ENTERPRISE CONTRACT MANAGEMENT: THE VANGUARD OF SUSTAINED COMPLIANCE

IN THIS CHAPTER:

- Compliance: Past, Present, and Future
- Sustaining Compliance
- Role of Technology in Achieving Sustained Compliance
- ECM and Compliance Management

4.1 OVERVIEW

To the casual student of business history, the recent evolution of modern enterprises may seem to be traveling a logical and gradual path, much as it has over prior centuries. Day-to-day market forces and the basic laws and paradigms of modern business may appear to be operating as they should, and except for the dramatic impact of information technologies and globalization and the ripple effects of crises such as 9/11 and Katrina, it might appear that the past decade has been one of evolution rather than revolution.
The casual student of business history would be wrong. While external appearances may not offer ready evidence of the underlying reality, modern business enterprises, especially those based in the United States, have undergone a quantum shift in priorities and practices—the corporate equivalent of a tectonic shift in the very center of gravity of modern business. Its name: compliance.

Compliance was thrust upon the business scene with the full force of every conceivable governmental agency, investor, and customer, driven by forces which had long been shifting under the surface. And in the aftermath of the era of Enron, modern business is faced with a new landscape, one defined by the strictest standards and codes of conduct ever imposed upon the free market system.

One of the great legacies of the revelations of corporate noncompliance during recent years is not the elucidation of the misdeeds themselves, but the exposure of the underlying weaknesses and vulnerabilities at the core of modern corporate culture. Historically, compliance has been viewed by businesses largely as a problem that had to be either circumvented or dealt with, a necessary cost of doing business, something to be tolerated. Even those companies not found guilty of deliberate violations of compliance requirements frequently sought the shortest possible path to meet minimum requirements in order to get on with business as usual.

Prior to the Enron era, compliance was not embraced as a potentially proactive force in the long-term growth and success of an enterprise. Compliance departments were not viewed as autonomous agents of quality and change, put in place to ensure a corporate culture of sustained quality and risk minimization. Utilizing a health metaphor, compliance has historically been regarded as a Band-aid, when in fact the patient was in need of a heart transplant.

Since compliance concerns virtually every aspect of an organization’s activities, it is fundamentally linked to that organization’s information technology architecture. Historically, compliance managers had little if any say over the design or role that IT played in the execution of their responsibilities. Compliance managers were expected to adapt to existing IT systems, instead of requiring that such systems be tailored to serve the purpose of compliance. When IT did not fit compliance, historically it was compliance that had to change.

But the compliance “earthquake” has permanently altered the modern business landscape. With compliance initiatives clearly at center stage for virtually all organizations, the relationship between proactive compliance and state-of-the-art IT solutions is at the vanguard of an organization’s survival. Moreover—and as a final chapter on the Enron era—compliance is now emerging as a force for vision in defining the core culture of modern enterprises, ushering in what
some have recently referred to as the era of compliance, where corporate governance is not a subject that deals with the avoidance of pain, but rather a standard to be sought and achieved through a systematic implementation of compliance initiatives by which compliance monitoring occurs in the normal course of business activities. Out of the debacles and shattered financial landscapes of the 1990s, a new attitude about compliance in modern business has emerged. In short, the rebuilding of corporate culture has begun, and forward-looking enterprises are now seeking their own road maps to ensure the future is built on bedrock.

One of the most profound consequences of this shift in corporate priorities and cultures has been the assignment of accountability up the corporate ladder to executives, directors, and senior managers. Shareholders, government agencies, watchdog groups, and the general public have all raised the bar for senior management in terms of assigning direct responsibility and consequent liability for noncompliance. No longer does turning a blind eye result in a slap on the wrist—real prison time and real financial loss await modern executives who do not place compliance at the forefront of their corporate agendas and mission statements. This shift in consequence and responsibility has led to an unprecedented top-down penetration of compliance as a priority at every level of an organization—a new ripple effect felt both deeply and broadly through an organization’s operations, staff, accounting, and record keeping.

A second factor shaping the landscape of the new era of compliance is the increasing level, complexity, and scope of challenges and demands placed upon large organizations, including:

- Increased regulatory, fiduciary, and legal demands
- Increasing competitiveness for public confidence and financial performance
- Increasing digitization of business relationships, including contracts
- Need for flexible systems that can respond to new compliance demands

Given the scale and complexity of large modern organizations, and the unprecedented compliance challenges they face, a logical question is:

**What role can technology play in modern compliance management?**

Clearly, information management is at the heart of compliance management; information is, after all, the very currency of compliance—from the manufacturing floor to the marketplace, from the boardroom to the courtroom.
Companies that manage and control their information in a compliance-oriented framework are best positioned to avoid problems and remain competitive.

The subtitle of this chapter on the subject of Enterprise Contract Management (ECM) is “The Vanguard of Sustained Compliance.” A fundamental premise of this chapter is that compliance involves an organization’s behavior in its relationships—with its employees, its shareholders, its customers, its suppliers, and with the public. Since the terms of such relationships are documented in a spectrum of contracts (including legislation, agreements, and resolutions), ECM is an essential compliance function. Moreover, ECM solutions best serve an organization’s efforts to achieve sustained compliance when they are designed, implemented, and monitored to integrate seamlessly into an enterprise’s IT architecture and fully embrace that organization’s contract universe.

In this chapter, the following aspects of ECM and compliance management are covered:

- An overview of compliance in both its historical and contemporary contexts
- An approach to achieving sustained compliance
- The role of technology in achieving sustained compliance
- The role of ECM in achieving sustained compliance

4.2 COMPLIANCE: PAST, PRESENT, AND FUTURE

4.2.1 Definition of Compliance

The first reaction of most people when they hear the word compliance is to think about regulations and legislation. However, in today’s business environment, compliance stands for much more. It involves ensuring not only that an organization meets the requirements of regulations, legislation, and standards defined by agencies that are external to the organization, but that it also enforces and ensures adherence to its own policies, procedures, standards, best practices, and plans.

Given this definition of compliance, there are three major domains of compliance within an enterprise:

- Regulatory (governmental and legal)
- Procedural/operational (within an organization’s business functions)
- Contractual (between an organization and other entities)
These domains are depicted graphically in Figure 4.1. The impact of each of these compliance domains upon an organization is evident when one considers the intimate linkages between the individual domains.

4.2.2 Evolution of Compliance in Modern Business

It is useful to reflect upon how compliance achieved its current status among corporate priorities. As stated earlier, the subject was once one of the least discussed among many organizations, and only in the past few years has it recently emerged as the buzzword in corporate mission statements.

Historically, many companies regarded compliance as a necessary cost center to mitigate the risk of lawsuits and to appease regulatory agencies. The saying “do enough to get by” might have been coined to characterize the culture of many organizations regarding compliance. “Tolerated but not embraced” and “pulled to the forefront only when needed”—these phrases do not inaccurately portray the general attitude of many corporate executives toward compliance before the decade of Enron and WorldCom.

It is not the intent of this chapter to suggest that all enterprises in the pre-Enron world deliberately attempted to circumvent the purpose of compliance. In fact, it is evident that most of the compliance failures of the past were not
deliberate, but rather were the inadvertent consequences of misplaced priorities. There was, however, plenty of blame to go around in the wake of Enron and WorldCom, the dot-com bust, and the stream of accounting scandals, fraud and corporate bankruptcies, insider trading, and executive compensation schemes. These events brought to light a reality that had long gone unobserved by the general public: in some corporate spheres, consistent disregard for compliance had become the norm.

4.2.3 The Current State of Compliance

In the aftermath of this era of corporate compliance debacles arose a network of rules, regulations, codes, standards, policies, procedures, and expectations that have permeated virtually every level of modern business—in many respects for the better. These regulations affect different industry sectors (such as healthcare organizations, financial institutions, insurance agencies, brokerage firms, federal agencies, publicly traded companies, etc.) in different ways and require that differing initiatives be put in place to meet a myriad of requirements. A high-level overview of some of the key regulations impacting businesses across industries today is presented below. An even more detailed list of such regulations is presented in the appendix of this book.

