CHAPTER TWO

# Importance of Governance, Risk, and Compliance Principles

ENTERPRISE ORGANIZATIONS AND CORPORATIONS, in particular, have faced governance issues since their earliest days. Someone or some group was in charge and took a lead in setting the rules for employees and other stakeholders to follow. While this worked with smaller single proprietorships or in the tightly centralized corporations of eras past, today's larger and often multiunit enterprises need broad-based units or functions for setting rules and procedures—they need efficient and effective governance processes.

Life would be easier for those same enterprises if they just had to rely on a central leadership to set those governance rules. However, enterprises today of any location or size are faced with ever increasing sets of rules and procedures ranging from local police and public safety ordinances to national and sometimes international laws and on to broad professional rules and standards. On a whole series of levels, an enterprise must comply with these laws and regulations. Failure to do so can result in a variety of penalties, and an enterprise needs processes to ensure that they are operating in compliance with the appropriate laws and regulations.

An enterprise always faces risks that it will be found in violation of one or another of these multiple laws and regulations. There are also risks that their own established governance rules will not achieve their desired results or that they may face some outside event beyond their control, such as a major weather event or a fire in a major facility. There is a need to manage these risks at an overall enterprise level.

While enterprises have always been concerned with various governance, risk, and compliance issues, the introduction of COSO ERM, or enterprise risk management, the major theme of this book, has brought all three of these governance, risk, and compliance concerns together into what has been called GRC principles. While other

chapters following discuss such issues as the importance of enterprise governance practices, risk management fundamentals, and corporate governance practices, this chapter looks at the importance of establishing a strong set or program of enterprise GRC principles, important tools for enterprise management.

## ROAD TO EFFECTIVE GRC PRINCIPLES

Business professionals did not even hear about the now increasingly familiar acronym GRC until a few years after SOx. As mentioned in the introduction to this chapter, the G stands for governance. In short, this means taking care of business, making sure that things are done according to an enterprise's standards, regulations, and board of directors' decisions. It also means setting forth clear stakeholder expectations of what should be done so that everyone is on the same page with regard to how the enterprise is run. The R is risk. Everything we do involves some element of risk. When it comes to running across freeways or playing with matches, it's pretty clear that certain risks are just not to be taken. When it comes to business, however, risk becomes a way to help both protect existing asset value and create value by strategically expanding an enterprise or adding new products and services. The concept of risk is even more important than just the COSO ERM we will be exploring in greater detail in the chapters to follow.

The C represents compliance with the many laws and rules affecting businesses and citizens today. Sometimes, people will also extend that C to include controls, meaning that it is important to put certain controls in place to ensure that compliance is happening. This might mean monitoring a factory's emissions or ensuring that its import and export papers are in order. Or it might just mean establishing effective internal accounting controls, and effectively implementing legislative requirements such as the Sarbanes-Oxley (SOx) rules discussed in Chapter 9 of this book. Put all together, GRC is not just what you have to do to take care of an enterprise, but a paradigm to help grow that enterprise in the best possible way.

As we stated in our introductory paragraphs, all enterprises, and corporations in particular, historically do not think of GRC as a combined set of principles. As much as an enterprise managed or cared about any of these areas, they were often managed as separate areas or concerns. Risk management is a classic case here. Enterprises thought of risk management in terms of insurance coverage and often managed their risks through an insurance department that had little to do with other enterprise operations. Similarly, we always had a need to comply with all levels of established rules, including the rules that were established to help govern the enterprise, but we have not historically combined them to form GRC concepts. Governance, risk, and compliance, or GRC, is an increasingly recognized term that reflects a new way in which enterprises today are adopting an integrated approach to these aspects of their businesses.

Going beyond just the acronym GRC, it is important to remember these represent core disciplines of governance, risk management, and compliance. Each of the disciplines consists of the four basic GRC components: strategy, processes, technology, and people.

