5

CHAPTER FIVE

Implementing ERM in the Enterprise

VIRTUALLY ALL LARGER PUBLIC companies today have some type of risk management department or function. All too often in past years, their formal enterprise risk management was structure as a lower level department which often was primarily responsible for purchasing insurance and implementing routine loss prevention programs for certain high-frequency exposures. That risk management function usually did not receive the respect it should deserve in today's era of COSO ERM. Often called the insurance department in past years, those risk management functions were not structured at a senior or C-level status in enterprise charts. A currently trendy term, *C-level* refers to an enterprise function headed by a very senior manager or officer-level person, such as a chief information officer (CIO) or chief audit executive (CAE). While perhaps not reporting directly to the CEO, C-level group heads often have a direct reporting relationship one level below the CEO, such as to the chief financial officer (CFO) or some other very senior manager. An effective risk management function here would be headed by a chief risk officer (CRO), an executive whose responsibility is to ascertain that enterprise risks are properly understood and translated into meaningful business requirements, objectives, and metrics.

Even if an enterprise has a traditional ''insurance department,'' the COSO ERM framework provides an enterprise with an excellent opportunity to reengineer their existing insurance-based risk management function along the lines of the COSO ERM framework or to create a separate new ERM function for the enterprise. Given the importance of risk management in today's enterprise, ERM functions should operate at a higher level than the traditional insurance-based risk function groups that sometimes operated side by side with such facility support functions as property security and loss prevention. While these latter functions are important to an enterprise, the ERM department should take a higher and more prominent role.

This chapter considers how to establish an effective risk management function following the COSO ERM framework and suggests duties and responsibilities for this important function as well as for the CRO. We will also suggest potential reporting connections for the group as well the appropriate levels and skills for the professionals who should manage the risk management function in today's enterprise. The chapter will provide insights on the roles and responsibilities of the CRO, who is very much part of that risk management function. The duties of this important risk management officer will vary across different enterprises depending on their size and type of operations, and while there certainly will never be a one size fits all description here, the chapter includes some general CRO best practices.

ROLES AND RESPONSIBILITIES OF AN ENTERPRISE RISK MANAGEMENT FUNCTION

The responsibilities of today's enterprise risk function have been broadened and deepened to include regulations, capital markets concerns, financial reporting, the many issues surrounding globalization, intellectual capital, and, of course, all aspects of IT. To be effective, the enterprise risk function and its CRO must have their eyes wide open regarding the various levels of risks impacting all levels of the enterprise. A more traditional risk management function, moving beyond the lines of an insurance department, should take steps to reorganize and reengineer themselves to follow the COSO ERM framework model, as introduced in Chapter 4. Of course, if there had never been such a formal operating unit in place, the launch of an enterprise risk management function provides an opportunity to strengthen controls and governance through the establishment of this risk management function.

We have described the COSO ERM framework shown in Exhibit 4.1 as a three-dimensional cube with various enterprise units along one dimension and operating functions across another. An enterprise will certainly not have a need for separate risk management functions for each of these units. For a public corporation, an enterprise risk management function should be a senior-level operating unit with authority covering the entire enterprise. For a larger enterprise with multiple and differing business operations, there may be a need for separate multiple risk management units, but all should report to a single responsible risk function headed by a CRO. An enterprise with some very different business units, such as for consumer lending or legal document processing, may see some significant risk exposure differences across these two lines of business and may want to have separate risk management groups to monitor and control the separate exposures in each. However, each of these groups may follow some similar procedures and should report up to a central, corporate risk management department typically led by a CRO.

Exhibit 5.1 describes the general functions or responsibilities of an enterprise risk management function. Whether a relatively small organization or a multidivision,

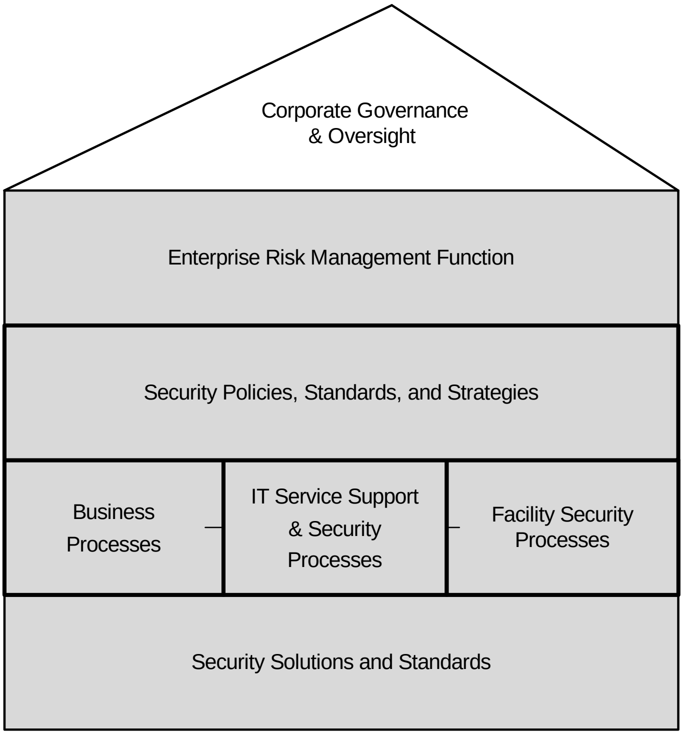

Corporate Governance
& Oversight
Enterprise Risk Management Function
Security Policies, Standards, and Strategies
Business Processes
IT Service Support & Security Processes
Facility Security Processes
Security Solutions and Standards

EXHIBIT 5.1 Enterprise Risk Organization Responsibilities

multicountry type of enterprise, any risk management function should follow these same general operational standards and guidelines. Many of these activities are referenced in other chapters, but the following paragraphs outline such a COSO ERM risk function. That enterprise risk function should develop policies to respond to either specific risks or regulatory requirements and then forcibly push the guidance down to the lines of business for execution, usually at their discretion. Given the closely interrelated business risks and strong regulatory-environment penalties for noncompliance, this is especially important because weak performance by any one business unit can place the entire enterprise at risk.

CRO Responsibilities

A key component of an effective ERM function is the need for enterprise leadership that is responsible for the overall risk management process. Enterprise risk management is usually the responsibility of a CRO, a designated senior enterprise officer responsible for administering and monitoring the overall enterprise ERM function. Although persons with the title of CRO have existed in industries ranging from financial services to the electrical power industry for some years, an increasing number of enterprises today are appointing persons with the CRO title to manage their risk functions. However, that title of "chief" means little unless the CRO has the authority and responsibility to effectively manage the enterprise risk program and to communicate these activities to senior management.

The major responsibility of the CRO is to manage the process of assessing risks throughout the enterprise, to implement appropriate corrective actions, and to communicate risk issues and events to all levels of the enterprise. The CRO should be responsible for the overall risk management function in an enterprise and should direct and manage a supporting risk management function. An effective CRO and the supporting risk management function are similar to the internal audit function. Just as internal audit has a staff of specialists to review all levels of internal controls and provide recommendations for corrective actions, an enterprise risk function should operate in a similar manner. It should monitor the overall risk environment in the enterprise as well as make recommendations for corrective actions as appropriate.

While internal audit functions,[1] with their relationships to the board audit committees, have been very much defined by auditing standards and legal requirements, the ERM process has not yet been given that level of recognition. If we have established a CRO, where or at what level does that individual belong or report? We feel that an enterprise's CRO should report and manage a function with many similarities to internal audit in today's enterprise. We have said ''many similarities'' because internal audit reports to the board of directors audit committee, but there often is no board risk management committee in today's enterprises. However, as will be discussed in Chapter 13 on the importance of effective enterprise governance practices in the corporate board room, today's board of directors should have a strong interest and responsibility in their enterprise's ERM function.

We suggest that an enterprise risk management function, headed by a CRO, should be one of the senior-level management executives in today's enterprise, reporting to the CEO or at least one level down, such as to the CFO or chief operating officer. The CRO is a key executive who should have the authority to review risks throughout the enterprise and to facilitate corrective actions to repair or minimize those risk situations. Using our Global Computer Products example company introduced in Chapters 1 and 3, Exhibit 5.2 describes a general position description for a CRO, reporting administratively to the CFO and directly to the chair of a board risk committee. The CRO could report in this matter or alternatively to the CEO on the same level as the CFO and other senior corporate officers. The function would have the responsibility to assess and evaluate risks throughout the enterprise, making recommendations for corrective actions as appropriate.