- **Sarbanes-Oxley Act (SOX):** Of all the recent regulations, the one that has received the maximum attention from organizations across all industries is the Public Company Accounting Reform and Investor Protection Act, also commonly known as SOX. This act has brought about the most extensive reform that U.S. financial markets have seen since the enactment of the Securities Act of 1933 and the Securities Exchange Act of 1934. While the complete SOX has eleven titles, Sections 302 and 404 have had the greatest impact in terms of ongoing compliance obligations. Section 302, which pertains to corporate responsibility for financial reports, requires the certification of disclosure in quarterly and annual reports by the chief financial officer. Section 404 requires that annual reports contain a discussion of the effectiveness of internal controls. These two sections place significant responsibility on the chief financial officer and an organization’s external auditors, who for the first time must provide an opinion on the reliability and effectiveness of the internal control representation made by an organization’s CEO and CFO. Finally, SOX Section 409 mandates significantly expanded disclosure require-
ments, with disclosures made as quickly and completely as possible after pertinent events affect an organization’s performance.

- **Gramm-Leach-Bliley Act (GLBA):** GLBA impacts banks and other financial institutions such as securities firms, insurance agencies, lending firms, brokerages, and credit counseling firms. It requires financial services companies to implement safeguards for customers’ current and legacy information. The act makes it illegal for a financial institution to share customers’ nonpublic personal information with third parties unless the organization first discloses its privacy policy to consumers and allows them to opt out of that disclosure.

- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA was originally passed in 1996 to help expand insurance coverage to the unemployed, but over the past several years it has been expanded to include privacy clauses and security requirements. HIPAA regulations require healthcare and insurance organizations to have procedures in place to prevent, detect, contain, and correct security violations. They must also have procedures and processes to regularly review records of information system activity.

- **Basel II:** Already a part of international banking law, the Basel II Accord is essentially a risk management mandate that requires proven IT security and administration. Capital reserves, supervision, and market discipline are Basel II’s three risk management pillars. Basel II requires banking institutions to reserve capital that can be used to cover operational risks, including those that arise from inadequate internal processes or external events.

- **FDA 21 CFR Part 11:** This legislation became effective in August 1997 and affects companies in all industries regulated by the U.S. Food and Drug Administration (FDA), including but not limited to biopharmaceutical (human and veterinary), personal care products, medical devices, and food and beverage. It establishes the criteria for the use of electronic records and signatures. For companies that meet Part 11 compliance, electronic records and signatures can replace traditional paper records and signatures, thereby enabling pharmaceutical and other FDA-regulated industries to streamline processes and reduce costs by moving to digital records.

- **Federal Information Security Management Act (FISMA):** Expansive in scope, FISMA was enacted by the Bush administration in 2002 in response to concerns about cyber-security. The act requires all federal agencies to develop, document, and implement agency-wide
programs to secure data and information systems that support agency operations and assets, including those managed by other agencies or contractors. Agencies will be subject to annual tests, including evaluations of their IT security systems. With some 3.4 million cybersecurity incidents documented by the U.S. government in 2005, many analysts believe the government will put additional pressure on federal agencies to secure their IT infrastructure quickly.

- **European Union Data Protection Directive (EUDPD):** The EUDPD is applicable to all local and international organizations doing any business with an organization in the member states of the European Union regardless of industry, shape, or size. It specifies that user data must be collected for a specific purpose, must be processed lawfully, and cannot be retained any longer than required. The intent behind the directive, therefore, is to protect the fundamental rights and freedoms of individuals and in particular their right to privacy with respect to the processing of personal data.

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** PIPEDA is a Canadian federal act that governs the collection, use, and disclosure of personally identifiable information in the course of commercial transactions. The act was created in response to EUDPD, which limits trade with nations that do not provide privacy protection equivalent to the European Union directives. The law requires organizations to obtain consent when they collect, use, or disclose personal information; provide an individual with a product or a service even if the individual refuses consent for the collection, use, or disclosure of his or her personal information unless that information is essential to providing the product or service requested; collect information by fair and lawful means; and have personal information policies that are clear, understandable, and readily available.

- **Department of Defense 5015.2:** This regulation provides implementation and procedural guidance on the management of records in the Department of Defense. This standard sets forth mandatory baseline functional requirements for records management application software used by Department of Defense components in the implementation of their records management programs. In addition, this standard also defines required system interfaces and search criteria to be supported by the records management applications and describes the minimum records management requirements that
must be met, based on current National Archives and Records Administration regulations.

- **Securities and Exchange Commission 17a-4**: This rule requires the retention of all customer records, financial transactions, bank records, and buy/sell orders. All correspondence is to be retained for six years. This includes e-mail and instant messages if an organization uses these for transactions. Organizations are required to keep a secure copy of every transaction, and records must be maintained on nonalterable, nonerasable media.

It is evident that compliance covers a much broader arena than just corporate accounting for most companies. These regulations have emerged for reasons ranging from data privacy to IT security, from workplace to employee safety, and from tighter controls around financial management to environmental concerns. There are regulations that apply to specific vertical sectors, such as the Federal Energy Regulatory Commission to energy, OSHA and ISO to manufacturing, HIPAA to healthcare and insurance, and Department of Defense 5015.2 to defense. In addition, companies with a global presence are required to comply with regulations not just in the United States but also in regions worldwide where they conduct business.

### 4.2.4 The Future of Compliance

As organizations across industries and geographies have rushed to meet the requirements of legislation, regulations, and standards, some key trends—and lessons learned—have emerged which will shape the future of compliance:

- **Execution approach**: Achieving compliance with regulations was often treated by many organizations as a distinct project with a definite beginning and end. Resources were reallocated from multiple departments, the focus of internal audit departments was redirected, consultants were hired to assist in achieving compliance, and the compliance initiative was assigned a higher priority over other business initiatives. However, achieving compliance is no longer a one-time requirement; the project implementation approach, which worked well for initiatives with a definite beginning and an end, no longer applies to current compliance initiatives. In the compliance environment of today and tomorrow, organizations need to institutionalize good corporate governance and effective internal con-
controls as part of day-to-day operations in order to achieve sustained compliance.

- **Business processes**: Much of the initial effort around achieving compliance was heretofore focused on implementing manual processes or custom applications to address specific compliance issues. While such efforts helped organizations achieve compliance in the short run, they did little to address the root cause of the problem—inefficient business processes. Leading organizations, therefore, must understand that sustained compliance requires a retooling of their underlying business infrastructure, architecture, and procedures. These elements need to be carefully designed, implemented, and monitored to ensure that good corporate governance and solid internal controls are embedded within the organization for sustained compliance.

- **Technology**: When many compliance efforts were initiated by organizations a few years ago, those responsible for implementation did not fully comprehend the role that technology could play in achieving compliance. At the same time, IT departments did not know how they would be impacted by these compliance efforts. However, as businesses began to dig deeper and came up with solutions to address compliance issues, it became clear that technology could, and eventually would, play a significant and perpetual role in an organization’s effort to sustain compliance.

  The software industry responded immediately to this need. A large number of technology solutions have emerged in recent years, each attempting to address the new and more stringent needs of organizations in managing newly required documentation, evaluation, testing, monitoring, and reporting activities. Most of these solutions are still in their infancy, and the compliance software market will undoubtedly go through a maturing period characterized by consolidation over the next three to five years. Organizations will need to continue to invest in technology solutions to support compliance efforts in some key areas such as document management, records management, workflow, and reporting.

