Executive Summary

This book argues that evaluating the corporate culture is an internal audit best practice and gives practical examples of how this can be done. To make the case that evaluating the corporate culture is a best practice, we need only look at the long history of major business frauds and failures. Root cause analysis leads inevitably to the culture of the organization. At the time of this writing we have a macro-level example — the global financial meltdown caused by the “culture of greed” on Wall Street.

Internal auditing’s stakeholders want assurance that their organization will not be the next highly publicized failure. To give them that assurance, the potential causes of such failures must be identified: weaknesses in the corporate culture.

But how can internal auditors evaluate something as vast and intangible as the culture? The short answer is that we cannot evaluate the culture as a whole, but we can evaluate specific elements of the culture. Throughout this book the term “soft controls” is used to refer to the informal, intangible levers of control such as tone at the top, the organization’s ethical climate, and management’s philosophy and operating style that together make up the corporate culture.

Evaluating soft controls, which are inherently subjective, and reporting weaknesses to those accountable is perhaps the greatest challenge internal auditors have ever faced. Traditional auditors believe we cannot and should not try to do this, but best practice audit departments like those featured in this book have found ways to do so.

The Institute of Internal Auditors’ (IIA’s) International Standards for the Professional Practice of Internal Auditing (Standards), in fact, points to the need to evaluate soft controls. If we are to “evaluate and improve the effectiveness of risk management, control, and governance processes (italics added),” we need to determine whether these processes are having the desired effect. For example, governance processes include the dissemination of ethics policies. To be effective, such policies must be understood, accepted, and acted upon by employees. That is, they must be integrated into the culture of the organization.

A specific example of ineffective ethics policies is worth mentioning here. Enron is the company whose failure in 2001 kicked off a wave of public scandals and led to the U.S. Sarbanes-Oxley Act of 2002 and similar regulations in other countries. This company’s formal governance structure and practices were a model of excellence, but the informal communications and behavior of management created a culture that was almost diametrically opposed to the stated values. A good internal audit department (Enron had outsourced theirs to Arthur Andersen) focused on evaluating soft controls could have identified the gap between the stated and real corporate values.

Objective and Central Findings of This Study

This research report began as an update to the author’s 1997 study, Control Model Implementation: Best Practices. That book was part of the vibrant control self-assessment (CSA) movement of the 1990s, which was fostered in large part by the first Committee of Sponsoring

The COSO framework, which has become the globally accepted criteria for evaluating internal control, emphasized the central importance of soft controls, especially the control environment. In the early 1990s the only well-known technique for evaluating soft controls was the CSA workshop. In fact, many people still equate the term CSA with the workshop technique. *Control Model Implementation* showed that other techniques were beginning to emerge. These techniques included surveys, structured interviews, and risk-based audit approaches that identify both hard and soft controls.

Current research suggests that soft control evaluation has evolved further from CSA workshops toward simpler survey and interview techniques, and is being integrated into the fabric of audit departments’ routine audit work. I believe this evolution reflects the improved image and credibility of internal auditing. Auditors no longer need a dramatically innovative technique — in which they carefully avoid expressing their own opinions — to surface soft control issues. The best audit departments are accepted as business partners whose opinion is listened to rather than fought against. This does not mean that they can venture baseless opinions, but it does mean that when they have solid evidence, even if some subjectivity is involved, they are taken seriously.

I should add that CSA workshops have not disappeared from the internal auditor’s tool bag completely. Five of the 19 audit departments presented in this book use workshops. Two do so selectively, when a particular situation calls for it. Two do so in combination with interviews and surveys. One used workshops with executives for an entitywide review. In general, though, workshops have evolved from an internal audit tool into a central technique in enterprise risk management (ERM) programs.

**Use of the Term “Best Practices”**

The term “best practice” is commonly used and easily misunderstood. Taken literally, it implies there is only one “best” way of doing something. Identifying the single best way would require defined criteria and some sort of contest. This is not, of course, how the term is used. In common usage, “best practices” are techniques that consistently produce better results than others and are benchmarks to strive for.

I believe that evaluating soft controls is a best practice. Consider the following hierarchy of audit techniques and findings:

- At the lowest level are techniques that only identify errors.
- At the next level are techniques that identify the control weakness that can lead to the errors.
- At the highest level are techniques that identify the root cause of the control weakness.