While a single CRO could theoretically perform all of the duties and responsibilities described in this example position description, there will normally be a need for a supporting staff of risk management specialists reporting to the CRO. These are persons with the abilities to understand and help implement corrective actions for general business, IT, and basic insurance-related risks. Whether it be recommending improved internal controls or helping to secure appropriate insurance coverage, an effective enterprise risk management function should have several staff specialists to help review and help minimize enterprise risks. ERM specialists should have the authority and responsibility to both identify specific enterprise risks and to actually help implement corrective actions to minimize those identified risks.

This description defines the roles and responsibilities of a chief risk officer (CRO) for this book's Global Computer Products example company. It is a newer type of position; there are limited standard or example CRO position descriptions published, although a Web search will find some examples.

- General Responsibilities

  The chief risk officer is responsible for assessing all risks that may impact the company—financial, operational, IT-related, and environmental—and for leading in developing appropriate actions to minimize those risks. Responsibilities include direct management of enterprise risk management functions at corporate headquarters units and domestic operations as well as advisory responsibilities over all nondomestic international risk management functions.
- CRO Reporting Relationships

  Reporting directly to the chief financial officer (CFO) for administrative purposes, the CRO reports to the board of directors risk committee for action and strategy guidance. The CFO also has a strong advisory relationship with the management risk committee, under the CFO, for collaborating on the development and implementation of risk management policies and procedures.
- Duties and Responsibilities
  - Develops, initiates, maintains, and revises policies and procedures for the general operation of the enterprise risk program and its related activities to prevent illegal, unethical, or improper conduct. Manages day-to-day operation of the program.
  - Performs an overall assessment of all risks impacting the enterprise, and reports to the board of directors risk committee on the status of these risks and actions taken to control them, at least on a quarterly basis.
  - Collaborates with other departments (e.g., internal audit, employee services, etc.) to direct enterprise risk issues to appropriate existing channels for investigation and resolution. Consults with the corporate legal department as needed to resolve difficult legal enterprise risk issues.
  - Responds to all identified fiscal, operational, IT, or general environmental threats through coordination with appropriate managers in the organization. Develops and oversees a system for uniform handling of such risk-related threats.
  - Acts as an independent review and evaluation body to ensure that enterprise risk issues/concerns within the organization are being appropriately evaluated, investigated, and resolved.
  - Monitors and as necessary coordinates enterprise risk activities of organization units to remain abreast of the status of all enterprise risk activities and to identify issues and trends.
  - Identifies potential areas of enterprise risk vulnerability and risk; develops/implements corrective action plans for resolution of problematic issues; and provides general guidance on how to avoid or deal with similar situations in the future.
  - Provides reports on a regular basis, and as directed or requested, to keep the Corporate Enterprise Risk Committee of the Board and senior management informed of the operation and progress of Enterprise Risk efforts.
  - Establishes and provides direction and management of the enterprise risk hotline.
  - Institutes and maintains an effective enterprise risk communication program for the organization, including promoting (a) use of the enterprise risk hotline; (b) heightened awareness of all levels of evolving risk threats, and (c) understanding of new and existing enterprise risk issues and related policies and procedures.
  - Works with the human resources department and others as appropriate to develop an effective enterprise risk training program, including appropriate introductory training for new employees as well as ongoing training for all employees and managers.
  - Monitors the performance of the enterprise risk program and relates activities on a continuing basis, taking appropriate steps to improve its effectiveness.

EXHIBIT 5.2 Chief Risk Officer (CRO) Position Description

While an enterprise risk management function may look similar to an internal audit department, there are some key differences. Internal auditors review internal controls and make recommendations for improvement but usually take no active role in helping to implement those recommended changes, unless specifically engaged as internal consultants. The effective enterprise risk management group, however, should take a more proactive role in helping to implement the necessary corrective actions. This often can be a challenging set of roles and tasks for enterprise risk analysts in an enterprise. Some examples of how an effective enterprise risk management function might operate include:

- An enterprise risk management analyst reviews the potential new product liability risks in a given business area. Rather than just recommending that the unit search for appropriate insurance coverage, the analyst might take an active role with other members of the enterprise risk group to help secure appropriate coverage.
- Either as part of a direct review or from general information, the risk management function may identify governmental actions that may place some foreign country operations at risk. The risk analyst might work with legal counsel, foreign unit management, or outside advisors to take actions to limit the effect of those governmental actions.
- An enterprise risk management specialist with strong IT skills may access system vulnerabilities in what is often called a firewall perimeter surrounding an area of IT operations. Perhaps working with technical IT staff members, the ERM specialist would help to implement a more effective enterprise-wide security strategy.

Another very important difference between an enterprise risk management function and internal audit is that the ERM group will usually go beyond just reviewing an area and making recommendations for subsequent follow-up. While their professional standards allow internal auditors to serve as internal consultants helping with solutions, they often just report their recommendations for responsible managers to take corrective actions. While their professional standards do allow internal auditors to act as consultants as well as reviewers,[2] many internal audit groups today only review and make recommendations but do not help to implement those recommendations. The effective risk management consultant, in contrast, often will take a very active role in helping to implement effective solutions. External auditors, pre-Sarbanes-Oxley (SOx), once were very involved in reviewing an area and then suggesting that their own consultants take appropriate corrective actions. The rules in SOx have eliminated that function, and external auditors today are only focused on attesting to the adequacy of financial systems internal controls. The role of internal auditors in enterprise risk management will be discussed in Chapter 14.

Risk Management Enterprise Governance and Oversight

Risk management historically was not a top-tier function in many enterprises. With its frequent association with the enterprise's casualty and liability insurance functions, these groups were sometimes called risk management but were often just known as the corporate insurance function. For many enterprises, these risk management groups operated as lower level support functions with essentially no role in entity-wide issues. Under COSO ERM, as was introduced in Chapter 4, today's risk management group should be much more than just the insurance department. An effective risk management function, led by its own CRO, should report to a senior management level in the enterprise. That explains the cap or upper enterprise level in Exhibit 5.1. While SOx mandates that internal audit must report to the audit committee, there is no such reporting requirement at this time for other important functions such as risk management.

Chapter 13 discusses the importance of ERM in the board room and suggests the establishment of a formal risk committee, separate from the audit committee and reporting to the full board. That chapter will provide some examples of how such a committee functions. We recommend that such a board level risk committee, as described in Exhibit 13.2, should be considered. Otherwise and without such a special risk committee, we are suggesting here that risk management should regularly and periodically report to the audit committee or even some other related board committee. This additional reporting responsibility can be a challenge for many audit committees. Given the internal audit management requirements that SOx has imposed on audit committees and on the board in general, those committees typically are busy enough such that they do not need another set of meetings and reporting relationships. However, the enterprise's risk management function is sufficiently important to the overall welfare of the enterprise, and time should be allocated for the CRO to meet with the audit committee or the full board on a periodic basis to describe the status of risk management activities in the enterprise as well as any identified problems or concerns. Because they already have established lines of communication, the CEO, CFO, or the CAE should work with appropriate board members to make arrangements for establishing this review process as well as periodic risk management briefings. These arrangements will be discussed in greater detail in a section in Chapter 13 on the importance of ERM in the board room.

Whether it be to a committee of the board or to the CEO, many risk management activities are sufficiently critical to the overall enterprise that decisions and planned actions should be passed over to the appropriate persons to make any risk-related decisions. For example, the federal Gramm-Leach-Bliley Act (GLBA) mandates that enterprises establish privacy protection over certain personal and financial data. However, there is some level of ambiguity in these rules even though there also can be potential legal penalties if the poorly defined rules are not followed. The CRO can help with an effective implementation here, but others such as the CEO and legal counsel should review and help decide how to establish effective compliance processes to operate within those rules. If the enterprise gets in trouble with such a violation, it is better to have other senior officers or even an appropriate level of the board to at least review and approve approaches rather than just pointing fingers as the CRO. This is enterprise governance!

