Gartner

Research

Publication Date: 25 September 2008 **ID Number: G00161529**

How to Negotiate With Auditors

Paul E. Proctor, Christine Adams

Addressing findings in compliance is a negotiation with your auditor. When making the case for what's appropriate, the more you know (and can document) about the controls, risks and processes that underpin your business, the better off you'll be.

Key Findings

- Addressing audit findings is a negotiation with your auditor.
- To pass muster with auditors, arguments should be properly organized, documented and thought out, and they should address real threats, while balancing costs and benefits.
- Evidence of well-thought-out policy positions, established processes and internal process auditing will be persuasive when dealing with external auditors.

Recommendations

- To create a defensible case to support decisions, focus on risk and materiality.
- Document risks and controls.
- Develop a proactive, process-oriented controls program.
- Formalize your risk acceptance process.
- Negotiate using arguments based on company size, scope and complexity of operations, industry standards or norms, established controls and the cost of controls

ANALYSIS

Negotiation is a fact of life in auditor/client relationships. The guidance contained in this research applies to regulatory, commercial and organizational compliance (see Note 1), as well as all types of parties, including internal auditors, external auditors, executives, boards of directors, regulatory enforcement officials, judges and juries, all of which we will refer to simply as "auditors." Audit and compliance requirements are generally standards-based guidelines, rather than technology "cookbooks." Thus, these requirements are subject to interpretation in terms of what the standard requires and when, where and how it applies. Some standards are imprecise or unclear; others haven't caught up with emerging business issues or business models. For these reasons, addressing scope and findings for compliance is likely to involve negotiations with your auditor regarding the appropriate interpretation and application of standards.

The end result of this negotiation should be an agreement that strikes a balance between meeting the letter and intent of a regulation (or its interpretation) and doing what's most appropriate for your organization, given its risk tolerance, size, capabilities, complexity, industry norms, means and threat environment. Gartner recommends that organizations familiarize themselves with the best practices for achieving appropriate business concepts and approach each negotiation prepared to defend their positions. Building a defensible business case applies to all audit situations.

How to Approach the Negotiation

To effectively negotiate with your auditors, the most important consideration is to understand what's driving the auditor's position. As with any negotiation, the more you are able to put yourself in the other party's shoes, the better able you will be to forge a resolution. A key consideration is the source of or context for the auditor's position — that is, the relevant standard or guidance. In general, disagreements emerge in three broad areas:

- Interpretation — When a standard is unclear or ambiguous, there's room for judgment in interpretation.
- Application — Sometimes, the basis for negotiation is whether the standard in question actually applies; materiality is a key consideration here.
- Misinterpretation — Auditors draw conclusions based on facts in evidence vs. a complete and comprehensive view with all the appropriate context; thus, there is room for misinterpretation.

People in audit or inspection roles are likely to be conservative in their approaches, because that's what the job requires. Consequently, an aggressive position is likely to be met with hesitation, particularly if there's no long-standing relationship and/or abundant information to provide context. You're better off finding an acceptable middle ground, presenting multiple alternatives, or providing more context or explanation regarding your thinking.

Both sides need to maintain an appropriate, productive and professional relationship. Clients often approach auditors adversarially in negotiations, which immediately reduces the chances of a mutually agreeable outcome. The tenets of a productive client/provider relationship — regular, open communication, mutual understanding and experience working together — hold true in the audit relationship. You're more likely to achieve an acceptable outcome if you work with (and not against) your auditor to determine a solution.

Thorough, on-point documentation is essential in making your case. If you're debating a specific issue such as an audit finding or the interpretation of a standard, then you must be prepared to

provide relevant detail and analysis to support your position. If you're negotiating the scope of a compliance project, then a broader (but nonetheless detailed) view of risk and control will be essential. The more you know (and can document) about your risks and the controls and processes you have put in place to address them, the better.

Arguments that are likely to pass muster with auditors should be properly organized, documented and thought through. They should address real threats, while balancing costs and benefits. Organizations can work toward such goals by taking the following steps:

- Identifying reasonably anticipated material risks with an ongoing risk assessment
- Identifying a reasonable and appropriate set of controls to address these risks
- Creating a defensible case to support decisions
- Developing a proactive, process-oriented controls program

Focus on Risk and Materiality

To understand an auditor’s mind-set, determine the role of risk and materiality. From the auditor's perspective, judgment-based considerations, such as materiality and risk, are fundamental concepts that underpin decision making regarding scope and procedures relevant to compliance with regulations. In the simplest terms, risk is a measure of uncertainty, and materiality is a measure of the impact of that uncertainty.