Another obvious hierarchy is the significance of the findings, ranging from minor errors to business failure. As stated before, root cause analysis often leads to weaknesses in soft controls, and this is especially true when major risks such as business failure are examined.
No practice is best for everyone and in every situation. Everything internal auditing does, and especially soft control evaluation, must be done in the “best” way for the particular organization it serves.

The evaluation technique must fit the size, environment, industry, and culture of the organization, and it must also be useable by the audit staff.

This book presents soft control evaluation techniques from a variety of organizations. All have proven effective in their environment. Hopefully, readers will gain insight into how to tailor a technique to their own organization by seeing how similar results are achieved in different organizations. Chapter 3, for example, shows how soft control evaluation is integrated into routine audits in two small audit shops and a very large audit shop. Allina and Securian (10 and 14 auditors respectively) succeed informally, by hiring auditors with business savvy and providing hands-on leadership. ING, with 700 auditors spread across the world, had to develop a sophisticated formal process to get similar results.

Summary of the Chapters

Chapter 1, “Introduction to Soft Controls,” elaborates on what I said above about the nature of soft controls and why internal auditors need to evaluate them. It also provides some basic principles that should be followed regardless of the specific technique used. It provides a brief overview of the first COSO report, because several of the techniques presented in this book use its terminology and structure. It ends with several pages of specific soft controls. These may be helpful in providing content for the reader’s development or enhancement of soft control evaluation techniques.

So far I have talked about soft controls as making up the corporate culture, which is an entitywide issue. But managers create subcultures with their own areas. When a subculture is dysfunctional in some way (i.e., has a soft control weakness), a host of problems can arise. Surveys can be a simple way to measure elements of the subculture and identify dysfunctions. Chapter 2, “Surveys Used during Audit Projects,” shows how four audit departments and one internal consultant use surveys to evaluate soft controls while reviewing a specific area or process. Their circumstances and method of application vary widely. The surveys also vary and are included as exhibits. The chapter concludes with guidelines for developing and applying similar surveys.

Chapter 3, “Participative, Risk-based Audit Projects,” shows how four audit departments integrate soft control evaluation into their everyday audit work. As mentioned above, two are small and one is very large, and their approach varies accordingly. The fourth is an audit department whose participative, risk-based approach became the basis for the organization’s ERM program. The chapter ends with guidelines for evaluating soft controls during audit projects, including techniques for effective soft control interviews.

Chapter 4, “Structured Entity-level Interviews,” shows how four audit departments evaluate entity-wide soft controls through structured interviews at various organizational levels. It concludes with guidelines for entity-level interviews that augment the interview guidelines in Chapter 3.

Chapter 5, “Entitywide Surveys,” presents six approaches to evaluating entity-level soft controls with surveys. Ameritech’s is a “classic” example that has been used as a model by many other
organizations. United Stationers’ is a direct descendant, but its value has been lessened by a human resources (HR) survey that covers much of the same ground. BP shows how an audit department can use the results of an HR-administered survey. The City of Austin shows how internal auditing can enhance an existing HR-administered survey. Lennox International shows how a survey developed by internal auditing can be transferred to another function. And Robeco shows a highly disciplined approach to developing a survey to fit a specific organization. The chapter ends with guidelines for developing and using an entitywide soft control survey.

Chapter 6, “Combination of Techniques,” profiles three audit departments that used a combination of surveys, interviews, and workshops. One does so for audit projects and one for entitywide reviews. The third has an integrated, COSO-based approach from entity-level risk assessment through audit execution. There are no guidelines in this chapter because the relevant guidelines were presented in previous chapters.

Chapter 7, “Soft Control Audit Report Comments,” discusses the challenges involved in disclosing soft control weaknesses in written audit reports. It presents three complete audit reports and 14 excerpts that address soft control weaknesses. It also references three audit reports included in previous chapters. Together, these report comments represent six audit departments with six different approaches. None are likely to be perfect models for another audit department, but readers should be able to combine what they like from each and add their own creativity to develop an approach that might work in their own organizations.

Final Word

Obtaining reliable information about soft controls is a challenge, perhaps the greatest challenge internal auditors have ever faced. We will never be able to meet that challenge to the extent we can with hard controls, because subjectivity is involved. But our stakeholders’ expectations and our professional Standards require that we try. As long as we use a “systematic, disciplined approach,” work in partnership with those accountable, and are careful in drawing conclusions from available evidence, we can accomplish a great deal.

Hopefully, readers who have hesitated to evaluate soft controls because of the tremendous challenge involved will find what they need to get started. I hope that readers experienced in this realm will find something to help them do even better.