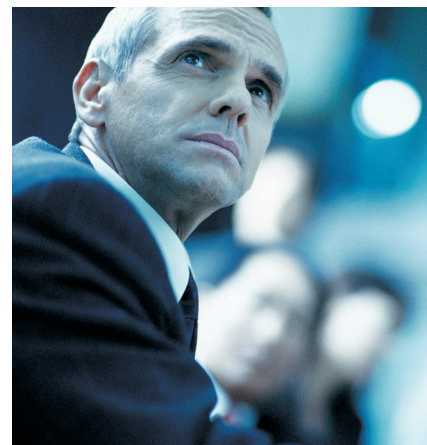


## INFORMATION TECHNOLOGY STRATEGIC INITIATIVES

*A Focus on Compliance Management Programs*



RISK ADVISORY • TAX • FINANCE & ACCOUNTING

### OVERVIEW

Expectations for Information Technology's contribution to the organization have increased dramatically, as has IT's participation in the organization's operations.

Today, exposure to legal, regulatory and compliance risks is an every day occurrence. Coupled with the current economic, regulatory and social climate, these risks have propelled corporate governance, compliance management and integrity to a top priority. More than ever, organizations understand the need to articulate and integrate the principles of a strong compliance management program (CMP) into their very fabric.

Integrating multiple compliance management requirements can help an organization more effectively and efficiently drive performance. At a high level, governance establishes objectives and parameters under which the organization must operate. Risk management helps the organization identify and address potential obstacles to achieving objectives. Compliance management ensures the parameters are accurate, and that the organization does indeed conduct business within those guidelines.

### TECHNOLOGY RISK MANAGEMENT DEFINED

Technology risk management is "the management of risk for recurring and nonrecurring business events supported by technology." These events can be grouped into the following areas:

- Organizational changes
- Compliance requirements
- Operational responsibilities
- Financial decisions

The stakeholders involved in these events include everyone in Information Technology and senior management. Whether the business is large or small, it will experience these events at one time or another.

### INFORMATION TECHNOLOGY STRATEGIC INITIATIVES

Every organization has to deal with threats and vulnerabilities. Those that succeed have developed and implemented risk management programs that focus on protecting assets. As new regulations and compliance requirements proliferate, organizations must make tough decisions between meeting these compliance requirements and accepting the associated risks. For most, non-compliance is not an option because of fines, penalties, and/or potential loss of reputation.

Top of mind issues for most CIOs are likely to include the following:

- Driving business value from Information Technology
- Implementing and executing an IT governance program
- Identifying and mitigating information security risks
- Identifying and mitigating information technology risks

Jefferson Wells delivers professional services in the areas of risk advisory, tax, and finance and accounting. We serve clients, including Fortune 500 and Global 1000 companies, through highly experienced professionals working from offices worldwide.

To learn more about our firm and our professional services, contact your local Business Development Manager or visit our Web site at [www.jeffersonwells.com](http://www.jeffersonwells.com).

## MAPPING STRATEGIC DECISION MAKING

While organizations should approach their overall operations strategically by beginning on the left side of the chart, most start tactically in columns 4 or 5.



- Identifying and mitigating business continuity risks
- Identifying and mitigating outsourcing/offshoring risks
- Streamlining management of IT-related legal issues
- Enhancing efficiency of compliance management programs

Most of those issues focus on legal or regulatory compliance. Typically, organizations approach their compliance initiatives from a task or one-off perspective. But due to the risk of non-compliance and to gain potential efficiencies and savings, CIOs should include compliance-related objectives into their overall IT and organizational strategic planning process.

## THE COMPLIANCE MANAGEMENT PROGRAM

In aggressive regulatory environments, new regulations are continuously emerging. The proliferation of legal and regulatory requirements has forced organizations to focus more heavily on developing compliance programs to deal with these new requirements. These include:

- **Regulatory compliance** - Compliance incorporating required safeguards and information technology controls to meet information security requirements. The Chief Compliance Officer is responsible for regulatory compliance in most organizations.
- **Sarbanes-Oxley (SOX) compliance** - Ensure documentation, assessment and testing of controls to meet attestation requirements of the client's external auditor. The Chief Audit Executive normally handles SOX compliance oversight.
- **Information security annual reviews/testing** - The Chief Information Security Officer ensures that annual security requirements are performed.
- **Payment Card Industry (PCI)** - Ensures operational compliance with payment card industry standards. The primary responsibility for this effort lies with the CIO.