Now more than ever, risk and materiality are useful concepts when determining how far an organization should go when implementing controls for any regulation. For example, a top-down, risk-based approach is a central tenet of a financial statement audit, as well as compliance with the Sarbanes-Oxley Act. PCAOB Release 2005-009 expressly addresses the uniqueness of each organization's situation, calling on auditors to exercise their judgment in "tailoring audit plans to the risks facing each individual client," rather than relying on standard checklists to identify risk.

Risk is usually mitigated by protective measures (controls) or transferred to a third party through such mechanisms as insurance. What remains (risk that is neither mitigated nor transferred) is known as "residual risk," and this must be accepted by the organization. Acceptance means understanding the known risks against which the organization is not protected, and what to do if one of these risk scenarios causes a loss. Residual risk becomes part of the operating plan.

It's impossible to protect against every risk or contingency. Even if perfect control or protection were possible, it would be prohibitively expensive and would be a disservice to the investors and other stakeholders that most regulations have been designed to protect.

For example, U.S. Health Insurance Portability and Accountability Act (HIPAA) regulations accommodate residual risk. Specific HIPAA regulatory language addresses the fact that there is no such thing as perfect protection, and the standards are written in such a way that organizations of different sizes and means can address the standards appropriately for their needs and still be compliant. HIPAA security standards avoid mandates for specific technologies as this would age the standard relatively quickly in a rapidly changing threat environment with the availability of new and more-effective technologies.

The Payment Card Industry Data Security Standard (PCI-DSS) takes a different approach by specifically requiring named technologies and solutions. In many cases, this reduced flexibility forces organizations to spend money on regulatory requirements, rather than on more-appropriate solutions for higher risks. However, there is room even in the one-size-fits-all approach of the PCI-DSS for negotiation when addressing a certification audit.

Federal Information Security Management Act (FISMA) standards also accommodate residual risk and the differing needs of organizations. Like HIPAA, FISMA requires assessment of risk and controls to guide the identification of gaps and the planning of remedial actions to address risk.

Understand Risk and Materiality for Your Organization

Although auditors can look to their experiences with similar organizations when making judgments about risk and materiality, they don't know more than you do about your organization, its key processes, associated risks and established controls. In the strictest sense, that's not their job.

This concept of materiality applies to all audits and findings, whether regulatory, other compliance or internal. Factors that influence judgments of risk and materiality should be considered as part of the defensible business case.

Company Size, Scope and Complexity of Operations

In general, smaller organizations with limited resources and simpler networks need to do less to ensure compliance than large organizations with complicated infrastructures.

Industry Standards or Norms

Understanding risk and materiality considerations for your industry, as well as how industry peers are addressing compliance issues, are important elements of a defensible business case. Most peer information is anecdotal. Auditors have greater insight in that they may draw on their experiences with other companies in a given industry to make determinations. We believe that benchmarking will emerge to help organizations maintain parity with their peers.

Established Controls

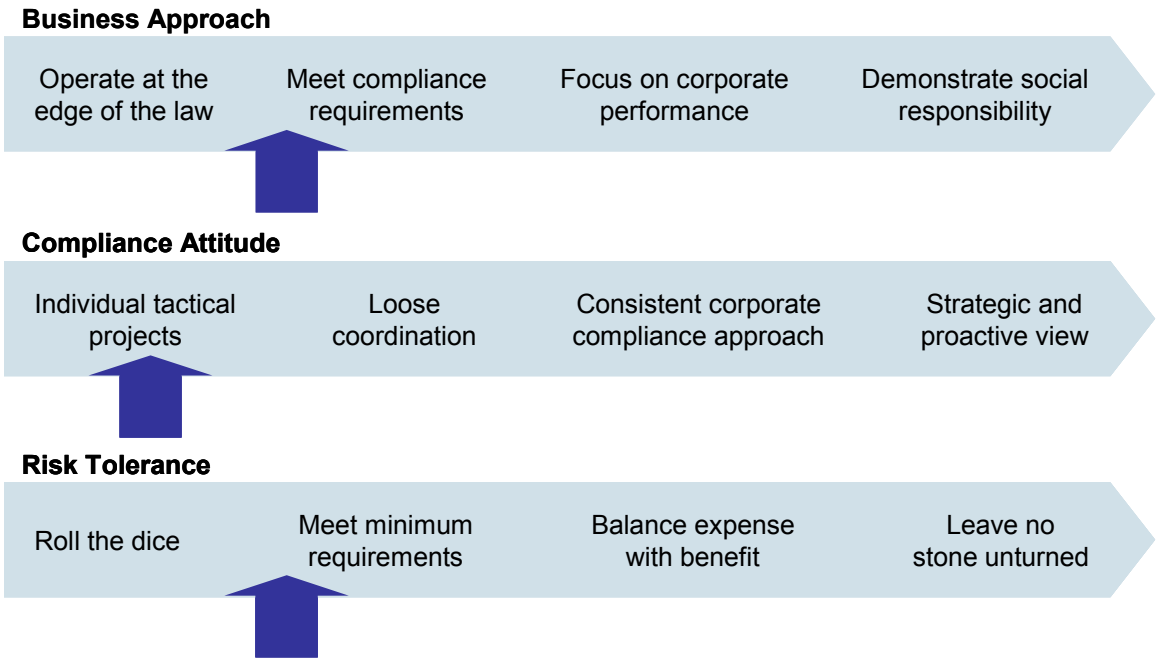
The nature and effectiveness of the established controls will be a key variable in the business case. Controls do not stand on their own; rather, there is a patchwork of compensating preventive and monitoring controls that reduce the material possibility of loss or misstatement below acceptable thresholds. Consider all relevant controls when building a defensible case.