- **Corporate communications**: Not surprisingly, considerable confusion has resulted from interpreting the numerous compliance regulations that have appeared on the corporate horizon during recent years. The need to resolve such confusion has given rise to an emerging interest in improving corporate communications and informa-
tion systems as they relate to compliance issues, policies, procedures, and training. Organizations have begun to understand the importance of defining roles and responsibilities of employees explicitly and ensuring that employees understand their changing roles in achieving compliance in the new regulatory environment. Business-to-employee communication and employee education are of critical significance in the effort to sustain compliance over an extended period of time.

- **Governance and risk management**: Given the present and future compliance environment which demands the embedding of good governance within an organization, it makes sense to view compliance initiatives within a larger corporate governance and risk management framework. In the past, the absence of a formal governance and risk-management-based approach left organizations with no way to prioritize their activities. Some initiatives focused on the wrong areas, resulting in a disproportionate amount of resources being spent on documenting and testing controls that did not truly mitigate risk.* To achieve compliance on an ongoing basis, organizations need to implement a comprehensive and structured governance, risk, and compliance management (GRC) model that is consistent with their strategy and risk management objectives and properly aligns people, process, and technology capabilities to meet these objectives.

Armed with knowledge of trends and lessons learned from the past, most forward-thinking organizations have realized the importance of aiming to achieve sustained compliance instead of focusing solely on the near-term low-hanging fruit (i.e., achieving compliance in the short run by putting manual processes or workarounds in place). Forward-looking organizations view compliance:

- Not as a burden, but as an opportunity to make positive changes throughout the organization
- Not as a one-time or just-in-time project, but as an ongoing process of continuous improvement
- Not from a silo approach, but with a holistic view across the enterprise within an integrated GRC framework

---

* Under Control: Sustaining Compliance with Sarbanes-Oxley in Year Two and Beyond, Deloitte Consulting, New York, 2005.
Not as a necessary and burdensome cost, but as an investment and a way to improve the overall efficiency and effectiveness of internal business processes and ultimately to reduce costs.

The next section in this chapter, therefore, describes a new vision of compliance and what organizations across various industry sectors can do to sustain compliance.

4.3 SUSTAINING COMPLIANCE

4.3.1 A New Vision of Compliance

As is evident from our discussion in the previous section, compliance efforts in most organizations have historically been treated as ad hoc, silo-ed, and disconnected one-time projects, growing layer upon layer, adding to the cost and resources, not fully realizing the advantages of sustained compliance. Instead of this reactive and often unproductive approach to compliance (which reduces the overall agility of an organization and thereby increases its risk), organizations would be better served with a new vision of compliance—one that embeds a culture of compliance into the underlying business fabric, supporting organizational efficiency with repeatable and sustainable processes.

This new vision of sustained compliance puts stakeholders first by embracing internal governance, ethics, and risk management guidelines. It also addresses external regulations and supports compliance with both the letter and the spirit of the relevant laws and regulations. Such a vision approaches compliance with financial and operational policies and procedures, as well as commitments to stakeholders, as seriously as it approaches legal and regulatory mandates.* It views stakeholders as any group that can impact the value of the organization, including customers, investors, employees, regulators, and society as a whole.

This new vision of compliance (see Figure 4.2) aligns compliance efforts within an organization through ongoing implementation of its goals and objectives. Moreover, this vision functions within an integrated enterprise-wide GRC strategy as opposed to treating compliance as a discrete function within the organization (see Figure 4.3). Treating compliance as a discrete function leads

FIGURE 4.2. A New Vision of Compliance

FIGURE 4.3. Governance, Risk, and Compliance Management Strategy
to unacceptably high costs, heightened risk, distraction from the corporate mission, and ultimately competitive disadvantage. However, when dealt with as part of a GRC strategy, compliance can be sustained for the long run and can become self-perpetuating because corporate culture, people, processes, and technology work collaboratively to ensure compliance with both internal and external policies.

### 4.3.2 The “Ripple Effect”

It is evident that a forward-thinking GRC strategy is founded upon effective compliance management. Such a strategy requires that the tenets of good governance, risk assessment, and compliance be completely integrated into the mission, culture, and daily activities of an organization, from the boardroom to the mail room. Only then will a strategy lead the organization down the path of achieving sustained compliance. When different organizations work toward individually achieving sustained compliance by deploying such a GRC strategy internally, the ripple effect and synergy between their efforts will cause the level of compliance across the corporate world to rise as a whole. Never before in the corporate sphere has the term “raising the bar” been more apropos.

Figure 4.4 illustrates the evolution of compliance that will occur when organizations implement an integrated, enterprise-wide, and forward-thinking GRC strategy. Such a strategy will influence suppliers, customers, and other business partners to follow suit. The “current state of compliance” depicted in Figure 4.4 indicates that the legal and regulatory universe is changing and expanding dynamically. In this current universe, with mandated deadlines looming, legal departments and compliance officers (the traditional risk managers within organizations) make their best guesses as to how to interpret and enact compliance requirements. Top management views such compliance efforts as a “one-time deal,” redeploying employees and pulling resources away from other efforts in order to meet compliance deadlines. In other words, the focus in the “current compliance universe” is almost exclusively internal and discrete. Those in senior management lack the visibility to see how compliance mandates affect their counterparts (i.e., their customers, suppliers, and other business partners). Moreover, senior management is not aware that the compliance engine is not running on all cylinders available to it.

Fortunately, the model of compliance evolution does not stop here. By the time the corporate world reaches the “intermediate state of compliance,” top management and legal officers will have been successful in complying with the letter of the law but, mindful of the disruption and costs such initiatives can
entail, will not want to repeat the monumental effort required to achieve compliance beyond its present state. In our model, such managers will realize that a superior way to address the demands of today’s regulatory environment is to deploy compliance efforts as part of an integrated and enterprise-wide GRC strategy, thereby transforming the perception of compliance within the organization from a burden to a catalyst for better business performance. At the same time, organizations will realize that, in order to achieve sustained compliance, they will also need to influence their business partners, customers, and suppliers to move toward a culture of compliance.
In the “optimal state of compliance,” all organizations make a conscious effort to function in a state of sustained compliance. Organizations encourage, if not require, their business partners to be compliant as well. Such peer pressure, coupled with a growing awareness of the long-term benefits and financial rewards of compliance, would ultimately transform the corporate world as a whole to function at this higher, sustained level of compliance.

4.3.3 Components of Sustained Compliance

As illustrated in Figure 4.5, to the extent that sustained compliance is a machine being assembled by an organization, there are three component parts that must be put together to work as a unit:

- People
- Process
- Technology

The following sections discuss the role that each of these components plays in ensuring that compliance can be sustained within an organization.

4.3.3.1 People

People are the agents responsible for the very acts of compliance. As such, they play the central role in ensuring sustained compliance via implementation of an integrated, enterprise-wide GRC strategy. Organizational executives, such as the CEO and CFO, are explicitly and often solely responsible for internal control. As they survey the corporate culture, they must reasonably map out how com-
pliance will be achieved and by whom. If a new GRC strategy calls for new tasks, executives have the responsibility of creating new positions or restructuring existing ones so that compliance demands can be met. As part of this exercise, organizations should identify the skills and competencies needed in these new or changed positions and ensure that a staff development or augmentation strategy will enable the transition from the current state to the desired state.

Most importantly, executives should remember that their vision is a guidepost for their employees. They need to set high standards and hold employees accountable to meet them. They also need to institute incentives to promote a culture of compliance and establish training programs to arm employees with all the tools and information needed to achieve and sustain compliance. Finally, they should continually communicate progress to employees and managers so that everyone is on board with establishing sustained compliance via a new GRC culture.