Since, typically, a number of compliance standards have to be met, a holistic approach is essential. Otherwise, the complexity of compliance initiatives can create inefficient overlapping controls or gaps that ultimately lead to non-compliance. A holistic CMP allows an organization to address multiple compliance requirements such as HIPAA, SOX, PCI requirements, and many others.

## DESIGNING A HIGH-PERFORMING CMP

Compliance is a key supporting mechanism for effective governance. Compliance with regulatory requirements and the organization's own policies is a critical component of effective risk management. Monitoring and maintaining compliance should not be viewed as an exercise to satisfy regulators. In fact, monitoring and maintaining compliance enables organizations to maintain their ethical health, support long-term prosperity, and preserve and promote their values.

Simply put, a compliance management program supports the organization's objectives, identifies the boundaries of legal and ethical behavior, provides a compliance structure for IT general controls and establishes a system to alert management when the organization approaches boundaries or an obstacle that could prevent the achievement of an objective.

Compliance can be a daunting challenge, but it is also an opportunity to establish and promote operational excellence throughout the entire organization and significantly improve the overall operational performance within IT. A high-performing, integrated IT compliance management program should be embedded in the organization's functional units and overseen by a separate group with overall responsibility and accountability. The focus on IT compliance should revolve around the organization's need, regulatory requirements and the IT general controls structure related to those needs and requirements.

Once an issue is detected, the organization must be prepared to respond quickly and appropriately to minimize its impact. Management should continuously improve its compliance management program. This will enable it to better prevent, detect and respond to similar issues in the future.

Like any other core capability and/or process, the compliance management program should strive to deliver tangible benefits and outcomes. Every organization is unique, with its own objectives. As such, some objectives of the compliance management program will also be unique. A compliance management program should deliver a few universal program outcomes/objectives. These include 1) an enhanced culture of trust, accountability and integrity, 2) prevention of noncompliance or preparation for noncompliance, 3) protection from negative consequences, 4) detection of noncompliance, 5) response to noncompliance, and 6) improvement of the program to better prevent, protect from, prepare for, detect and respond to noncompliance.

An important characteristic of a high-performing program, and one that cannot be overstated, is the existence of a strong culture and tone at the top. A strong culture provides important benefits. For instance, a strong culture can compensate when controls are deficient or lacking.

The success of an effective compliance management program depends on its ability to meet the challenges of constant change, increasing complexity, rapidly evolving threats, adequate authorization and funding, appropriate tools to facilitate measurement, comprehensive training and an early awareness of the approach.

## IMPLEMENTING THE PROGRAM

In many programs, implementation is the most difficult step and the area where most failures occur. If well executed, however, it can represent the biggest opportunity to create a positive influence on the organization's performance and culture. A partnership between the organization and the IT function is crucial to implementation success.

The engaged involvement of key stakeholders is critical to a successful implementation or major enhancement of a compliance management program. This includes effective communication and initial agreement by all major parties, regarding objectives, goals and the overall purpose of the program. By working together, compliance management officers, executive management and the board can help ensure a compliance management program not only contributes to the improvement of the organization's governance practices but to the achievement of its strategic objectives.

An important first step is to integrate compliance management by addressing both the letter and spirit of the law or regulation. For some companies, this means translating the requirements into internal policy and procedures and

designating penalties or consequences for not adhering to these internal standards.

Compliance management processes must be embedded into the organization's fabric. Organizations must methodically assess and prioritize present and emerging compliance management risks. Such research should take into account the organization's culture, compliance management history and industry issues. The organization's processes should incorporate compliance management program needs. Boards should routinely discuss risks and how they are addressed with management.

Demonstrating leadership behind these principles is key to gaining momentum. The board should ensure senior management consistently communicates and models the organization's values and behavioral expectations as identified in the compliance management program.

The compliance management program should require accountability and ownership. To become a true part of the organization's fabric, the compliance management program should promote a corporate culture that emphasizes making individuals accountable for their actions. The board and management should ensure employees have appropriate training and information and should participate in training themselves.

Issues and problems should be, and in some cases are, required by law to be investigated and proactively managed to resolution. Unethical or illegal behavior should be addressed promptly. Employees must be required to raise and resolve violations of compliance or ethical standards. To do so, they must feel confident they can take action without fear of retaliation. Such fears have been reduced, but not eliminated, with the introduction of the SOX whistleblower protections and other regulations.

