather than limiting it to a few disciplines, organizations put themselves in a better position to focus time and money in the most appropriate risk areas for the business. A well-defined scope can also help make sure that the program encompasses all production environments and that it extends to all stages of the IT lifecycle, including development, testing, and maintenance. Definition of scope is particularly important within organizations that outsource elements of their IT operations to third parties.
Risk management strategy

Just as there need to be formal objectives for the IT risk management program, there also needs to be a formal strategy for achieving those objectives. Defining the strategy can be the responsibility of individual stakeholders within the varying disciplines, but ideally it should be done in collaboration between all stakeholders under the direction of the program's governing body.

To provide the greatest opportunity for success and ensure executive support, the strategy should be aligned with the organization's overall business strategy. Once the strategy has been defined and agreed upon—preferably with agreement at the executive board level as well—it needs to be communicated to all stakeholders, as described earlier in this document.

Reporting mechanisms

One of the reasons that many organizations struggle with IT risk management is that they don't have a clear picture of the effectiveness of their day-to-day management processes. They need a way to track, monitor, and report on their progress at implementing their strategy and attaining their objectives. Whether the data is gathered manually or in an automated fashion, it is desirable to have a reporting mechanism that is comprehensive in nature such that it can capture all aspects of the enterprise's IT risk management concerns. Ideally, the mechanism should be granular enough to be able to provide the detail on activities and trends required by stakeholders and the governing body, empowering them to properly carry out and manage their various responsibilities.

Executive management dashboards can provide an excellent solution for a risk management program's reporting needs. Their graphical and easy-to-comprehend interfaces facilitate the ability to chart progress and identify trends. Dashboards also enable stakeholders to leverage a common and integrated view of what is occurring in relation to IT risk, providing another means to help business and IT goals to remain aligned, while enabling the governing body to appropriately focus on and prioritize their risk areas.

Control areas and policies

Control areas and policies deal with enabling the effective execution and governance of the IT risk management strategy in line with the organization's IT risk culture and attitudes. It's about defining and establishing procedures that empower the stakeholders throughout the enterprise to invest in managing risk in accordance with the organization's agreed-upon objectives and strategies.
The topics of concern for control areas and policies include:

- Compliance definitions
- Policy definitions
- Execution procedures
- Risk tolerance alignment
- Monitoring and reporting
- Change management
- Business case definition
- Enforcement policy

**Compliance definitions**

In an IT risk management program, compliance deals with not only complying with the objectives of the program, but also understanding and complying with any government regulations and industry standards that are applicable to the organization. It is vital that all organizations understand how exposure to compliance risk can impact their business. As part of defining its risk management objectives and strategies, the program’s governing body needs to identify what regulations or standards apply to their business, as well as what their risk attitude is toward complying with them.

In addition to regulatory and external standards compliance, organizations should also develop policies and processes that enable them to be in compliance with management standards that are relevant to their business, such as ITIL® (Information Technology Infrastructure Library) and ISO 9000. By identifying all of their various compliance requirements, organizations should be able to create a comprehensive compliance framework. Such a framework should be audited on a regular basis, with its results made available to all stakeholders.

**Policy definitions**

To enable individuals to comply with and reach the program’s IT risk management objectives, they need to know what they need to do to achieve those objectives. Policies and procedures should be created in accordance with the defined scope of the program to guide individual and group behavior in regard to IT risk management. The policy creation process should include all appropriate stakeholders, and if feasible, the process can be aided by the help of external auditors with expertise in IT risk management.
Policies should be written in a clear and structured manner to enable people across the enterprise to act in a consistent and standardized fashion in those areas that affect IT risk. They should be holistic in nature, addressing people, processes, and technologies. Attention should be given to defining the policies in a way that makes it as easy as possible for individuals to follow them, facilitating consistent compliance. Inconsistency in compliance will have the effect of adding risk rather than removing it.