The reference to GLBA highlights just one of the many laws or other rules where risk-based decisions are needed. In addition, Chapter 13 discusses the importance of

ERM in the corporate board room and how that function should become more involved with this very important process. Whether it be members of the board, the CEO, or others of sufficient stature, there should always be some level of governance and oversight above the enterprise risk management facility to review and make any necessary hard decisions.

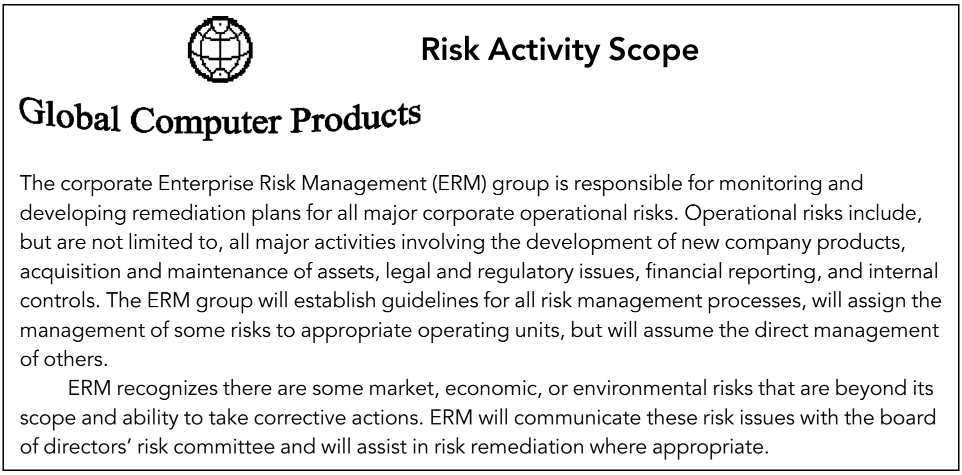
ERM Activity Scope and Review Planning

Other chapters describe many different and important ERM activities. For example, a process for estimating the likelihood and consequences of various risks facing an enterprise was discussed in Chapter 3, while Chapter 16 provides guidance in understanding the various levels of risks in an IT environment. These and others are all important activities of the enterprise risk function. An effective ERM function should not, however, just go from one risk-related area to another without any type of organized plan or approach. While a risk management function, by its nature, will be somewhat of a crisis-driven group, that same ERM function should still follow a risk review plan covering an extended time period. By its very nature, risk management will always be responding to crises as they occur, but that response should try to follow a standard, consistent approach throughout the enterprise.

An enterprise ERM function should first develop an understanding of and document the risk areas that are in their scope of operations. There are always some risk events either too big or too minute to be included within the scope of the ERM group. We are referring to very major events such as violent weather, major economic disruptions, and the like. The CEO along with the risk management organization may be able to have some high-level risk response plans in place for such events, but often cannot realistically do much beyond having some very general plans or statements of support in place. Similarly, there will always be some risk areas that are perhaps troublesome difficulties but are not within the scope of the ERM group. An enterprise risk management group needs to formally document the risk areas that are within its scope as well as any that are just "too big" or "too small." Of course, the risk management group should not post signs on its front doors stating "don't call us unless . . ." but should have some internal guidelines coving the types of risks it can realistically manage.

These enterprise risk scope declarations should be formally reviewed and approved by the board or CEO-level management. This is the type of scope information, however, that does not need to be communicated to all levels throughout the enterprise. There is no need to formally declare that the risk of food commodity thefts in employee dining rooms worldwide are outside of ERM's scope. That will only raise "no one cares" types of potential actions. Just as an internal audit function will develop some general scope-related statements, the enterprise risk group should do the same.

Our example company first introduced in Chapter 1, Global Computer Products, provides a method to describe this risk scope approach. The risk environment there was described in Exhibits 1.4 and 1.5. Using these descriptions, Exhibit 5.3 summarizes the risk activity scope for our sample company, Global Computer Products. Again, this type of risk responsibility scope document should be an internal ERM policy statement and



Risk Activity Scope

Global Computer Products

The corporate Enterprise Risk Management (ERM) group is responsible for monitoring and developing remediation plans for all major corporate operational risks. Operational risks include, but are not limited to, all major activities involving the development of new company products, acquisition and maintenance of assets, legal and regulatory issues, financial reporting, and internal controls. The ERM group will establish guidelines for all risk management processes, will assign the management of some risks to appropriate operating units, but will assume the direct management of others.

ERM recognizes there are some market, economic, or environmental risks that are beyond its scope and ability to take corrective actions. ERM will communicate these risk issues with the board of directors' risk committee and will assist in risk remediation where appropriate.

EXHIBIT 5.3 Risk Activity Scope: Global Computer Products

would not be developed for general distribution to enterprise stakeholders at large. Rather, it shows ERM's areas of risk management expertise, where the enterprise is responsible for various risks, and the acceptance of other entities, such as the legal department or local fire departments, for handling other risks. This is the type of document that the CRO should share in a board or CEO-level briefing so that they are aware of the ERM's planned area of scope. The CRO should gain approval and endorsement for these high-level plans or should adjust them in light of suggested changes.

Beyond these high-level scope statements, the risk management group should establish a strong understanding of the higher risk areas that are with their defined scope and develop risk management project plans for these enterprise risk areas. This is the process of defining risk likelihood and criticality as was discussed as part of risk management fundamentals in Chapter 3. Regarding the selected higher risk areas, the enterprise ERM function needs to develop a monitoring or review approach. That is, if a risk area has been selected as one for risk management concern, the ERM group should place the area on its ''radar screen'' for potential situation monitoring or reviews. This risk monitoring approach differs from internal audit that just selects some area for review and then performs an internal controls review of that area. Such reviews will typically result in a formal internal audit report with its findings and recommendations.

Based on its estimate of the higher likelihood and higher loss probability risk areas, the enterprise risk management function should monitor and review risk areas taking the following approaches:

- **Initiate Immediate Action to Resolve the Risk.** Based on initial risk assessment reviews and input from others in the enterprise, there may be some outstanding risks that appear about to occur and that can be fixed or corrected almost at once. Examples would be an item of production equipment that looks as if it will fail soon because of ongoing minor failures or the compliance status of some regulation where governmental authorities have not asked questions as yet but enterprise compliance seems shaky. Either through their own actions or coordination with others, risk management should schedule appropriate correction actions as soon as possible.

- **Review the Risk Area and Propose Corrective Actions to Reduce Risk Exposures.** With this approach, the enterprise risk management group acts somewhat like internal auditors or internal consultants. They will review some potentially higher risk area and make suggestions for corrective actions to improve or limit the risk. They do not have the same level of authority as internal audit with its audit committee and SOx Section 404 continuous monitoring responsibilities, but the ERM group's special knowledge of understanding risk management situations should give them a special level of respect. This process of enterprise risk reviews is discussed later in this chapter.
- **Arrange with Internal Audit to Perform a Review of a Selected Risk Area.** In some instances, the nature of the high-risk area may be caused by or based on poor internal controls. While the enterprise risk group can assess internal controls and business risks, in some instances it may be more efficient for the enterprise management to request that internal audit perform an internal controls review, following their standards, over the potential higher risk area. This will require some coordination but can be very effective if there are strong communication links between risk management and internal audit. These arrangements are further discussed in Chapter 14.
- **Monitor the Risk Area on a Continuous Basis.** Some identified risks represent areas where a risk event may not occur because of weak internal controls that could be improved but because of external factors require monitoring. An example might be the risk of currency devaluation in a foreign country unit. Risk management needs to assign someone from the ERM team as well as local management to monitor these types of potential events. While plans for corrective actions should be in place, there is no need to activate them until the actual event occurs.
- **Develop Plans to Take Action Only in the Event of a Risk Occurrence.** This is a more passive approach, but still can be appropriate for some lower likelihood but higher impact risks that still should at least be on the "radar screen." With plans in place and frequently updated, the risk management group would need to go into action only if the risk event occurs or appears to have a high probability of occurrence. This is a fire extinguisher mounted on the wall type of risk management approach. It is important that such a fire extinguisher remain charged, but it is only used in the event of an actual fire.