### 4.3.3.2 Process

Organizations are only as strong as the business processes in place that allow employees to carry out their responsibilities in an accurate, timely, and effective manner. Not only does compliance impact existing business processes, but it may also require that new processes be put in place to directly manage compliance-related issues. Therefore, organizations must survey both the processes required and how they will allocate/designate resources to carry out compliance-related tasks. Typical questions that arise during this phase of the consideration are:

- What processes and activities must be accomplished routinely to ensure the effectiveness of an enterprise-wide GRC program?
- What processes expedite compliance rather than add complexity?
- What processes need to be standardized or formalized?
- What processes are in place for training and for ensuring accountability?

A fundamental process to be considered is risk management, a primary function of which is to identify shortcomings in organizational infrastructure, policies, and related systems. In addition to preparing for proactive compliance, process developers must consider risk management and remember to incorporate elements into their strategies that proactively address the systematic identification of failures, errors, and other forms of inadvertent and deliberate risks.
to the organization. Similarly, mandates such as SOX require protection for whistle-blowers. Processes for addressing these issues should not be secondary to other processes designed to improve the GRC structure, but rather should be logically and systematically included as part of the overall compliance initiative.

The key to optimizing the process dimension of compliance is balance. In addition to preparing for the proactive aspects of new compliance implementation, process developers should also focus on incorporating and refining systems to address failures and errors in information flow and its operational consequences.

Because some employee turnover is inevitable, executives and employees should create process documentation regarding the fulfillment of all of their relevant duties. This is critical not only for new employees to understand an organization’s business processes, but also for auditors and regulators who inspect corporate records to ensure that document retention and disposition policies are enforced and followed consistently throughout the organization.

4.3.3.3 Technology

It goes without saying that achieving the state of sustained compliance via an integrated, enterprise-wide GRC strategy would be a more daunting task without the aid of technology. Technology provides the necessary basis for a seamless GRC and fluid work environment in any organization. Businesses across geographies and industry sectors have already experienced firsthand that inefficiencies related to suboptimal automation of business processes can have a significant negative impact on an organization’s profitability and competitiveness. Further, a piecemeal approach to addressing specific regulatory requirements using technology solutions adds IT applications layer by layer, thereby increasing the initial as well as ongoing costs and resources for an organization.

Leading organizations are utilizing an array of new and existing technologies to achieve sustained compliance. Although organizations may be able to use the tools currently in place, many are finding that more versatile technology solutions are necessary to meet GRC requirements. Such new technology solutions also aid in enterprise-wide congruency and process augmentation. Technology vendors have already developed a wide range of such solutions (see Section 4.4.3). These solutions, if implemented correctly, can provide the margin of difference between compliance success and failure, especially in large and complex organizations. Also, the process efficiencies and other related benefits obtained from implementing such solutions can rapidly offset their implemen-
tation costs. However, it is crucial that the developers and implementers of a GRC framework keep their eyes open to redundancies and complexities in processes and technology solutions—unnecessary elements that can actually negate otherwise constructive compliance efforts.

As organizations begin to implement GRC into their business cultures, no decisions should be made without taking into account all three of the interlocking components of compliance—people, process, and technology. The subsequent sections of this chapter focus on the role of technology and specifically one particular emerging technology solution—the ECM solution—in guiding an organization down the path of sustained compliance.

**4.4 ROLE OF TECHNOLOGY IN ACHIEVING SUSTAINED COMPLIANCE**

In today’s corporate environment, technology plays an essential role in addressing compliance issues. This section focuses on the critical and growing importance of information and related technologies in both addressing current compliance issues and as a powerful tool for forward-thinking managers seeking sustainable solutions for their organizations’ future compliance demands.

**4.4.1 The Relationship between Technology and Compliance**

A fundamental mandate in this new era of compliance is for organizations to reexamine and reengineer their underlying business processes. Once viewed as optional (and consequently piecemeal), rethinking and retooling are now comprehensive, embracing virtually every level of an organization: user access, inbound and outbound e-mails, reports, public relations, employee data, and every other source of information generation, transmission, flow, and storage.

Understandingly, such changes in business processes often require changes in the IT systems that support and enable them. Thus, compliance has generated a new and never-ending workload for IT departments. To complicate this process, compliance departments have traditionally operated under considerable IT constraints and have had little influence over IT strategy to achieve either their own objectives or those of the organization. Their involvement has usually been after the fact, only to ensure that whatever has been done was in compliance with regulatory requirements.
Due to this reactive defensive, rather than proactive offensive, approach of compliance departments, specialized technology solutions were not traditionally procured and implemented with the goal of enhancing the compliance function within an organization, with the notable exceptions of when such changes were required to meet a specific regulatory requirement or in response to a breach of a regulatory requirement. Not surprisingly, the resulting evolution of compliance-related IT has proven suboptimal in relation to the challenge, further exacerbating the process and costs associated with achieving tangible results.

The solution to this dilemma is emerging as the relationship between technology and compliance becomes increasingly evident. Today’s leaders in corporate compliance function proactively at an early stage in the development of enterprise-wide applications so that compliance requirements can be embedded in the business processes of the organization, leading to sustainable compliance.* Compliance managers are reinventing themselves in response to the urgent need to fulfill a more visionary, active, and influential role in the organization, thereby strengthening the relationship between compliance and IT at a strategic, as well as operational, level.

While it is critical for compliance managers to be actively involved in IT initiatives from an early stage, it is equally important to engage the IT department in proactively identifying opportunities based on clearly defined compliance processes. By so doing, such initiatives can leverage technology, both to improve controls and to enable compliance managers to spearhead truly effective compliance programs. Because the compliance function touches virtually every business process, and because many of the IT systems within an organization are disparate and poorly integrated, the challenge for IT professionals is often to leverage the organization’s existing IT infrastructure to the extent possible. Amidst such challenging conditions, the goal is to create a compliance management information system that secures, monitors, and preserves information from multiple systems (e.g., enterprise resource planning, supplier relationship management, customer relationship management, finance and accounting management, and human resources management) and to do so in a manner that minimizes compliance breaches and related shortcomings. Moreover, the compliance manager’s task does not end at the corporate front door; in the event of an audit, IT must serve to expose and present the organization’s information in the most accurate yet least incriminating way, which requires timely and sophisticated linkages of IT across the enterprise.

The preceding discussion highlights the fact that in this new era of compliance, IT professionals are faced with new, significant, and ever-changing challenges. However, current technology often does not offer IT managers the capability to adequately address compliance challenges presented to them, nor to efficiently perform compliance-related tasks. In the absence of technology designed to meet today’s compliance challenges, the goal of achieving a seamless enterprise-wide compliance interface often eludes even the most capable of today’s IT professionals. Oftentimes, IT professionals must interlace applications in an attempt to create compliance continuity across different departments. Additionally, while such programs are under way, IT is expected to maintain data integrity and security to protect against the misuses of such data, even including potential actions by disgruntled employees or administrators. Thus, while IT may not address all of an organization’s compliance needs, it is—and will remain—an integral part of an overall long-term compliance implementation program. This fact places technology squarely in the center of an organization’s compliance future.

4.4.2 How Does Technology Address Compliance Requirements?

The previous section illustrated how technology is an integral part of an organization’s overall long-term compliance implementation program. Without adequate and appropriate technology, companies would incur significant risks at all levels and expend inordinately high overhead costs attempting to staff a department solely for the tracking and management of organizational information. In this section, we will see how technology addresses compliance in a way that both systematically organizes data flow and cuts costs.

Technology helps an organization meet compliance requirements in the following ways:

1. **Efficient and effective business processes**: Technology instills confidence that in addition to reducing and automating business processes and cycle times, an organization’s policies, procedures, guidelines, and best practices are followed consistently across the board. While it is important to ensure consistency in business transactions, it is equally important to ensure that the meeting of compliance requirements does not reduce an organization’s efficiency or dramatically increase costs related to core operational functions. Technology helps translate this burden of compliance into a benefit for an
organization by embedding and systematizing compliance into the fabric of the organization’s culture, thereby leveraging the results of compliance implementation to provide greater visibility and transparency to senior management for key decision making.