Cost of Controls

When building a defensible case about a control that is unnecessary for compliance, cost can be a consideration; however, the presentation of this justification is sensitive. It should be presented as the increase in risk mitigation does not justify the cost, rather than simply as "it costs too much."

As part of this exercise, it is also useful to critically assess your company's attitude and approach toward compliance, as well as your tolerance for risk. Figure 1 presents some parameters for self-assessment. The further to the left you find your company on the attitude, approach or risk tolerance scales, the more conservative your auditors are likely to be in setting compliance requirements. It is possible that there is a mismatch in your company’s tolerance vs. the tolerance of the auditors. Question auditors about their assumptions concerning risk tolerance to ensue that there is no disconnect.

Figure 1. Approach, Attitude and Tolerance



Source: Gartner (September 2008)

Document Risk and Controls

A thorough, well-documented and methodical assessment of material risks and key controls should be considered a minimum requirement for negotiating purposes. One of the unintended outcomes of Sarbanes-Oxley compliance is that it has illuminated how poorly many organizations document their controls. This is especially true of company-level controls, such as the control environment and the information and communication policies. On the other side of the spectrum is the company that documents every control, but fails to identify and prioritize the risks that the controls are intended to mitigate. Seeking third-party advice can support defensibility, because third parties have no vested interest in the outcome. The most-inappropriate individuals to perform the audit are the people responsible for addressing the findings.

Formalize Your Risk Acceptance Process

One effective argument to compel auditors is that the risks have been recognized and a business decision has been made to accept the risk. Organizations should formalize their risk acceptance process to avoid the impression that business acceptance is a matter of convenience to address a finding. This is more effective in addressing internal audits, in which conscious business decisions to accept risk should guide the auditors, not vice versa. It is more challenging in regulatory audits where an organization will be held to a perceived standard of due care; however, good regulations accommodate the residual risk, and a business's acceptance of risk should affect an auditor's opinion. Develop a process for risk acceptance, and document risk acceptance decisions with management sign-off.

Conduct Audit Training to Stay Within the Scope of the Audit

Gartner clients have reported that overzealous employees cause difficulties in audits by reporting on issues that are not germane to the area being investigated. Being truthful in an audit is critical,

but staying within the defined scope will enable the auditors to accomplish their tasks more effectively. A risk assessment is the proper place for open conversation about risks and control effectiveness. An audit is the place to assert and defend decisions. Employees should be advised to answer the questions they're asked and not offer information they believe might be "helpful."

Don't Wait Until It's Over

If compliance can be considered an ongoing agreement between you and your auditor, then the negotiation process can be considered ongoing as well. Discussions as to what is reasonable and appropriate can occur on several occasions:

- When scoping the compliance program
- At key milestones, such as the designation of key controls
- When making major changes to policies, processes and systems
- When setting the scope of the audit
- When determining whether deficiencies are significant or material
- When developing remedial actions

A good relationship with auditors is important in developing a comprehensive risk management program. It is a good idea to work with auditors when they develop their annual audit plans so that you identify areas of risk where there would be the most benefit from their attention.

RECOMMENDED READING

"Select and Implement Appropriate Controls for Regulatory Compliance"

"Gartner for IT Leaders Overview: The IT Compliance Professional"

"A Risk Hierarchy for Enterprise and IT Risk Managers"

Note 1
Compliance

Compliance can be thought of as interpreting what the regulations say, understanding where your company stands, documenting a plan for achieving compliance, executing the plan, and devising measures and controls to prove that you've implemented the plan. Organizations must realize that compliance is a set of expectations and requirements agreed on by two parties. These include combinations of implicit and explicit bargains to which both parties must adhere. In this context, a bargain doesn't mean low cost, rather a mutual undertaking wherein you and your auditor come to terms.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509