Based on this set of potential risk events ranging from those that need to get corrected at once to others only placed on a watch list, risk management should develop an annual risk assessment action plan. Such a time plan would assign responsibilities for the coverage of various risk events, estimate the enterprise risk group's time to correct and review, and include some time and budget estimates. This can become the

Global Computer Products ERM Group Plans—Fiscal Year 2012

Operating Division	Planned Risk Assessment Activity	Responsibility	Planned Actions	Start Date	Due Date	Estimated Remediation Costs
Product Dev.	New Product Security Risks	ERM & IT	Corrective Action Plan			
Product Dev.	India Computer System Operations	ERM	Review			
Product Dev.	Key Documentation Controls	ERM & IA	Corrective Action Plan			
Finance	Vendor Agreements	ERM	Review			
Finance	Staff Risk Management Training	ERM & HR	Implement			

EXHIBIT 5.4 Annual Risk Action Plan Example

enterprise risk management group's action plan for the period. The plan should be reviewed and approved by senior management, and when others such as internal audit are expected to complete portions of the action plan, these events should be coordinated. Exhibit 5.4 is an example of this type of action plan using the Global Computer Products example company.

Although planning approaches can vary, this sample plan shows areas where the risk management group is planning a formal risk assessment of some areas, where it is planning on helping to install some improvements elsewhere, where it is coordinating a review with internal audit, and where it is just monitoring an area. Because the latter also takes time and resources, monitoring activities should be planned as well.

Risk assessment corrective action plans are somewhat different from many other enterprise events because they must be based, in part, on actions that must be taken in the event of an unanticipated risk event. An explosion at a nearby but unrelated other production facility could hamper operations at a company-owned facility. However, that explosion is an entirely unknown and unanticipated event. The risk management team would have to spring into action to help get the company facility back in operation if such an unexpected event occurred. That action would certainly interrupt the annual risk action plan, but also would provide a priority type of list showing where adjustments should be made.

The financial accounting rules of establishing allowances for doubtful accounts can help in planning for these unknown risks. When selling goods, an enterprise typically ships the goods and sends the customer an invoice for short-term but later period payment. The transaction is initially recorded as an accounts receivable due from the customer with the final sale recorded when cash is received. However, no matter how good are the customer credit screening processes, there will always be a risk that some customers just do not pay or pay only partially after protracted disputes. Based on the overall payment history of all of its customers, companies establish an allowance for doubtful accounts reserves to offset and estimate that a certain but hopefully small number of customers will never pay. An enterprise risk management function should use this type of approach when planning its risk management monitoring activities. Although it will typically not have any history or advance knowledge regarding these risk events, it is prudent to develop the risk management plan with the allowance that there may be some level of unanticipated risk events during the period.

When developing these scope assessments and risk action plans, the CRO and the risk assessment team should always allow for and consider the broad objectives of the COSO ERM framework. That is, plans should be based on an enterprise-wide basis with an application across every level and unit. This says that there must be a strong level of communication, collaboration, and risk planning across the overall enterprise. This requires a much more expanded view of customer credit risks than traditional business risk management approaches to enhance and protect the value of the overall enterprise.

RISK MANAGEMENT POLICIES, STANDARDS, AND STRATEGIES

COSO ERM has moved the enterprise risk management function from a more traditional, risk-by-risk approach to a perspective that covers the entire enterprise on a continuous monitoring approach. To achieve that scope, however, the risk management function must encompass all enterprise units and levels. It cannot just be run or managed by a CRO with a small staff at headquarters. The ERM function must be managed and communicated to a wide group of responsible persons throughout the enterprise. In addition, the enterprise risk management function, under leadership by the CRO, needs to develop some risk management policies and standards that are followed by units in the enterprise, following a consistent strategy. Designated managers throughout the enterprise should be trained on these risk management policies and then charged with their implementation.

Our point here is that while enterprise risk should be managed and directed by a central CRO-led function, responsibilities and tasks need to be pushed down and across the enterprise by building a risk-sensitive culture throughout the enterprise. Stakeholders at all levels need to be aware of some of the risks that the enterprise is facing, the consequences of those risk exposures, and some of the steps they can put in place to limit those risks. The following list provides some of the steps necessary to build and implement an effective risk management culture in an enterprise:

- **Build a Risk-Awareness Culture.** As part of building an effective ethical culture in an enterprise, the ‘‘tone at the top’’ messages of senior executives to others in the enterprise are very important. When a CEO addresses key employees about the importance of having an ethical culture and strongly endorses and supports the enterprise’s code of business conduct, others will typically pay attention. The same concept holds true for risk awareness, but this can sometimes be a little different.

Information Security Content Risks. There are multiple areas where an enterprise might have numerous levels of unprotected information assets such as information technology (IT) program source code and tables, product plans, engineering drawings, product formulations and patent materials, and database lists of customers and vendors. There is a need to understand and document these various types of information assets and the current control procedures in place, with an emphasis on the most potentially vulnerable. These should then receive priority for content protection controls, and special scrutiny should be given to higher value document management or content management systems. Since the enterprise may not be able to establish content protection controls over all data assets, there should be a formal, documented record outlining why one set of content assets are at a higher, more immediate corrective action level than others.

Establishing Content Compliance. Content protection policies and procedures need to be clearly communicated to all stakeholders—employees, vendors, and others, similar to employee code of conduct guidance. These rules as to what types of content are sensitive and how they can be copied or captured should be defined as clearly as possible. All stakeholders should be asked to acknowledge that they have read and understand these content protection rules and they agree to abide by them.

Content Protection Technology. Sensitive content leakage incidents can occur at many levels including poorly controlled wireless transmissions, accidentally posting sensitive information on a public Web site or e-mailing sensitive information to a personal Web mail account. Traditional IT control procedures such as identity management and access control lists are necessary, and specialized software content monitoring and filtering tools should be considered. Typically, these tools register or ''fingerprint'' sensitive content stored in the file system or in content management repositories. Installed at the Internet gateway, such tools should be selected to monitor all of the content flowing out of the organization and detect attempts to transmit sensitive information. Policy actions need to be established to include alerting, logging, and actual blocking of the attempted transmissions.

EXHIBIT 5.5 Content Management Risk Awareness Guidelines

Due to the wide variety of internal and external risks that an enterprise faces at all levels, it is difficult if not impossible to build a comprehensive risk-oriented code of conduct document that is circulated throughout. However, an enterprise can develop and circulate some risk awareness documents that target either certain functions in enterprise operations or external threat risks. As an example, Exhibit 5.5 discusses some typical information security protection and content-related controls. Failures or violations here could put a single unit as well as the overall enterprise in jeopardy. Copying a description of a corporate financial plan through an e-mail cut and paste process and then sending it out could create an enterprise-wide trade secrets loss risk. Chapter 16 includes discussions of other IT enterprise security risks.

An enterprise should focus on multiple internal risks, such as information security protection, and develop and circulate this type of guidance to its various organization levels. This is the type of information that can be communicated through messages on Web intranet home pages, employee newsletters, or comments at management meetings. The whole idea is to communicate the concept that an enterprise always faces certain risks but those risk exposures can often be limited by awareness and participation in the enterprise risk management program.

These types of efforts will launch a risk awareness program and hopefully initiate a risk awareness culture.

- **Creating the Enterprise-Wide Risk Management Organization.** We have discussed the importance of promoting any existing enterprise risk management function to what has been described as C-level or a function headed by a CRO. In addition to just one individual with a CRO title, it is important to build an effective enterprise risk management function or group to support that CRO. As we have suggested through these chapters, an effective enterprise risk group or department will be somewhat of a hybrid between a traditional internal audit group and the older traditional insurance department that once was called risk management. It should also be a more active group that both monitors events but sometimes initiates its own program of corrective actions. An effective risk group should cover all aspects of the enterprise in terms of specialized facilities and locations of operations. While the specialties can vary, it is often very effective to have specialists with an understanding of accounting and finance risks, risks covering all aspects of IT operations and communications, and risks impacting areas of enterprise operations. For example, if an enterprise is a provider of health care–related insurance claims processing, its risk coverage over areas of operations might include a strong knowledge of the Health Insurance Portability and Accountability Act (HIPAA) rules, a complex, health-related, U.S. security-related law.

  An effective ERM function should be covered by staff professionals with a good understanding of the risks impacting the enterprise in that given area as well techniques for limiting risk exposures. This might involve expertise within the risk management group, contacts with specialized help when needed, or close coordination with other functions within the enterprise. For example, risk issues over IT disaster recovery and continuity planning are discussed in Chapter 16, and risk-related issues here might be covered by specialists within the IT organization. However, the enterprise risk management group should establish close communication and coordination links with those IT specialists.