2. **Single version of the truth**: Technology enables an organization to organize, monitor, and archive documents and information in a common repository or other integrated IT systems. This ensures that a single active version of each document (such as organizational policies, procedures, and contracts) exists and that prior versions have been correctly archived for future reference or audits. While the initial focus of most organizations has been on implementing some form of an ECM solution to achieve this single version of the truth, recent compliance requirements have caused a shift in focus. The focus has moved from content management to rigorous records management protocols, a more stringent approach to the management, retention, and disposal of critical business records. Technology solutions that provide such records management capabilities enable organizations to archive documents for efficient retrieval and viewing without placing them at risk of alteration. Such systems greatly foster automation of an organization’s policies and procedures regarding document retention and disposal. Furthermore, as new regulations have emerged on the corporate horizon, and as new requirements are added, IT solutions must continue to provide records management capabilities tailored to existing and newer forms of document retention and disposal (e.g., data generated and stored in electronic documents such as e-mails and instant messages).

3. **Collaboration and workflow**: Technology provides organizations with a digital work space that facilitates content collaboration between co-workers and business partners on documents, records, Web content, and other digital assets. This allows organizations to apply user-controlled document-level security limitations regarding access to generate, read, edit, or delete documents and information. It further provides the capability to track revisions of content including associated comments, e-mails, and discussions. In addition to facilitating collaboration, such technology also facilitates workflow management though the automation of structured business processes, transactions, and events. This includes routing of tasks, documents, and information from one user to another in a way that ensures compliance with an organization’s policies, procedures, and guidelines. Workflow
management results in streamlining and simplifying business process and in improving organizational efficiency, flexibility, process control, and procedural compliance.

4. **Secure and role-based access:** The advent of Internet-enabled IT solutions, intranets, and extranets has helped organizations make the transition from closed business models to more open and adaptive forms. While this has helped improve efficiency and productivity across organizations and geographies, it has also led to an exponential increase in the complexity involved with managing users and user access to systems and documents. To address this rapidly changing and complex issue, current technology provides role-based access to facts, figures, and business transactions, enabling the establishment, enforcement, and segregation of duties and access levels. Such technology increases the probability that users execute business events and transactions in accordance with their roles and responsibilities as they are documented and approved by upper management. Moreover, in such a system, no one person has total administrative control, but rather authority is distributed so that data integrity and confidentiality remain intact and locally monitored. No single person has the freedom to change information without appropriate authorization, knowledge, and understanding of the system as a whole. In addition to providing secure and role-based access to users within an organization, technology also enables maintaining an audit trail of all business transactions (i.e., tracking and recording critical information such as who made what changes, when, and where).

5. **Real-time monitoring and alerts:** Technology enables proactive and real-time monitoring of business transactions and data activity across multiple systems and locations, providing the capability to automatically alert administrators or authorized personnel to any abnormalities, exceptions, threats, or security breaches. This dramatically improves the capabilities of senior management to understand and respond to problems before they become showstoppers or outright compliance breaches. The net effect of such real-time monitoring capability is to significantly reduce the overall risk and the cost and time an organization spends in reparative versus preventive measures associated with data integrity and security.

6. **Real-time, reliable reporting:** The new era of compliance demands that organizations respond rapidly to evolving markets and changing supplier/customer dynamics. Analyzing such information requires
substantial analytical horsepower operating in real time, without which routine conduct of such analysis would be considered impossible given the complex IT infrastructure of most organizations. Such infrastructure is often an amalgam of application silos, each dedicated to separate divisional data populations, such as supplier relationship management (SRM), customer relationship management (CRM), supply chain management (SCM), finance and accounting management, and human resources management. Today’s IT enables rapid and seamless integration between such individually useful but often disparate and constantly changing data structures. When integrated correctly, such information silos turn into a comprehensive gold mine of information from which data can be rapidly extracted using today’s advanced analytics tools. These analytical tools facilitate development of business forecasts, optimization of resources on the fly, and recommendation of appropriate actions with unprecedented speed, agility, and accuracy based on near real-time reports, synthesis of previously submerged information via data mining, and other advanced techniques. Some of the newer IT tools also provide interactive analysis capabilities through which users can slice and dice extracted data and execute a wide variety of what-if scenarios and other higher level logical analyses, correlations, and forecasts. Thus, businesses are no longer restricted to using the rearview mirror technique for making critical decisions to respond to changing market conditions. They can now operate with greater agility, adaptability, and compliance by making informed decisions based on reliable real-time reports and supporting tools.

No single technology solution provides all the benefits mentioned above. Instead, organizations need to combine the functionality of several different technology platforms, some of which may already be in place and some that will need to be acquired. The goal of the next section is to shed some light on a variety of emerging IT solutions designed to assist organizations in addressing today’s compliance requirements and those that will undoubtedly arise in the future.

4.4.3 Technology Solutions That Are Being Used to Address Compliance Issues

Compliance management is a term that describes a rapidly maturing software category that combines applications and provides capabilities in integration,
collaboration, reporting, and monitoring. Software vendors in this space can be classified into the following segments:

1. **Compliance management specialists**: This category includes the best-of-breed software applications that were designed specifically to address compliance management within an organization. These applications automate the design, documentation, review, approval, and testing of an organization’s internal controls framework, thereby reducing the time to compliance and expediting audits. Some of the key vendors in this space are Certus, HandySoft, OpenPages, Paisley Consulting, and Stellent. Such vendors are expanding the functionality of their products to support broader enterprise risk management strategies. Since these products are relatively new to the market and have not completely achieved maturity, user-friendly functionality and integration with other enterprise-wide applications are still in development.

2. **Enterprise risk management (ERM)**: ERM solutions enable senior management to effectively prepare for both uncertainties and their associated risks as well as for opportunities for the organization to grow and remain competitive. Such solutions help identify, analyze, and manage the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. Since regulatory risks fall under the greater umbrella of enterprise risks, ERM solutions can be very effective and efficient in identifying and addressing compliance-related issues. Some of the key vendors in this compliance software space are Capterra, CSC, Methodware, Noweco, OpenPages, Paisley Consulting, Risk Track, and Vericept.

3. **Enterprise resource planning (ERP)**: ERP applications are multimodule software applications that enable organizations to manage a variety of business processes such as finance, controlling, SCM, product life cycle management, asset management, etc. This category includes vendors such as SAP and Oracle. SAP released its Management of Internal Controls solution in September 2004, while Oracle had released its Internal Controls Manager product in August 2003. The strength of these applications lies in their ability to integrate seamlessly with the other products in the suite of applications provided by the individual vendors. This seamless integration allows organizations to leverage their current configurations and master data, including security and access controls, from their ERP
applications. However, ERP systems have traditionally demonstrated poor integration with existing document management and records management systems.

4. **Enterprise content management (CM):** CM applications support the evolutionary life cycle of all digital information resources, such as images, documents, and text, from creation, review, storage, and dissemination to destruction. CM systems provide an infrastructure for the compliance framework, providing functionality such as enterprise search, electronic forms processing, scanning and imaging support, e-mail archiving, records retention, security and access control, versioning, audit trail, electronic signatures, spreadsheet remediation, check-in/check-out, and interfaces to archive content to permanent media. However, CM systems usually lack the functionality to assist in authoring standard business documents such as purchasing contracts, sales contracts, and service agreements, which should be developed using standard—and approved—clause language and contract templates. Some of the key vendors in this category are Documentum (recently acquired by EMC), FileNet, Interwoven, OmniRIM, Stellent, Vignette, and Xerox DocuShare.