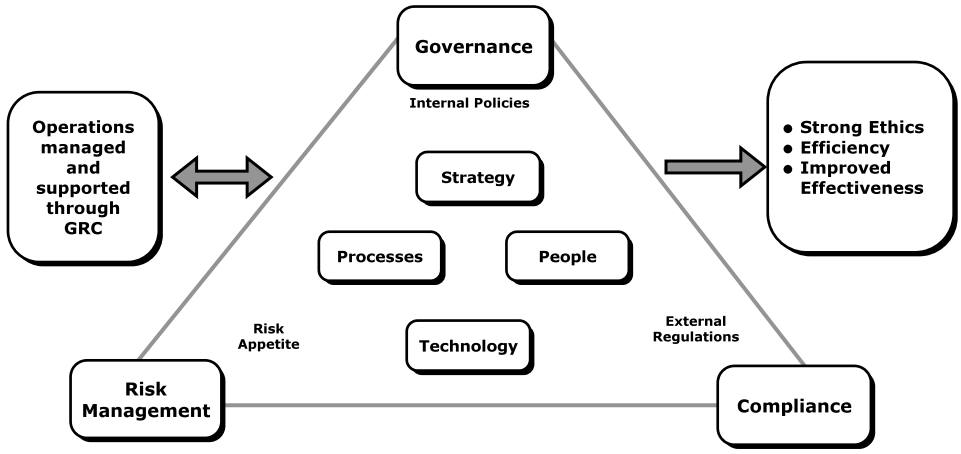


**EXHIBIT 2.1** GRC Concepts

Exhibit 2.1 illustrates this GRC concept. Governance, risk management, and compliance principles are tightly bound to tie these principles together. The diagram also shows that internal policies are the key factors supporting governance, that external regulations drive compliance principles, and that an enterprise's risk appetite is a key element of risk management. Within this triangle, we have the components of strategy, effective processes, technologies, including IT, and the people in the enterprise to make all of this work. Off to the left side, the exhibit shows that an enterprise requires management attention and support, and correct ethical behavior, organizational efficiency, and improved effectiveness are keys. The sections following will discuss each of the GRC components further and indicate where they are discussed in other chapters.

## IMPORTANCE OF GRC GOVERNANCE

The three GRC principles should be thought of in terms of one continuous and interconnecting flow of concepts and with neither G, R, or C more important or significant than the others. While the preponderance of the chapters to follow cover risk management and COSO ERM, we start our GRC discussion here with governance. *Corporate* or *enterprise governance* is a term that refers broadly to the rules, processes, or laws by which businesses are operated, regulated, and controlled. The term can refer to internal factors defined by the officers, stockholders, or the charter and basic objectives of a corporation, as well as to external forces such as consumer groups, clients, and government regulations.

Moving down from senior corporate levels and into enterprise operations, we can define enterprise governance as the responsibilities and practices exercised by the board, executive management, and all levels of functional management with the goals of

providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly. Governance really refers to the process of establishing rules and procedures within all levels of an enterprise, communicating those rules to appropriate levels of stakeholders, monitoring performance against those rules, and administering rewards and punishments based on the relative performance or compliance with those rules.

A well-defined and enforced set of corporate governance principles provides a structure that, at least in theory, works for the benefit of everyone concerned by ensuring that the enterprise adheres to accepted ethical standards and best practices as well as to formal laws. In recent years, corporate governance has received increased attention because of high-profile scandals involving abuse of corporate power and, in some cases, alleged criminal activity by corporate officers. An integral part of an effective corporate governance regime includes provisions for civil or criminal prosecution of individuals who conduct unethical or illegal acts in the name of the enterprise.

Although it is difficult to describe all of the concepts of corporate or enterprise governance in a few short paragraphs or a single picture, Exhibit 2.2 shows enterprise governance concepts with an executive group in the center and their interlocking and


**EXHIBIT 2.2** GRC Governance Concepts

related responsibilities for establishing controls, a strategic framework, performance, and accountability. Governance, a key portion of GRC principles, is embedded in many of the chapters going forward but in particular in Chapter 6 on effective enterprise governance practices and Chapter 10 on governance and risk portfolio management.

## RISK MANAGEMENT COMPONENT OF GRC

The major objective of this book is to introduce and describe the importance of the COSO enterprise risk management (ERM) framework and to describe how COSO ERM is a key component of enterprise GRC principles. Chapter 3 discusses risk management fundamentals in greater detail, but risk management should be part of the overall enterprise culture from the board of directors and very senior officers down through the enterprise. The chapters following emphasize that there are four interconnected steps in effective GRC processes and in enterprise risk management as shown in Exhibit 2.3 and as follows:

1. **Risk assessment and planning.** An enterprise faces all levels of risks, whether global issues based on weather or currency threats to weather-related threats at local operations. We cannot plan or identify every type of risk that might impact an enterprise, but there should be an ongoing analysis of these various potential risks that may face an enterprise. These matters are discussed in Chapter 3.
2. **Risk identification and analysis.** Rather than just planning for the possibility of some risk event occurring, there is a need for a more detailed analysis on the likelihood of these risks coming to fruition as well as their potential impacts. There is a need to quantify the impacts of the identified risks and to determine mitigation strategies in the event the risk event occurs. Mitigation refers to assessing the best way to manage or eliminate an identified risk. The final factors associated with these

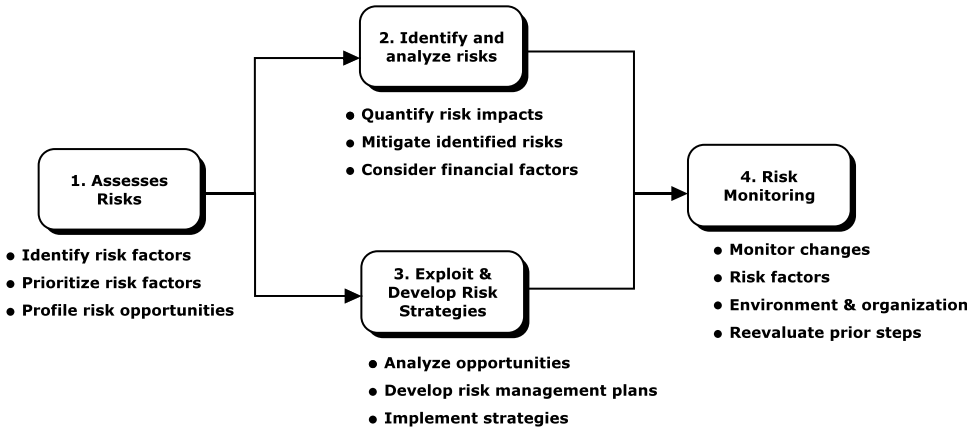


**EXHIBIT 2.3** GRC Risk Management Processes

risks should also be identified. An identified risk will be much more significant if we can identify the total costs to the enterprise if the identified risk occurs.

3. **Exploit and develop risk response strategies.** Essentially a concept that should be considered in parallel with risk identification, an enterprise should develop plans and strategies to return to normal operations and then recover from the risk event. This may include an analysis of risk-related opportunities. That is, if there is an identified risk that some older production equipment may fail, an opportunity may be to abandon that production line and install new equipment following a newer technology and possibly even at a newer, more friendly location.
4. **Risk monitoring.** Tools and facilities should be in place to monitor for the identified risks possibly occurring. A smoke detector fire alarm is an example here, although most risk-related monitoring requires a wide series of special reports, established and measurable standards, and a diligent human resources function. The idea is to keep ahead and to reenter these prior risk management steps as necessary.

Risk management should create value and be an integral part of organizational processes. It should be part of decision-making processes and be tailored in a systematic and structured manner to explicitly address the uncertainties an enterprise faces based on the best available information. In addition, risk management processes should be dynamic, iterative, and responsive to change with the capabilities of continual improvements and enhancements. The COSO ERM–related chapters following look at many other aspects of risk management, a very important part of GRC principles.

## GRC AND ENTERPRISE COMPLIANCE

Compliance is the process of adhering to a set of guidelines or rules established by government agencies, standards groups, or internal corporate policies. Adhering to these compliance-related requirements is a challenge for an enterprise because of the following issues:

- **The frequent introduction of new regulations.** Using the United States as an example, a wide swath of agencies, such as the Environmental Protection Agency (EPA), regularly issue new rules that may have wide impacts on many enterprises, despite their prime business purposes. Companies have a challenge to monitor these rules and determine which apply to them.
- **Vaguely written regulations that require interpretation.** Again using the United States as an example, in 2010 Congress passed a massive health care reorganization bill, which was printed on many thousands of pages, covering issues and rules that the legislators who passed the bill never even read, let alone understood. Even today, we are still looking at these rules and interpreting what they mean. Compliance with those types of rules can be difficult.

