CHAPTER ONE

1 What Is GRC, and Why Does It Matter?

IF YOU'VE SEEN THE movie *A Few Good Men*, starring Jack Nicholson, Tom Cruise, Demi Moore, and Kevin Bacon, you'll likely remember the courtroom scene where Bacon's character asks a witness if a military manual includes the term "code red." He receives the desired reply: "No, sir," indicating that a code red—a punishment allegedly used on a soldier—doesn't exist. But Cruise's character counters by asking where the manual provides the location of the mess hall or other realities of military life, also receiving the desired response: "Well, Lieutenant Kaffee, that's not in the book either, sir." Cruise successfully makes the point that although there's no specific, tangible place to look for a code red, this does not mean that a code red doesn't exist.

Why this diversion to Hollywood? The same applies to the term *governance, risk management, and compliance*. You've probably never seen any company with a unit or function called governance, risk management, and compliance, or GRC for short. But certainly that doesn't mean GRC doesn't exist.

Indeed, it does exist and has tremendous impact on a company's ability to succeed. It may sound extraordinarily boring, conjuring up thoughts of insignificant plumbing deep in the recesses of an organization. But that's just not

the case. GRC, in fact, is extremely important to every company, influencing virtually everything done from strategy formulation and implementation to every kind of operational decision.

WHAT IS GRC?

Few of us have the patience for dealing with technical definitions, so if you'd rather skip to the next section, no problem. But if you've heard about GRC[1] and would like a better a sense of its genesis and what it is, read on.

Some months ago I spoke at a conference where the moderator turned to me saying, "GRC is an acronym used by many people, but with many different meanings—what does it mean to you?" Here's my response.

GRC originated in the management consulting world several years ago. Technology firms and others quickly picked it up and used it to describe available services and software solutions. And while sometimes the term is used by compliance officers, risk officers, or internal auditors, it is rarely used by line executives or board members.

As for what it means, GRC is a combination of related although somewhat disparate concepts. The term *governance* traditionally has been used in the context of a company's board of directors. A definition of governance I particularly like is: *the allocation of power among the board, management, and shareholders.* But today the term is used also to encompass an array of actions taken by management in running a company, from senior levels down throughout the management ranks.

The R is for *risk management*. This term is used in many different ways, from a simple risk assessment to a full-blown enterprise risk management process. The C stands for *compliance*, initially meaning adherence to applicable laws and regulations, though many users now include adherence to internal company policies as well.

I refer to these pieces as "disparate" because GRC isn't really one end-to-end process that companies employ. While the elements of GRC relate to a company's strategic and other business objectives, they also pertain to activities and processes at different levels of an organization. Indeed, there's significant overlap, in that risk management can and should be designed to address compliance as well as other categories of a company's objectives.

Okay, leaving terminology for now, let's look at why GRC is truly relevant.

WHY GRC MATTERS

As you look over the following chapters, you should get a good sense of exactly why GRC matters to every organization. Let it suffice here to highlight a few key points.

A critical element of GRC is a company's culture, including the oft-used term *tone at the top*. Inherent in culture is the extent to which a company and its people embrace integrity and ethical values. Why is this important, especially so in today's environment? Because companies operating from a base of integrity and ethics not only stay out of trouble, they build on that foundation to drive success. Such companies attract the best people to their organizations, as well as the most desirable customers, suppliers, financiers, and business partners. And the opposite is also the case.

No, we've not seen empirical evidence put forth in academic studies, but we do see anecdotal evidence. Take Johnson & Johnson, for example. Back in the 1980s when the Tylenol scandal hit, J&J's culture of integrity and ethics drove a quick decision—to pull every last unit of Tylenol off drugstore shelves. The action was costly, but it positioned the company extremely well in the consumer marketplace, providing tangible dividends for decades to come. But the recent travails of J&J have been quite different. When Tylenol, Motrin, and other products of its McNeil Consumer Healthcare Products unit were found to make people sick, the company was accused of failing to report and investigate the matter, and its reputation has taken a hit.

Another company suffering charges of not doing the right thing is Toyota, which has had numerous recalls due to vehicle safety issues and allegations of failing to inform regulators. Toyota has lost market share to competitors, and we can surmise that while some customers simply are concerned about safety, others have stayed away due to anger at the company's failure to be forthcoming in reporting the dangers.

In the Preface to this book I mentioned Arthur Andersen; that firm represents another good illustration of how integrity and ethical values are perceived in the marketplace. Andersen did not implode from doing a bad audit of Enron, an allegation that was never proven in court. Rather it was brought down because of a Department of Justice indictment on alleged illegal destruction of evidence—the famous destruction of documents related to its Enron audit. After the DOJ action, Andersen's clients no longer wanted to be associated with the firm. There also were concerns about whether the firm would be around to complete critical audits, and key personnel saw what they

perceived to be the handwriting on the wall and left to join other firms. But the problem began with an unethical—not illegal, as the U.S. Supreme Court ultimately decided—lapse in judgment.

In the coming chapters we look more closely at how and why these and other companies suffered while others continued to succeed. I think you'll find what's coming easy to digest. Although you might not be intimately familiar with GRC—if you were, you probably wouldn't have picked up this book—you will recognize key elements. And of course this isn't rocket science. I've no doubt you'll find what's in the coming chapters not only relevant but easily understood and readily implementable.

NOTE

1. In some circles, GRC stands for governance, risk, and compliance, leaving out management for brevity.