  In addition to covering core specialized areas, the enterprise risk group should provide coverage to the entire enterprise in all of its locations. There is little value for a Houston-based enterprise with a CRO and the corporate risk management group to provide guidance that covers just Texas or even total U.S. operations if that guidance does not extend to some operations that may be in another country such as Argentina. There must be communication and coverage throughout the global enterprise. While establishing risk management staff functions worldwide may not always be cost-effective, strong training and procedures can establish some dotted-line relationships with other groups out of the home country to create an ‘‘eyes and ears’’ risk-monitoring process at other locations as needed.

  Enterprises are organized in many different sizes and shapes, and there is no one best risk management enterprise approach. However, there should be some CRO-led central or corporate risk management guidance to communicate risk-related objectives and plans to senior management. Based on the Global Computer Products’ background description in Exhibit 1.5, Exhibit 5.6 shows the enterprise

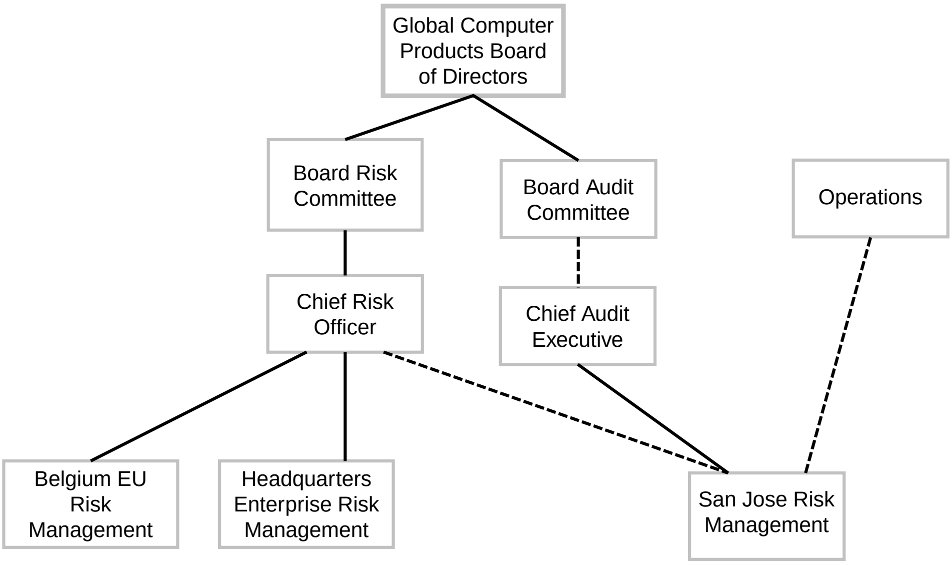
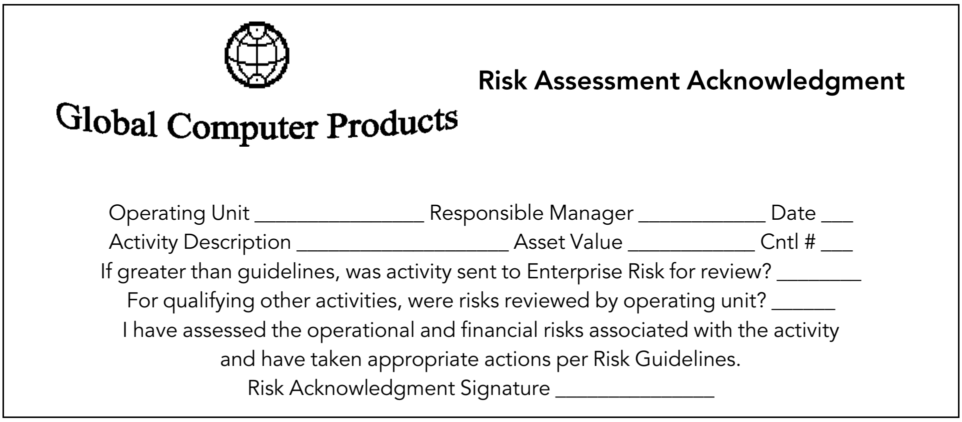


EXHIBIT 5.6 Global Computer Products Risk Management Organization

risk management enterprise chart for our Global Computer Products example company. It suggests a corporate enterprise risk management function based at its Chicago-area headquarters as well as a small risk management function located in its Belgium distribution center. This latter group would be responsible for monitoring European Union (EU) risk-related legal and regulatory issues as well as risks associated with the distribution operations there. Global's internal audit function has a branch or field facility near the computer security facility in San Jose, and the corporate enterprise risk function has established a strong dotted-line relationship for risk management with that group. Through policies, procedures, and training, risk management activities at other Global locations are handled through coordination and communication to assess risk issues at those facilities.

- **Enterprise Risk Management Policies and Standards.** In addition to building an effective enterprise risk management organization along with messages to help foster a risk-sensitive culture in the enterprise, a series of risk management policies and standards should be developed and communicated throughout. While the headquarters, CRO-led risk management team should be constantly assessing and reviewing higher level risks, there will be many risk related decisions that must be made at all levels such as the selection of a major new vendor, the acquisition of a significant new asset, or many smaller scale transactions. Risk assessment policies and standards should be developed that call for all members of the enterprise to consider enterprise concerns and considerations.

  An effective method to introduce risk awareness throughout the enterprise is to develop and distribute a risk assessment sign-off form that stakeholders are asked to consider whenever making a decision for the enterprise that involves more than



Global Computer Products

Risk Assessment Acknowledgment

Operating Unit ______________ Responsible Manager ___________ Date ___
Activity Description __________________ Asset Value ___________ Cntl # ___
If greater than guidelines, was activity sent to Enterprise Risk for review? ________
For qualifying other activities, were risks reviewed by operating unit? ______
I have assessed the operational and financial risks associated with the activity
and have taken appropriate actions per Risk Guidelines.
Risk Acknowledgment Signature ______________

EXHIBIT 5.7 Risk Assessment Sign-Off Acknowledgment Form

some parameter of *X* dollars, where *X* is a number to be determined depending on the location. Such a sign-off requirement should be included with all major purchasing transactions, such as a new material purchase requisition, and Exhibit 5.7 is an example of the types of words that might be included in such an acknowledgement. The idea is to request that all front-line managers, including those at smaller units or at foreign locations, personally acknowledge that they have considered relative risks when signing off or approving some financial transaction within their area or responsibility.

The purpose of such a risk assessment signoff form is not to "get" some employee who signed the form for some financial transaction that resulted in a failure, but to encourage all stakeholders to acknowledge that they have considered risks when authorizing and approving a financial transaction above some designated value. That value, of course, should vary depending on the size and scope of the unit. For a chain of fast-food restaurants, as an example, a procurement manager with responsibility for the entire chain might be asked to acknowledge consideration of risks for all supply purchases over $25,000, while a unit manager in that same chain would be asked to acknowledge consideration of risks for transactions over perhaps $500. At appropriate levels, all members of the enterprise should be asked to evaluate relative risks when making financial decisions.

This guideline form only asked stakeholders to specifically acknowledge that they have considered risks above some monetary level, but such a form does not cover such matters as legal risks, market risks, or IT-related risks. However, it can be a method to encourage all stakeholders to consider appropriate risks when making any transaction-based decisions in their area of responsibility. To encourage this type of thinking even further, an enterprise should deliver some overall risk awareness training to all levels of the enterprise. The idea is to get all levels to always remember that there are risks involved with any transaction and that the enterprise, by policy, should not enter into transactions that are above the enterprise's risk tolerance level.

BUSINESS, IT, AND RISK TRANSFER PROCESSES

The next and very important level to building an effective enterprise risk management program is to understand the risks directly impacting the enterprise and then to develop general remedial procedures covering them. We have grouped these direct impact risks into three general risk areas of business, IT, and transfer-related processes. While these categories are broad and arbitrary, transfer processes cover the insurance types of protections that are external to or beyond the regular control of enterprise managers. These also might include insurance coverage for a potential production plant fire, the risk that a governmental unit will impose some unexpected regulation, or the risks of general geopolitical changes in some area of operations. The category of IT risks covers both what auditors call general controls areas as well as business application–specific risks. These general controls areas include risks in IT continuity planning concerns such as a malicious attack on the IT network, discussed in Chapter 16. The remaining risks are classified as business-related risks and include a wide variety of concerns.