5. **Financial control management (FCM):** FCM applications automate much of the day-to-day work performed in finance organizations to ensure that users complete all critical work in a timely and consistent manner and in compliance with regulations and organizational policies. This creates greater confidence in the production of financial statements. These applications record and produce evidence about control activities and financial control procedures, and detect and manage exceptions to resolution through review to disclosure, if applicable. Some of the key vendors in this category are Movaris and Cartesis.

6. **Business intelligence (BI) or business analytics (BA):** This is a broad category of applications for gathering, storing, analyzing, and providing access to data to help end users make better business decisions. By providing full, role-based access to financial information, these applications assist in establishing and enforcing standards for data retrieval, usage, and review across an organization. This secure and controlled access provides a basis for automating the financial review process, minimizing error-prone manual processes and solidifying the effectiveness of internal controls required to achieve compliance with numerous regulations. Some of the key vendors in
this space are Actuate, Business Objects, Cognos, Hummingbird, Hyperion, Informatica, SAS, and Siebel Analytics.

7. **Business performance management (BPM):** BPM applications are often touted as the next generation of BI applications. The concept behind BPM applications is that all aspects of business planning, operational and financial management, and performance management should be treated as an integrated platform. This is in contrast to the common approach of providing scorecards, analysis, and reporting as a set of disconnected applications. These applications emphasize the use of metrics beyond financial ones to guide business process management strategies. Some of the key vendors in this software category are Chordiant, Exigen, FileNet, Fuego, HandySoft, Hyperion, Insession, Plexus, Proforma, Savvion, and Ultimus.

8. **Business activity monitoring (BAM):** BAM applications specialize in monitoring transactions, applying controls in gaps between separate IT systems, and gaining access to data combined in stand-alone systems or blocked by proprietary software platforms that do not communicate well with other software applications. BAM applications can detect potential fraud and anomalies in financial process execution, which can provide additional assurance that internal controls are in place and can substantiate assertions for the SOX Section 404 controls evaluation. Some of the key vendors in this space are ACL Services, Active Reasoning, Akonix, Approva, Oversight Systems, and Tripwire.

9. **Business-to-employee (B2E) portals:** B2E portals are also known as employee relationship management systems. These portals are a customized, personalized mix of news, resources, and applications that simplify access to corporate information, personal data, transactions, and services. They enable employees of an organization to stay up-to-date with what is going on within the organization, from daily news and information to communications across all business functions around the world. Many organizations are increasingly using B2E portals today as a means to collaborate and communicate on compliance-related policies, standards, guidelines, and training. The portals enable the direction of compliance-related material, in text and video format, to targeted audiences and help improve awareness of the organizational and individual obligations to achieve compliance. Some of the key vendors in this software category are HP, Kronos, Microsoft, Oracle, SAP, Soffront, and Vignette.
10. **Complaint handling systems**: Although the function of complaint handling is closer to CRM, it is mentioned here because it can provide critical information associated with an organization’s compliance-related actions. For example, a complaint handling system can highlight the concentration of complaints by product or by region, along with applicable market indicators. Such information would be important in order to understand what type of regulation risks an organization might have to address so that remedial actions could be taken immediately. Several functionality-rich complaint handling systems are available in the market today from vendors such as Remetrex or Lynk Software. These systems provide strong workflow management, monitoring, and reporting capabilities. This functionality is also embedded in most advanced CRM tools such as the ones provided by Oracle, Right Now, Sales Logix, SAP, SAS, and Siebel.

11. **Issue management systems**: Issue management systems have been used for several years to record, track, and report issues with an organization’s enterprise-wide applications such as ERP, SCM, CRM, and SRM. However, their use within the compliance space has been restricted so far primarily because of the risk that such information may be used during litigation. Forward-thinking organizations that wish to become more proactive understand that they can deploy such systems to gather information in order to address and mitigate risks before they become major issues. Some of the key vendors in this software category are AutoTask, ExtraView, LinkEdge, Serena, and TrackStudio.

12. **Enterprise Contract Management (ECM)**: ECM solutions support the life cycle of all contracts within an organization, from contract creation, collaboration, execution, and administration to analysis and reporting. The capabilities of an ECM system overlap with those of many other software categories described above. For example, a major component of an ECM solution is document management, including records management and workflow management, which is the focus of CM solutions. ECM solutions minimize error-prone manual contracting processes, provide secure and controlled role-based access to contracts, and provide extensive reporting capabilities. In this respect, they share the capabilities of BI, BA, BPM, and BAM applications. These applications also integrate to a wide variety of existing enterprise-wide applications, such as ERP, ERM, SRM,
CRM, portals, etc. Some of the key vendors in this space are Accruent, Ariba, Contiki, Ecteon, Emptoris, I-many, Ketera, Nextance, Procuri, SAP, and Upside Software.

The remaining sections of this chapter describe the capabilities of ECM solutions and how such applications address the demands placed on an organization by a multitude of regulations discussed in previous sections.

4.5 ECM AND COMPLIANCE MANAGEMENT

ECM has profound potential for sustained compliance, especially in three critical areas:

- Procedural compliance
- Contractual compliance
- Regulatory compliance

By establishing an integrated ECM/compliance system, an organization not only instills a culture of compliance for present operations, but it lays the foundation for future compliance challenges and opportunities. Figure 4.6 illustrates the critical role that ECM plays in compliance management within, and across, organizational boundaries.

4.5.1 Procedural Compliance

As an organization continues to work toward the new vision of sustained compliance by adhering to its own operational and financial policies and procedures along with business conduct guidelines and standards, the organization is participating in procedural compliance. This is an organization’s attempt to self-govern and impose guidelines so that each transaction is in line with certain boundaries the organization has created to ensure success. Such procedures govern the type of sales an organization conducts, the type of vendors from which it procures goods and services, and the type of communication it makes available to both internal and external audiences.

Without ECM, companies face the tedious task of manually entering clauses that communicate the organization’s boundaries in each contract; however, unless a template is developed and made available to the contract authors, chances are the language used in the clauses will not be standard across the
enterprise. Each contract, therefore, requires meticulous review by designated individuals who are charged with ensuring and enforcing procedural compliance. This greatly increases the risk to an organization that uses several contracts and has limited staff to ensure their integrity. Furthermore, without a standard
contractual system, some employees may unethically take the liberty of executing their own contracts with unacceptable terms. This generates tremendous risk for an organization in many regards.

An effective and efficient ECM solution implements an organization-wide contract creation, approval, execution, monitoring, and analysis system, with appropriate templates for clauses, contracts, and notifications/alerts. These templates allow organizations to stay within their said procedures and reduce the time needed to both create and review the contracts. ECM solutions also manage contracts in such a way that other critical considerations such as budgetary constraints and corporate vision are included in the process of creating, executing, and monitoring contracts, and designated staff is alerted when these considerations are compromised.

4.5.2 Contractual Compliance

One of the biggest challenges facing CEOs, CFOs, and other senior managers is that of contract life cycle management. Contracts have life terms and stipulations that must be heeded to make them effective. This includes proper payment, reporting, and renewal. As contracts continue to determine things such as employment, sales, vendors, federal grants and loans, supplies, and more, they must be monitored so that both the organization and the party to which it is bound fulfill their responsibilities for mutual profitability. Furthermore, contracts must remain highly visible while remaining secure against unlawful access or changes.

ECM provides mechanisms for monitoring contractual stipulations as well as for securing the contracts themselves. Alerts can be issued when certain terms need attention, and methods for automatic payment and reporting take the managerial responsibility from staff. Systems may be set up to send contracts to certain staff automatically, and safeguards can be put in place so that only appropriate individuals can edit contracts and their terms.

ECM takes much of the burden of contractual maintenance from staff and automates it in an organized, efficient, and streamlined system that allows for much better contractual compliance and, overall, better profitability for the organization. As contracts are fulfilled by both the business and outside parties, companies face fewer audits and fewer instances of delinquent accounts.