- **No consensus on best practices used for compliance.** Rules are filled with regulations stating such things as ''All transactions must be supported by a receipt.'' Does such a rule require receipts for transactions less than $1.00, less than $25.00, or some other value? There are often no guidelines here and everyone seems to have their own interpretations.
- **Multiple regulations often overlap.** U.S. states and local governmental units from different geographies may issue rules that cover similar areas but may have different requirements. These differences will be eventually resolved in court, but compliance until matters are resolved can be a challenge.
- **Constantly changing regulations.** Regulatory agencies in particular are often constantly changing or reinterpreting their rules, making strict compliance a challenge.

Therefore, compliance becomes a continuous process, not a one-time project, and continues to drive business agendas as organizations are being held accountable for meeting the myriad of mandates specific to their vertical markets.

In addition, enterprises might also be required to address cross-industry legislation, such as Sarbanes-Oxley (SOx), discussed in Chapter 9, and other internal control processes, such as ISO 9000 or Six Sigma. Simply stated, the breadth and complexity of these laws and regulations has caused challenges for many enterprises over the years. Enterprises need to approach their GRC compliance principles from a more strategic perspective that could help them move beyond simply meeting individual compliance mandates to realizing tangible business benefits from their infrastructure investments as a whole.

The scope of compliance also permeates other aspects of an enterprise. Exhibit 2.4 illustrates some issues an enterprise should consider as it attempts to establish its scope and approach to compliance. A consistent approach on the use of compliance-driven capabilities and supporting technologies across an enterprise can provide these potential benefits:

- **Reduced total cost of ownership.** Investments can be leveraged across multiple regulations. For example, many regulations specify document retention requirements, which can be met by a single investment in a content and records management system.
- **Flexibility.** One of the difficulties with compliance is that new regulations are introduced and existing regulations are changed on a frequent basis. By centrally managing compliance initiatives via organization-wide compliance architecture, an enterprise can quickly adapt to these changes.
- **Competitive advantage.** A broad and consistent compliance architecture can allow an enterprise to better understand and control their business processes, which allows them to respond more quickly and accurately to external or internal pressures. Furthermore, certain regulations may contain tangible business benefits through reduced minimum capital requirements, which could be enabled by an enterprise-wide compliance architecture.

| Scope of Compliance | Area for Considerations |
|---|---|
| Strategy | ■ As an organization develops its strategy, it must determine which regulations are relevant.<br>■ Compliance sustainability needs to be an integral part of any compliance strategy. |
| Organization | ■ The organizational structure must be established to meet the specific requirements (or intent) of each regulation (e.g., Sarbanes-Oxley recommends the Chief Executive Officer and President be two different people). |
| Processes | ■ Key processes must be documented and practiced.<br>■ Audits or reviews must take place to ensure documented processes are effectively being used to address compliance/regulation requirements. |
| Applications and data | ■ Applications must be designed, implemented and continuously tested to support the requirements of each regulation.<br>■ Data must be properly protected and handled according to each regulation. |
| Facilities | ■ Facilities must be designed and available to meet the needs of each regulation (i.e., some regulations may require records to be readily available at an off-site location). |

**EXHIBIT 2.4** Scope of Compliance Architectures Considerations

Effective GRC compliance processes help an enterprise to transform their business operations and gain deeper insight and predictability from their business processes as they address regulatory-driven requirements. Key business drivers here include the ability to better manage information assets, demonstrate compliance with regulatory and legal obligations, reduce the risk of litigation, reduce cost of storage and discovery, and demonstrate corporate accountability.

## IMPORTANCE OF EFFECTIVE GRC PRACTICES AND PRINCIPLES

In addition to effective risk management and COSO ERM processes, an enterprise needs to adopt strong governance and compliance processes as well, with the objective of establishing an effective GRC program. While many of the chapters going forward focus on COSO ERM and the key elements of an effective risk management program, we should not forget the importance of strong risk and governance processes. GRC practices and principles will be folded into all of the following chapters, with several devoted to specific risk and governance issues.

Chapter 6 discusses the importance of effective governance practices. It discusses roles and responsibilities for the people and functions needed for effective governance

and outlines approaches for communicating various levels of governance rules. Similarly, Chapter 7 looks at compliance issues for today's enterprise. The chapter outlines a framework approach for an enterprise to identify its most significant compliance issues, to communicate those compliance rules, and then to monitor its actual compliance performance. The chapter discusses how legal and internal audits can help it to achieve compliance.

While enterprise risk management and COSO ERM are very important to an enterprise, strong programs of governance and compliance are important as well. An enterprise should focus many of its activities on following strong GRC principles.