Timing can be a major consideration in assigning business risks to these areas of operations. IT-related risks are a good example of this timing consideration. The risk of a virus attack on the IT systems network is a very immediate type of concern. The risk event could occur with little warning, and the response to that risk also should be immediate. The business risks associated with a financial accounting error are of less immediate concern tied to periodic financial reporting cycles, and technical process risks are often more longer-term types of risk events.

While it is often difficult to easily split all risks into these three broad areas, this suggested split provides a good method for assigning all enterprise risks to appropriate people or functions in the enterprise. For example, while IT systems and related technologies cover all aspects of business operations, their technical nature and the need for specialized knowledge makes it convenient to assign them to an IT risk category ‘‘bucket.’’ Similarly, what we have called technical and transfer-related risk controls are those best monitored and controlled by persons outside business operations. These might include the law department for legislative rule matters, facility operations for fire control issues, and specialists in insurance coverage. Although the number of enterprise risk categories can be expanded, the idea is to somewhat divide up responsibilities for enterprise risks at a very high level.

The following summarizes some of these important enterprise risk categories. While we have discussed these on a fairly broad level, an enterprise should consider its basic areas of operations and develop a tailored and specific list based on these areas.

- **General Business Operations Risks.** The wide majority of enterprise risks discussed throughout these chapters should be considered as business operations risks. These are the wide range of financial, competition-related, and business operations risks that are major enterprise concerns. Following COSO ERM guidance, these risk areas can be considered in the following manner or order:
  - **Risk Management Focus.** Emphasis should be on financial risks associated with breakdowns in internal accounting controls.

  - **Business Operations Scope and Risk Objectives.** Protecting enterprise value with an emphasis on treasury and insurance.
  - **Risk Management Emphasis.** Objectives should be established over financial and other business operations covering only limited risk areas, operations, and processes.

  COSO ERM has broadened these traditional risk factors and moved to an overall entity-level set of considerations. Following the description of the enterprise-wide risk framework discussed, the risk management function should establish communication links and monitor both risk events and activities throughout the enterprise. This is the portion of an effective risk management function that should identify significant risk areas in all levels and dimensions of the enterprise and should take steps to both review the levels of exposures to those risks and initiate corrective actions.

- **IT General and Application-Specific Risks.** While Chapter 16 will discuss more details on the types and natures of IT risks, it is usually convenient to classify IT-related risks in the same manner that we classify IT internal controls—general and application specific. General controls are the pervasive factors or control considerations covering IT infrastructure operations such as password security systems or software change management processes. This control type covers all IT operations and is not specific to any one application. Many IT-related risks also can be considered general IT risks. The risk that IT may not be able to continue operations in the event of some massive electrical outage will impact all IT operations and the applications running in that system and its network operations.

  The two unique aspects of this area are the needs for ongoing and real-time monitoring of the risk environment as well as both the needs for technical skills and tools to respond and react. A major area of concerns are the risks surrounding the telecommunications network, including wireless connections, that supports many of today's enterprises. Whether it be an e-mail network necessary for enterprise-wide communications or many applications, all operations should be operating and communicating with one another. Whether a malicious virus or denial of service attack on the network, an internal controls failure of some key application, or just extended delays due to heavy legitimate traffic, these IT networks are exposed to a wide variety of risks. There is a need to monitor these risk events and to respond at once.

  An effective enterprise risk management function needs to establish specialized personnel and tools to monitor and respond to its IT-related risks. Some of these might be assigned to the IT function and its ongoing IT operations, security monitoring, and technical remediation activities. In many respects these activities are part of overall IT service support and service delivery ongoing activities. We do not think of the process of assigning IT network access passwords and monitoring password violations as just a risk-related activity but as a good IT operations management internal control procedure.

- **Alternative Risk Transfer and Facility Related-Risks.** We have discussed that prior to COSO ERM, many enterprises thought of their enterprise risk

> management operations primarily just in terms of insurance coverage and physical asset protection mechanisms. While we now should be thinking of risks on a broader, strategy-setting level, the risk-based concerns about having appropriate insurance coverage or physical perimeter protections still have not gone away. There will continue to be a need to monitor those risk areas and to establish appropriate control processes. The term *risk transfer* is really the process of securing and purchasing insurance. An enterprise may face a risk that it may incur a major facility fire. While there is not a significant chance that there will be a fire, the repair and recovery costs could be very expensive to the enterprise. Rather than setting up a fund to cover any fire losses or just hoping against hope that the enterprise will not have to incur the losses associated with such a major fire, today we usually will transfer that risk to an insurance carrier who offers similar insurance to many others and will bet that while there may be risks of fires at one or another enterprise production plant, they will not incur such losses at all of them. Thus, they can cover the costs of an enterprise's plant fire risk lower than if the enterprise self-insured itself.
>
> In addition to risk transfers through insurance, there are other alternative financial risk transfer mechanisms through the general investment or financial-related products called derivatives. A broad and complex field, financial derivatives are often used as tools to cover or hedge against financial losses. A simple example here is the process of selling a stock or investment "short." If some security seems to be priced quite high today, and the investor feels that it may go down in price soon, the investor can sell that stock short even if the investor does not own the stock today. The investor borrows money for the stock and then sells it at today's high price. Once—and hopefully if—the stock goes down in price, the investor covers the loan of the borrowed stock by buying more stock at the current lower price. The investor must pay interest for the loan on the borrowed stock but can profit on the transaction if all works well.
>
> Although a short sale is not considered to be a true financial derivative, it illustrates the concept of a financial risk protection mechanism. There are many other types of derivative transactions that an enterprise can use to hedge or transfer its financial risks. However, while a CRO and the enterprise risk management function should have some understanding of hedging financial risks through the use of derivatives, the enterprise risk management function should seek specialized financial help if it seeks to structure any financial derivative transactions. Making some very wrong bets or developing a poorly structured derivative transaction could result in massive costs to the enterprise.

There are still a variety of other facility-related or broad risk categories that we have suggested belong in this category of an effective enterprise risk management program. These include but are certainly not limited to:

- Building and Facilities Security. This category can include all security beyond just IT facility and network security and include plant perimeter security controls, employee badges, and many other related matters. Other specialized people in the enterprise typically manage these risks, but the enterprise risk management group both should have a good understanding of them and should monitor risk events in these areas.

- **Legal and Regulatory Risks.** Whether it is litigation actions against the enterprise or new laws being considered by legislative bodies, an enterprise should have a good understanding of the developments and issues in these areas. The CRO or some designated member of the enterprise risk function should maintain close ties with legal counsel or through other sources. In many respects, this area of risk management primarily involves understanding and appropriately communicating risk-related matters to others in the enterprise.

This list could be expanded to other issues as well. The point is that an effective enterprise risk management should install continuous monitoring processes to review, understand, and take appropriate actions on all risks that may impact an enterprise. An enterprise group, reporting to a strong CRO, should be able to introduce effective enterprise risk management programs.

Although we have suggested that one person should be designated as the CRO to manage the enterprise risk management function and that it should consist of three basic functions, we have not suggested the size for such a group. Much will depend on its planned activities, if the enterprise risk group is performing some direct risk assessment reviews, and if they are also helping to install preventive controls in other areas. The size of an enterprise risk management function will often be about the size or slightly smaller than the total internal audit group.

RISK MANAGEMENT REVIEWS AND CORRECTIVE ACTION PRACTICES

The effective enterprise risk management group often operates in a manner very similar to internal auditors. Much of internal audit's work involves monitoring ongoing issues and making recommendations to improve internal controls or acting as internal consultants to management. However, as was discussed in Chapter 3, the enterprise risk management group should identify significant areas in the enterprise with high levels of likelihood of occurrence. These are the risks to the enterprise where there is a high likelihood of the event occurring. In those situations, the risk management function should not just sit back and wait for the risk event to occur. Rather, this is an appropriate time to review the risk area and make some recommendations to lessen the risk and improve surrounding internal controls. Risk management review reports can be a major responsibility of the risk management function.