4.5.3 Regulatory Compliance

Regulatory compliance is defined as compliance to mandates imposed by outside organizations or government. Contractual management must address regu-
ulatory compliance in great detail, as the consequences of not meeting such regulations are grave, resulting in costly penalties or even a cessation of business opportunity.

Organizations enter into various contracts regarding sales practices, property rights, employment stipulations, and other legal matters that outside regulators have determined. These types of contracts allow businesses to operate and thrive in their given industries. These contracts, in turn, require a certain level of awareness of their stipulations and clauses for either party to be successful. Noncompliance with regulations most often results in steep fines or restriction of service.

ECM addresses regulatory compliance in the most crucial of ways. In contrast to the high-maintenance properties of contracts, ECM allows organizations to incorporate several methods to ensure regulatory compliance, not only efficiently but in a proactive and consistent manner. As mentioned before, ECM allows any given organization to automate payments according to the demands of a contract without any other action required by staff. ECM may act as a calendar to address every segment of a contract’s life cycle, including its execution, review, payment schedule, and renewal. In the case of evergreen renewals, simple notices can alert executives that such renewal is about to occur in case they care to review the contract or other party’s performance. Given the far-reaching impact ECM solutions have in addressing regulatory requirements, it makes sense to dive deeper into this aspect of ECM.

4.5.4 ECM Solutions Address Sarbanes-Oxley Requirements

SOX, enacted in 2002, has arguably been one of the most stringent and far-reaching set of business regulations to ever be enacted on the corporate world. This regulation explicitly and directly affects all U.S. public organizations; however, its impact is being felt by smaller organizations as well, because the larger customers and suppliers of such smaller organizations have begun to assert control over their internal processes for all business activities. It makes sense to discuss the role of ECM solutions in addressing SOX requirements before jumping into the discussion of how ECM solutions address common requirements of most regulations. Table 4.1 describes how ECM solution capabilities enable an organization to address the requirements of different sections of SOX regulation.
### TABLE 4.1. How ECM Addresses Sarbanes-Oxley Act Requirements

<table>
<thead>
<tr>
<th>Regulation</th>
<th>How ECM Addresses the Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley Act Section 302: Corporate Responsibility for Financial Audits</td>
<td>Provides role-based access and information along with a rule-based engine to ensure that business processes set up by an organization (such as segregation of duties and approvals based on criteria such authority limits, material groups, divisions, etc.) are adhered to.</td>
</tr>
<tr>
<td></td>
<td>Ensures that executive-level staff of an organization has complete visibility to all new or amended contracts, controls, approvals, and transactions using automated e-mail notifications, alerts, and executive dashboards.</td>
</tr>
<tr>
<td></td>
<td>Delivers proactive and advanced alerts to appropriate personnel, highlighting exceptions that require specific filings or actions.</td>
</tr>
<tr>
<td></td>
<td>Provides audit trail and log to ensure accurate tracking.</td>
</tr>
<tr>
<td></td>
<td>Provides capabilities to ensure that revenue recognition rules are complied with systematically.</td>
</tr>
<tr>
<td>Sarbanes-Oxley Act Section 401: Disclosures in Periodic Reports</td>
<td>Provides capability for storing, searching, sorting, managing, and reporting contracts and related documents.</td>
</tr>
<tr>
<td></td>
<td>Provides functionality to search based on key fields such as vendor number, effective start and end dates, contract owner’s name, etc.</td>
</tr>
<tr>
<td></td>
<td>Provides functionality to add an unlimited number of custom fields which can be used by an organization to capture stakeholder information that may be deemed important.</td>
</tr>
<tr>
<td></td>
<td>Legacy data load utility programs allow an organization to pull its existing contracts with suppliers and customers into a central repository. This enables complete accounting of all the contractual relationships of an organization.</td>
</tr>
<tr>
<td></td>
<td>Integration of an ECM solution with ERP, SRM, CRM, and other enterprise-wide applications ensures that business transactions are conducted in accordance with negotiated terms and conditions listed in contracts.</td>
</tr>
</tbody>
</table>
### TABLE 4.1. How ECM Addresses Sarbanes-Oxley Act Requirements (continued)

<table>
<thead>
<tr>
<th>Regulation</th>
<th>How ECM Addresses the Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes-Oxley Act Section 401: Disclosures in Periodic Reports (continued)</td>
<td></td>
</tr>
<tr>
<td>• Provides reliable and real-time reporting with capabilities to report exceptions to approved business processes in a standard format.</td>
<td></td>
</tr>
<tr>
<td>• Allows exporting contract information and other related data (such as total quantity of goods ordered versus received, total number of purchase orders generated against a contract, total value of items ordered against a contract, sum total of invoices paid to date against a contract) to third-party reporting applications to meet the requirements of timely and accurate reporting.</td>
<td></td>
</tr>
<tr>
<td>• Delivers proactive, advanced, and varied alerts to appropriate personnel, highlighting exceptions that require specific filings or actions.</td>
<td></td>
</tr>
<tr>
<td>Sarbanes-Oxley Act Section 404: Internal Controls Report</td>
<td></td>
</tr>
<tr>
<td>• Each annual report shall contain an “internal control” report which shall:</td>
<td></td>
</tr>
<tr>
<td>□ State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting.</td>
<td></td>
</tr>
<tr>
<td>□ Demonstrate an assessment of the effectiveness of the internal control structure.</td>
<td></td>
</tr>
<tr>
<td>• External auditors need to attest to and report on the organization’s internal control report.</td>
<td></td>
</tr>
<tr>
<td>• Provides capability to configure contracting processes with the system along with flexibility to set up approval rules, workflow, notification triggers, alerts, and report schedules, which help establish, facilitate, and institutionalize internal controls across an organization.</td>
<td></td>
</tr>
<tr>
<td>• Customized workflow allows organizations to tailor the system in accordance with their contracting processes. This ensures and enforces consistent handling and routing of contracts and enables adherence to prescribed business rules and best practices.</td>
<td></td>
</tr>
<tr>
<td>• The document repository provided within an ECM solution ensures that all contractual documents are secured, stored, and archived in accordance with a document retention and disposition policy.</td>
<td></td>
</tr>
<tr>
<td>• User roles that define who can do what in the system, along with approval rules based on delegation of authority, ensure appropriate segregation of duties.</td>
<td></td>
</tr>
<tr>
<td>• Maintains an audit trail for each business transaction that includes details such as who, what, when, and how. This enables attestation that internal controls are being complied with.</td>
<td></td>
</tr>
<tr>
<td>Regulation</td>
<td>How ECM Addresses the Requirements</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| **Sarbanes-Oxley Act**  
Section 409: Real-Time Disclosures  
- Issuers shall disclose to the public on a rapid and current basis additional information concerning material changes in the financial condition or operations of the issuer, which may include trend and qualitative information and graphic presentations, and may be deemed as useful or necessary to protect the investors or in the public interest.  
- Provides standard (or out-of-the-box) reports to assist with SOX reporting. Also enables creation of custom and ad hoc reports that assist in managing, monitoring, and tracking supplier/customer performance against negotiated terms and conditions.  
- Provides rich reporting and analytics tools.  
- Capable of integrating with an organization’s existing reporting engine.  
- Provides several standard reports and capability to generate ad hoc reports.  
- Provides role-based reporting and/or dashboards.  
- Provides standard reports to monitor and ensure effective use of clause templates and contract templates in the contract authoring process.  
- Supports analysis of contracts based on negotiated terms.  
- Sends notification (exception reporting) to appropriate person to highlight any unusual or suspicious accesses based on predefined triggers.  
- Provides capability for storing, searching, sorting, managing, and reporting contracts and related documents.  
- Provides mechanism to execute document retention and disposition policy.  
- Maintains an audit trail for each business transaction that includes details such as who, what, when, and how.  
- Provides elaborate redlining, audit trail, version tracking, and document check-in and check-out capabilities to meet an organization’s auditing and reporting requirements.  
- Supports secure electronic signatures. |
4.5.5 ECM Solutions Address Common Requirements of Multiple Regulations