## MEASURING PERFORMANCE

Like any other critical activity, an organization's compliance management program should be measured. By using accurate, timely data on the organization's performance, managers know whether they are moving the organization closer to its objectives. Measuring compliance management program performance also helps organizations gauge their improvement and learn whether its tactics are contributing to achievement of its strategic objectives. Additionally, keeping the board informed is a critical activity, and robust performance reporting facilitates that important effort.

Measurement can be performed in any number of ways. The measurement platform helps ensure program objectives are aligned with and contribute to the organizational objectives in a documented method. Measurement should focus on effectiveness, efficiency and responsiveness.

Effectiveness encompasses both design and operational effectiveness. Design effectiveness describes the degree to which a system or process is logically designed to meet legal and other defined requirements. Does the system or process contain all the necessary elements to thoroughly evaluate risk? Was it designed for maximum effectiveness? If not, what features must be added to improve the system? Design effectiveness is very much a logical test that considers all requirements, risks and boundaries to determine if the system is appropriately designed.

Operational effectiveness describes the degree to which a system or process operates as designed. If the system was designed properly, does it function correctly? Does it operate the way it was designed? If not, how must it be managed to elevate its level of operation? Operational effectiveness helps management understand if, given a strong design, the system is operating as intended.

The concept of efficiency captures the cost of the process or system, including the financial impact and cost of internal labor. Financial efficiency describes the total amount of financial capital required to execute a process. The internal labor cost represents the type and level of individual(s) required to participate in the process. While human capital costs can be partially captured in purely financial terms, intangible opportunity costs must also be captured. In other words, if the program relies too heavily on senior executive time and focus, it may represent more than just purely financial costs, such as salary, benefits and other overhead. The loss of executive time and focus on other strategic objectives such as growth, profitability, talent retention and customer loyalty must also be considered.

Responsiveness should be viewed on two dimensions, the system's ability to operate quickly and flexibly in response to changing circumstances. Cycle time describes the total hours and/or total duration needed to execute a process. Flexibility and adaptability describe the degree to which the system can adapt to changes, including new requirements or organizational change.

Changes may be internal or external. New regulatory environments, changing market conditions, or altered public perceptions and concerns require the organization to make adjustments. A responsive measurement system adapts quickly to changes in the environment using a long-range perspective - foreseeing and preparing for changes that are more distant.

A measurement system and approach should embody these principles:

- Objectives-focused
- Results-oriented
- Efficient

Organizational objectives should include program metrics and measurement, helping management understand how the program contributes to overall enterprise objectives.

The measurement system and approach should be simple and cost-effective to ensure sustainability. Management should look for opportunities to gather data from existing systems rather than creating entirely new systems.

Senior management and the board of directors should commit to a measurement approach and ensure a high-level executive is charged with overall accountability. This should include a commitment to program longevity, since it may take a long time to realize the measurement program's full potential.

Key metrics and indicators should be specific, simple, measurable, actionable, relevant, timely and smart. There should be a balance between leading and lagging indicators. Lagging indicators show how the company has already done (revenue growth in the past quarter, number of workplace accidents in the last year). Leading indicators are predictive of future performance. Examples are on-time delivery rate, which can lead to higher customer satisfaction ratings and, in turn, more sales to existing customers.

Indicators should provide visibility into both short-term and long-term objectives. Overemphasis on short-term objectives can stifle long-term growth by short-changing new product development. Emphasis on short-term financial results, such as quarterly profits, can lead to reduction in spending on research for new product development, or purchasing cheaper components to raise profit margins, leading to lower product quality, more product returns, complaints from customers and loss of business.

Focusing on internal trends will help management understand them. Once internal trends are understood, the use of external benchmarks will be more meaningful.

While the measurement process provides an indicator of compliance success, there should also be metrics around the measurement process. The measurement system should be reviewed and improved on an ongoing basis. It is only by gaining experience measuring performance that the organization can really refine and improve the system.

## CONCLUSION

Compliance and compliance management programs can no longer be viewed as one-off programs simply designed to address a specific need or to "check a box." To be effective, compliance must become part of the organization's overall strategy and operations.

Today, the approach to compliance must be a holistic one, and the compliance management program should be designed for improved performance and maximum efficiency.