**Execution procedures**

Once policies have been defined and documented, stakeholders need to become aware of the policies and how to comply with them. Steps should be taken to continually educate all stakeholders so that they completely understand the policies. Processes also must be put in place that make it easy for stakeholders to effectively execute and comply with defined policies. These processes might include additional training to make sure that stakeholders have the skills necessary to execute against the policies. Processes might also be technology-based to automate some or all aspects of policy procedures. The key to proper execution is to have a formal means in place that enables personnel to understand and execute IT risk management policies and procedures in a manner that is both effective and consistent.

**Risk tolerance alignment**

To make sure that IT risk management initiatives meet the desired objectives of the program, all policies should be appropriately aligned with those objectives. This means that policies should also reflect the risk tolerance and attitudes of the organization’s culture as a whole, including both IT and business perspectives. This alignment helps avoid risk gaps, project duplication, and wasted resource investment. To help maintain risk tolerance alignment, cost/benefit analysis should be performed periodically to measure the effectiveness of the policies to determine the actual impact that policy compliance has on the business.

**Monitoring and reporting**

Tying directly to the reporting mechanisms discussed in the “Governance” section, IT risk management programs should have a way of monitoring the progress of initiatives. This monitoring capability also needs to provide a way to generate reports that allow key business stakeholders to analyze and evaluate the success of the program. It should provide sufficiently granular detail to facilitate this stakeholder analysis.
Change management
The IT risk landscape is constantly changing, and as it changes, the risk attitudes and concerns of an organization often change with it. As this happens, the program must be able to recognize these changes and have the flexibility to modify its objectives to match the new risk concerns.

Organizations should have formal processes or policies in place that enable it, on an ongoing and periodic basis, to monitor and evaluate the risk landscape. At a minimum, this requires that a specific stakeholder be assigned the responsibility to monitor and pay attention to any changes in the IT risk landscape.

To facilitate the ability to proactively adapt to these risk changes, the policies should also outline processes for intelligently and quickly making any necessary changes to the program’s objectives and structure. Failure to pay attention and adapt to changes in the IT risk landscape in a timely manner can leave an organization critically exposed and vulnerable.

Business case definition
All too often, IT risk management is viewed just as an insurance policy against something bad happening to the organization. While its primary concern often focuses on protecting an organization from events and incidents that can have a negative impact on business, an effective IT risk management program has the inherent ability to have a positive impact on an organization’s bottom line. Improvements made to an IT infrastructure as a result of optimizing IT risk management can contribute to increased operational efficiencies, improved quality of service, and reduced IT infrastructure costs.

When defining a business case for IT risk management initiatives, failure to highlight these positive impacts may lower the chances of having them approved at the executive level. Some IT risks are often relegated to “what if” scenarios, where they might be viewed as risks that are unlikely to affect the business. Business cases have a greater chance to receive approval when they can demonstrate that risk management initiatives not only protect the organization from potential harm, but that they can also improve business operations, service, and profitability.

To facilitate the creation of a balanced IT risk management business case, it’s helpful to leverage existing standard business case parameters that can be used to conduct formal benefit analyses for specific projects. These business case parameters should be based on best practice scenarios, and ideally should have evolved over time, shaped and defined with the involvement of the proper business stakeholders. Processes should also exist to review and update these parameters with appropriate frequency.
Enforcement policy

Just as there need to be incentives and penalties associated with the compliance of IT risk initiatives, there needs to be someone who is clearly identified as responsible for the enforcement of all IT risk management policies. All stakeholders need to be aware of this person’s role and responsibilities, as well as the consequences of failing to comply with a policy. These consequences should be documented and fully understood by all stakeholders.

To facilitate policy enforcement, a stakeholder map should be created and kept up-to-date that identifies which stakeholders are impacted by specific policies. Processes that support policy enforcement, such as notifications of policy breaches to concerned stakeholders and formal escalation procedures for dealing with breaches, should be put in place.