While not every higher risk area identified will be subject to such a review, the enterprise risk function should borrow some techniques from their internal auditors and perform appropriate assessment reviews of higher risk areas, what we call risk assessment reviews (RARs). These reviews should examine key areas in the enterprise and make recommendations for both improving internal controls and reducing risk likelihoods.

This RAR approach places enterprise risk activities in an almost parallel path with traditional internal audit activities. However, with some advance communication and coordination, these reviews will not compete with internal audit activities but will enhance and support similar internal audit and internal controls–related reviews. We can see how this process works by reviewing the Global Computer Products sample company. As part of an overall discussion covering this area, Exhibit 8.3 identified Global's San Jose receiving and inventory controls process as a significant risk area requiring audit or internal controls review attention. If the enterprise risk management group sees significant exposures in this area and if internal audit has no planned reviews here, the enterprise risk management group should schedule a review of this area.

The RAR assessment is a newer type of review, and the risk management group should develop such a review approach, communicating their review plans and procedures with senior management, internal audit, and the board audit committee.

Risk Assessment Report Characteristics	Internal Audit Report Characteristics
Report Objectives	
Evaluate operational and other risks based on established plan or risk-related events. The report will make suggestions for corrective actions or will report on the progress of remediation efforts.	Evaluate the adequacy of financial, operational or IT internal controls following an internal audit plan approved by the audit committee. The report will make recommendations for improvement as appropriate.
Responsibility for Completing Work	
Enterprise risk management staff with support from IT, internal audit, and other subject management experts.	Internal audit
Review Evaluation Process	
Review of documentation, observations, and test procedures as appropriate.	Review of documentation, observations and test procedures as appropriate.
Standards Governing Reviews	
Currently no professional risk review standards with the exception of ISO 31000 (see Chapter 17).	IIA, International Standards for the Professional Practice of Internal Auditing
Report Final Recipients	
Board risk management committee, if established, or else senior management such as CEO or CFO.	Audit committee of the board
Reporting Process Responsibility	
Chief risk officer (CRO)	Chief audit executive (CAE)
Report Corrective Actions Responsibility	
Risk management reports RAR findings and may review recommendation follow-up status and may become actively involved in implementing corrective actions.	Internal audit reports findings and may review recommendation follow-up status but generally has no responsibility for implementing recommendations.

EXHIBIT 5.8 Risk Assessment Review and Internal Audit Report Comparison

This type of review is not designed to compete with internal audit review activities but to improve the risk environment and enhance internal controls. Exhibit 5.8 shows this comparison between the functions and objectives of this new RAR risk-related review and a traditional internal audit report. A new type of compliance reporting, risk management should review its plans for RAR reports with senior management, internal audit, and more importantly, the audit committee.

The RAR process should proceed in a manner similar to the process of planning, performing, and reporting the results of internal audits.[3] The key difference here is that the RAR reviewers would emphasize a wide range of identified risks in the area selected and then would suggest approaches to eliminate or minimize these risks. Although there can be many variations due to the nature of the initially identified risks, the enterprise risk reviewers should form a standard set of review steps to review the identified area. Exhibit 5.9 shows the risk review steps that might be used to review risks embedded in the Global Computer Products San Jose receiving and inventory controls area.

This example might better explain the RAR review process with references to the Chapter 1 Global Computer Products example and the related discussion of its potential risks in the area of San Jose operations receiving and inventory controls. Given this hypothetical risk situation, assume that the enterprise risk management team has

The following outlines the steps necessary to perform a risk assessment review (RAR) in compliance with the COSO ERM framework:

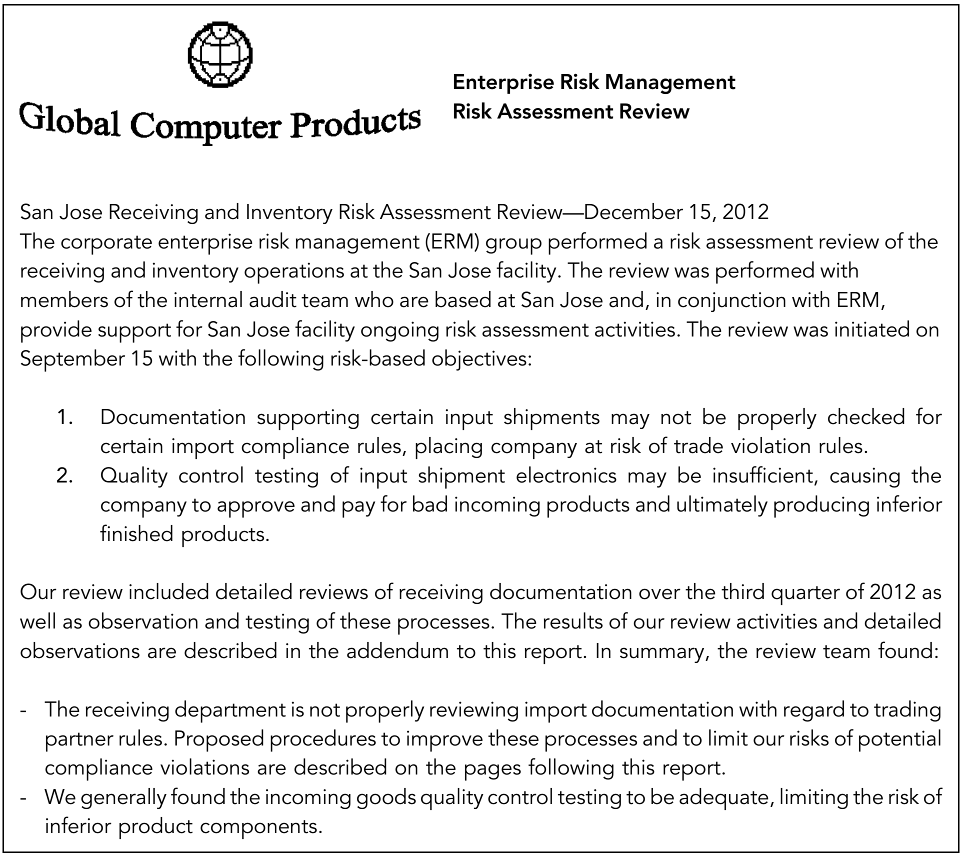
1. Schedule review based on long-range risk assessment plans, management request, or unanticipated risk event.
2. Develop preliminary objectives for the RAR:
   a. Review current risk status for management reporting.
   b. Risk-related assessment in conjunction with internal audit or other group.
   c. Perceived enterprise risk exposure in area to be reviewed.
3. Review supporting data to gain understanding nature of risk, its severity, occurrence probability, and alternatives for risk mitigation.
   a. Review supporting data or perform tests of data to better understand the nature of deviations or further risks of occurrence.
   b. Reconcile results of reviews with preliminary risk assessment objectives.
4. Develop cost-based alternative risk mitigation strategies, such as risk substitution or risk acceptance.
   a. Review mitigation strategies with responsible management to assess feasibilities.
   b. Develop best approaches for risk mitigation.
   c. When practicable, test proposed mitigation strategies.
5. Develop exit strategy for RAR.
   a. Recommendations for immediate corrective action to be performed by operating unit.
   b. Corrective actions to be performed through a planned scheduled project.
   c. Corrective remediation performed by the ERM team.
   d. Documented avoidance of risk.
6. Publish RAR with copies to responsible management, the risk committee, and a request for RAR wrap-up actions at a designated date.

EXHIBIT 5.9 RAR Sample Review Guidance

decided to implement an RAR process in this area. Risk management would perform a review similar to an internal audit review and should develop what internal auditors call a program of set procedures to perform the review. This type of review guidance can be developed through discussions with internal audit on how they would perform reviews in this area as well as on the enterprise risk management group's knowledge of the special concerns in this area.

As a result of such a review, the enterprise risk management group would prepare and release this type of RAR report. Such a report is similar to an internal audit report that includes audit findings and recommendations. Exhibit 5.10 shows a sample of an RAR report for this example area of San Jose operations. The idea here is that an enterprise risk management should operate in a manner similar to an internal audit function but should concentrate their reviews on significant enterprise risks. This type of exercise should not compete with internal audit but should enhance an enterprise's review and understanding of significant risks.