Program office

To ensure that IT risk management is approached in a comprehensive manner and that it serves the needs of the business as a whole, program management and governance should have a centralized IT risk management program office. Areas of concern for the IT risk management program office include:

- Management and conformance
- Funding and priorities
- Coverage
- Currency
- Project lifecycle
- Benchmarking and continuous improvement

Management and conformance

If feasible, the IT risk management program office should be a dedicated and well-defined operation. However, whether the program office is made up of dedicated personnel, a virtual unstructured team, or a single individual who splits time between this and other responsibilities, is not as critical as making sure that the program office can keep project initiatives aligned with the organization’s objectives. It must also be able to manage and coordinate those initiatives in a centralized fashion.

The program office should employ standard practices to ensure conformance and alignment with the program’s objectives. It should also be staffed with individuals that have the necessary expertise and skills to ensure that it operates effectively.
Funding and priorities
The program office must have sufficient influence to obtain the funding it needs to initiate projects that meet the organization’s risk objectives. Funding will typically be justified and obtained as a result of the project business cases that it presents to the executive board. To give its project business cases the best advantage, the program office might consider leveraging standard templates and processes that have proven successful in business case creation in the past.

The program also needs to make sure that the spending of allocated funds aligns with risk prioritization and the organization’s objectives. This starts with an effort to document all of the program’s priorities and then publishing those priorities to project stakeholders. Mapping out how all the priorities of the IT risk management program align with the program’s defined objectives can further aid this effort. The program office should also be prepared to handle priority changes that affect its budgets and resource allocation.

Coverage
The program office needs to have a comprehensive awareness of all the risks that the organization faces. An IT risk list, also known as a risk register, can help provide this awareness by showing the coverage of all previous, current, and proposed IT risk mitigation areas. The risk register should be constructed in a manner that helps the program office detect any gaps in their program operations, policies, and initiatives. It can also help the program office be sure that its scope is aligned with the scope of the IT risk management initiatives as a whole. In addition to having comprehensive awareness of risks, coverage also deals with having the appropriate levels of executive sponsorship to help guarantee that the program office can secure the funding it needs, when needed.

Currency
As mentioned earlier, the risk landscape is constantly changing. The program office needs to have methods and processes to keep its view of IT risk current, as well as keep the program’s priorities and objectives aligned with that changing landscape. This includes having suitable mechanisms in place to react in a timely manner to new mandates delivered by the executive board or governance body.
Project lifecycle
Whenever IT risk projects are initiated, the program office needs to manage them throughout their lifecycle. Ideally, the program office should act as a “governor” to any IT risk management projects that are running within the business. Just as the IT risk landscape changes, project scope can change or projects can encounter problems that need the attention of the program office. The program office needs to stay in control and involved with each project to keep initiatives on track and to ensure that each project creates the maximum value to the business. It needs to be aware of the status of all current and pending projects. It needs to be able to facilitate effective communication between itself and all IT risk management project managers. The program office should also have the authority to make project decisions based on the program’s objectives and direction from executive levels.

Benchmarking and continuous improvement
Effective benchmarking tools and processes need to be available to the program office to allow it to analyze the success, failure, and effectiveness of its projects. Along with the ability to evaluate project effectiveness, the program office should create and maintain procedures that continually improve the effectiveness of individual projects and the program office as a whole.

IT risk register
In its simplest form, a risk register is a list of risks. The risk register is key to helping stakeholders become aware of and understand the IT risks that affect their enterprise. As such, it should be comprehensive in nature, identifying all of the security, availability, performance, and compliance risks that pose a threat to a business’ ongoing success. To allow the organization to properly define and prioritize its IT risk management objectives, the risk register should also prioritize those risks.

In creating an effective IT risk register, the following aspects should be considered:

- **Scope and content**—The IT risk register needs to be comprehensive in nature, providing a holistic view of all applicable risks, preferably with information on potential impacts, probabilities, priorities, owners, and proposed action plans.

- **Lifecycle maintenance**—The IT risk register should be a living document that changes on a regular basis as the risk landscape changes.
• **Assessment and prioritization**—Risks need to be assessed and prioritized through an ongoing effort. The results of this effort need to be reflected on the IT risk register.

• **Gap analysis**—Processes must exist that can identify gaps in the IT risk management program. The IT risk register should be designed to aid in these processes.

Furthermore, the risk register should also be enduring in nature, meaning that once a risk appears on the register, it should remain on the register (even if in a dormant state) until the control area related to that risk changes. A dormant risk is a risk that has been subjected to remediation/mitigation and is currently considered to be in alignment with the prevailing tolerance level. However, the risk should still be subject to periodic review in accordance with changes in the prevailing risk landscape or the organization’s tolerance to that risk type. Such changes could cause the risk to become out of alignment and therefore require further mitigation or remediation.

**Project management**

The success of the IT risk management program depends largely on how effectively its varied initiatives and projects are executed. To achieve the highest levels of execution, organizations should follow standard best practice models for project management such as PRINCE2 (PRojects IN Controlled Environments, a de facto standard used extensively by the UK Government and is widely recognized and used in the private sector, both in the UK and internationally). Following accepted project management practices facilitates an organization’s ability to identify risk and mitigate them appropriately through well-run and highly effective projects. It also helps make sure that the planned objectives can be successfully achieved on time and on budget.

Keys to successful project management for IT risk initiatives include:

• **Ownership**—Each IT risk management project must have a designated project manager that is fully accountable for its outcome, and each project should have an executive sponsor that supports the project.

• **Planning**—A structured and formally approved project plan should govern the implementation of each project.

• **Controls**—Controls need to be in place to ensure that project plans are adhered to, and the control process should be monitored to ensure compliance with established policies.
• **Reporting**—Formal procedures should be in place to make sure that project managers are regularly and properly reporting project status to the program office and applicable stakeholders. Escalation processes must also exist to identify and resolve critical issues in a timely manner.

• **Review**—The project plan is a living document that should be reviewed often by the appropriate stakeholders. Preferably, such reviews should follow a formal structure and be comprehensive in nature to allow future projects to benefit from past experiences.

**Conclusion**

As organizations increase their reliance on information technology to drive their business success, it becomes more critical for them to be aware of, and effectively manage, their IT risks. While many organizations recognize the need to augment their IT risk management activities, too many of these efforts fall short because they don’t take a comprehensive approach to IT risk management. To succeed, organizations must address all aspects of IT risk concerns, including security, availability, performance, and compliance. IT risk management efforts must look at the needs of the organization from a holistic perspective, aligning business concerns with IT concerns. Also, rather than addressing IT risk in a tactical and reactive manner, organizations need to define and execute an overarching strategy that coordinates and embraces the IT risk needs of the entire business and IT environment on an ongoing basis.

The creation of an internal IT risk management program can empower organizations to take a holistic approach to IT risk management. It provides a vehicle to align business and IT objectives and establishes an environment that allows organizations to proactively, and on a continuing basis, effectively mitigate the risks that threaten a business. It provides a framework that helps organizations build a comprehensive IT risk management strategy to address all of their critical risk factors and fit their unique situation and needs.

Symantec defines IT risk management as an enterprise-wide approach to refining people, processes, and technology to achieve the organization’s preferred balance of IT costs and risks in order to improve the company’s overall performance. Its experience and expertise in the security and infrastructure management areas uniquely qualify Symantec to help organizations take a comprehensive approach to understanding and managing the risks to their IT systems, while reducing the complexity of those IT systems. Unrivaled in its depth of IT risk management and its breadth across the four key areas of risk—security, availability, performance, and compliance—Symantec understands how to apply technology and best practices to effectively manage IT risk.
Building a Comprehensive IT Risk Management Program

Furthermore, Symantec Global Services offers comprehensive services that help organizations assess their IT risk management needs, as well as design, implement, and manage comprehensive IT risk management programs tailored to fit their unique business, infrastructure, and risk tolerance requirements. Symantec Global Services provides the right people, processes, and technology to optimize an enterprise’s IT infrastructure and service delivery while managing their business and IT risk. When it comes to IT risk management, businesses can count on Symantec Global Services to help them keep their enterprise up, running, and growing—no matter what.
About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.