Launching these RAR exercises will require some coordination with senior management, internal audit, its audit committee, and others. This should not be viewed as



Global Computer Products

Enterprise Risk Management
Risk Assessment Review

San Jose Receiving and Inventory Risk Assessment Review—December 15, 2012
The corporate enterprise risk management (ERM) group performed a risk assessment review of the receiving and inventory operations at the San Jose facility. The review was performed with members of the internal audit team who are based at San Jose and, in conjunction with ERM, provide support for San Jose facility ongoing risk assessment activities. The review was initiated on September 15 with the following risk-based objectives:

1. Documentation supporting certain input shipments may not be properly checked for certain import compliance rules, placing company at risk of trade violation rules.
2. Quality control testing of input shipment electronics may be insufficient, causing the company to approve and pay for bad incoming products and ultimately producing inferior finished products.

Our review included detailed reviews of receiving documentation over the third quarter of 2012 as well as observation and testing of these processes. The results of our review activities and detailed observations are described in the addendum to this report. In summary, the review team found:

- The receiving department is not properly reviewing import documentation with regard to trading partner rules. Proposed procedures to improve these processes and to limit our risks of potential compliance violations are described on the pages following this report.
- We generally found the incoming goods quality control testing to be adequate, limiting the risk of inferior product components.

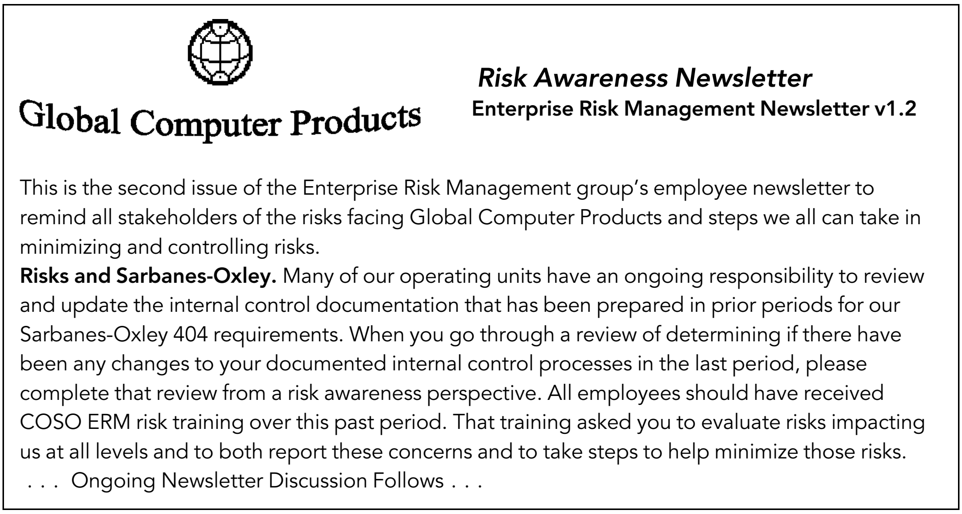
EXHIBIT 5.10 Sample RAR Report: San Jose Receiving and Inventory

competition or a distraction from internal audit's efforts but a special and unique set of reviews concentrating on significant enterprise risks. The concept of RAR reports is a somewhat new and different activity for risk management groups but represents an area that will promote the effective implementation of COSO ERM.

ERM COMMUNICATIONS APPROACHES

While an effective enterprise risk management function will perform many behind the scenes protective functions for an enterprise, strong communication procedures are essential for the function's success. Beyond the regular communications of an enterprise risk specialist talking with IT regarding some suggested risk actions or the CRO communicating with the enterprise general counsel regarding the status of some litigation action, the enterprise risk management function should communicate its concerns and activities to appropriate levels throughout the overall enterprise. These communications should include making senior management and the board aware of enterprise risk concerns, describing the enterprise risk review process through a series of RAR reviews, and awareness on overall enterprise risks. These areas of concern include the following:

- **Board or Senior Management Risk Concerns.** Board of director audit committees should be aware of the importance of internal audit, and how SOx with its legislative requirements has emphasized things. Because of their history as the insurance department or a similar lower level function, enterprise risk management often has not yet had that level of attention from corporate boards. This will change! As discussed in Chapter 13, boards of directors have become increasingly aware of enterprise risk concerns as defined in COSO ERM. An enterprise CEO should introduce the CRO to the board with arrangements established for regular reports to the board on higher risk areas in the enterprise.
- **RAR Reporting Processes.** We have introduced and discussed the RAR reporting process. While similar to traditional internal audit reports, these RARs focus on enterprise risk concerns in limited but specialized areas. They will almost always contain recommendations to improve the risk environment in some area. However, they will sometimes be an account of an area where the enterprise risk group has identified the risk area and assisted in installing processes to eliminate the risk concern.
- **Enterprise Risk Awareness Programs.** An effective enterprise risk management group should develop communication processes to make all members of the enterprise aware of an enterprise's risk management approach. This may be as simple as a newsletter, but it should provide some information on the current risk environment as well as some guidance for employee decision making in this area. As has been discussed in previous chapters, every enterprise should somewhat define its appetite for risk. A newsletter or other communication can help deliver that message through the enterprise. Again using our Global Computer Products



Global Computer Products

Risk Awareness Newsletter

Enterprise Risk Management Newsletter v1.2

This is the second issue of the Enterprise Risk Management group's employee newsletter to remind all stakeholders of the risks facing Global Computer Products and steps we all can take in minimizing and controlling risks.

Risks and Sarbanes-Oxley. Many of our operating units have an ongoing responsibility to review and update the internal control documentation that has been prepared in prior periods for our Sarbanes-Oxley 404 requirements. When you go through a review of determining if there have been any changes to your documented internal control processes in the last period, please complete that review from a risk awareness perspective. All employees should have received COSO ERM risk training over this past period. That training asked you to evaluate risks impacting us at all levels and to both report these concerns and to take steps to help minimize those risks.

. . . Ongoing Newsletter Discussion Follows . . .

EXHIBIT 5.11 Risk Awareness Newsletter Example

company, Exhibit 5.11 is an example of an enterprise-wide risk awareness communication. More information on ERM communication and education programs is discussed in Chapter 17 on establishing an effective culture throughout the enterprise.

CRO AND AN EFFECTIVE ENTERPRISE RISK MANAGEMENT FUNCTION

Both the position of CRO and a formal enterprise risk management function are new to many enterprises today. However, to implement this very important function of COSO ERM, an enterprise should establish both of these concepts. An effective enterprise risk management group will improve the overall enterprise controls environment and will improve many of the procedures for an effective GRC culture as discussed in other chapters. While the enterprise risk function can operate similar to an internal audit function with its own RAR reviews, it is important to remember that the CRO and the designated risk management function have some overall responsibility for the overall COSO ERM framework as described in Exhibit 4.1. That three-dimensional framework included eight levels of risk management such as risk assessments and control activities in one dimension with considerations given to all levels of the enterprise in a second dimension. The third dimension of this framework covered the compliance, reporting, operations, and strategic elements of risk management, covering the other two dimensions or perspectives.

Will a single CRO or even a relatively small enterprise risk management group be able to effectively manage all aspects of such a complex ERM framework as part of an overall GRC approach? This is not a job that can be handled by just one person or group.

Effective team and responsibility structures and linkages must be built. The CEO of an enterprise is certainly not responsible for every activity that takes place on a day-to-day basis, but should have control and reporting procedures in place to make certain the overall processes are performed as defined and that problems are communicated at appropriate levels, with that CEO and the board having final responsibility in the sense of ‘‘the buck stops here.’’

The CRO and the ERM function should have broad oversight responsibilities in monitoring and establishing processes to manage the overall enterprise risk management function. This will require considerable communication and education such that staff at all levels can be better aware of the risks surrounding their areas of activities and can accept or reject those risks with a risk appetite that is consistent with overall enterprise high-level guidelines.

This chapter has described an enterprise risk management function—following the COSO ERM framework—that is a key element of GRC processes and is a somewhat new function to many enterprises today. The function is closer to internal audit than the traditional risk-related insurance functions, but it cannot be just another responsibility of an internal audit group. An effective enterprise risk management function led by a strong CRO with high-level reporting responsibilities will become an important component in many major enterprise organizations going forward.

NOTES

1. For a good general overview of internal auditing, see Robert Moeller, *Brink's Modern Internal Auditing,* 7th ed., Hoboken, NJ: John Wiley & Sons, 2009.
2. Ibid.
3. Ibid.