The previous section presented the role of ECM solutions in addressing requirements of SOX regulations. However, it is imperative to remember that ECM solutions (or for that matter any technology solution) should not be implemented to address specific requirements of a specific regulation. The regulatory environment is changing rapidly in terms of the number of regulations and their requirements and complexity. Therefore, instead of focusing on the letter of the law, the goal of every organization should be to achieve compliance with the spirit of the law. Only then will an organization stay ahead of the curve regardless of the new regulatory requirements or changes to existing regulations that may occur. With this in mind, Table 4.2 presents a discussion of how ECM solutions address the common requirements of multiple regulations or, in other words, how ECM solutions help organizations achieve compliance with the spirit of the law.
### TABLE 4.2. How ECM Solutions Address the Common Requirements of Multiple Regulations

<table>
<thead>
<tr>
<th>Requirement</th>
<th>How ECM Addresses the Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process focus</strong></td>
<td>▪ Supports contract life cycle end to end</td>
</tr>
<tr>
<td></td>
<td>▪ Supports other parties’ paper process</td>
</tr>
<tr>
<td></td>
<td>▪ Supports creation of multiparty contracts</td>
</tr>
<tr>
<td></td>
<td>▪ Supports integration with precontracting processes such as RFQ, RFP, RFI, etc.</td>
</tr>
<tr>
<td></td>
<td>▪ Supports multiparty participation in contract review and refinement via e-mail, fax, or online</td>
</tr>
<tr>
<td></td>
<td>▪ Configuration options allow setting up an organizational structure within the software that mimics the real-life organizational hierarchy</td>
</tr>
<tr>
<td></td>
<td>▪ Ability to assign users in roles and departments and set up approval rules to enable desired workflow, approval flow, and e-mail notifications</td>
</tr>
<tr>
<td></td>
<td>▪ Supports planning, scheduling, and controlling resources required during different phases of the contract development process</td>
</tr>
<tr>
<td></td>
<td>▪ Enforces approval rules at clause level as well as contract level</td>
</tr>
<tr>
<td><strong>Content and document management</strong></td>
<td>▪ Provides real-time visibility across functions or geography based on security roles and permissions assigned to any user</td>
</tr>
<tr>
<td></td>
<td>▪ Provides capability for storing, searching, sorting, managing, and reporting contracts and related documents</td>
</tr>
<tr>
<td></td>
<td>▪ Provides mechanism to execute document retention and disposition policy</td>
</tr>
<tr>
<td></td>
<td>▪ Provides functionality to search based on key fields such as vendor number, effective start and end dates, and contract owner’s name</td>
</tr>
<tr>
<td></td>
<td>▪ Allows expanded search based on any other contract attributes</td>
</tr>
<tr>
<td></td>
<td>▪ Provides capability to add as many user-defined fields as required</td>
</tr>
<tr>
<td></td>
<td>▪ Provides functionality to link documents together or create a parent-child hierarchy between documents (for example, master services agreement linked to compensation agreement or a scope of work agreement)</td>
</tr>
<tr>
<td></td>
<td>▪ Provides functionality to perform mass changes to master data or contracts (for example, updating the internal contact on all records that meet particular criteria), and provides extensive audit trail functionality for any changes made to the data or documents in general</td>
</tr>
<tr>
<td>Requirement</td>
<td>How ECM Addresses the Requirement</td>
</tr>
<tr>
<td>-----------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Mechanism to enforce and ensure use of standards, rules, and best practices** | - Allows the contract author to use the results of precontracting activities to create a new contract  
- Allows configuring users, user groups, security roles, and permissions to support specific access-control-related business requirements  
- Provides the functionality to develop a template library (clause templates, contract templates, and e-mail notification templates)  
- Allows a contract author to use alternate clauses (i.e., preapproved clauses that can be used in place of the standard clauses in the contract templates)  
- Provides assisted contract authoring functionality (i.e., a wizard that helps a user select and build the right contract based on answers supplied to a series of questions)  
- Provides functionality to create amendments and link them to the original contracts  
- Supports integration with word-processing applications such as Microsoft Word and to spreadsheet applications such as Microsoft Excel  
- Supports integration with project planning and scheduling software such as Microsoft Project or Primavera  
- Supports multiparty participation in contract review and refinement via e-mail, fax, or online  
- Capability to support and manage life cycle of all types of contracts (for example, sales agreements, lease agreements, maintenance or service agreements, intellectual property agreements)  
- Enforces approval workflows at clause level and contract level to ensure compliance with appropriate industry-specific or local, national, or global regulations  
- Enables alerts and/or workflow triggers based on specific contract milestones, such as effective end date, next review date, volume thresholds, payment schedules, etc.  
- Provides standard reports to monitor and ensure effective use of clause templates and contract templates in the contract authoring process  
- Provides prebuilt adaptors and graphical user interface (GUI) integration tools for linking to existing enterprise systems  
- Provides real-time integration with other procurement-specific systems, such as SRM, supplier portal, enterprise spend management, e-procurement, e-sourcing, and ERP |
### TABLE 4.2. How ECM Solutions Address the Common Requirements of Multiple Regulations (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>How ECM Addresses the Requirement</th>
</tr>
</thead>
</table>
| **Mechanism to enforce and ensure use of standards, rules, and best practices (continued)** | - Supports integration with applications that manage associated financial processes, such as invoice verification and payment and commitment management  
- Provides utility programs for loading master data such as product data, vendor data, vendor contact information, and user data  
- Provides functionality to load legacy contracts automatically  
- Provides localization capabilities (i.e., multiple languages, multiple currencies, different date and currency formats) |
| **Accountability** | - Allows configuring users, user groups, security roles, permissions, and approval rules to support workflow and approval process per business requirements  
- Provides capability to track cycle time of contract life cycle, along with the ability to identify bottlenecks in the process |
| **Audit trail** | - Provides sufficient redlining, audit trail, version tracking, and document check-in and check-out capabilities to meet an organization’s auditing and reporting requirements  
- Captures the following:  
  - Who: Who accessed the data?  
  - What: What tables, columns, records, fields, and file attachments were accessed?  
  - When: When was it done?  
  - Where: From what location (IP address) within or outside the network?  
  - How: From which part of the application was the change made?  
  - Result: Was the change successful? Was the query/report successful?  
  - Exception reporting: Sends notification to appropriate person to highlight any unusual or suspicious accesses based on predefined triggers  
- Provides functionality to track contracts related to capital projects by project phase or milestones  
- Provides functionality to track actual versus planned time and costs for different phases of the contract development process  
- Provides standard reports to monitor and ensure effective use of clause templates and contract templates in the contract authoring process  
- Supports secure electronic signatures |
4.5.6 Lessons Learned from Initial ECM Solution Implementations

It is evident from our discussion in the previous section that ECM solutions are powerful tools that offer enhanced capabilities to manage all stages in the life cycle of contracts. If deployed correctly, use of such solutions can lead to superior visibility; procedural, contractual, and regulatory compliance; and an overall improvement in competitiveness both within and beyond the organization. It is therefore of great importance to discuss the lessons learned from past ECM implementations in the context of achieving sustained compliance to promote recurrence of successful outcomes and to preclude the recurrence of unsuccessful outcomes. Listed below are some of the key lessons learned from the first wave of ECM solution implementations:

- **Silo-ed implementations**: Historically, many organizations have missed “the big picture” regarding ECM initiatives and their role in compliance management. Often, organizations fail to align their ECM initiatives with other enterprise-wide programs, treating ECM implementation in a “silo-ed” manner rather than making it an integral part of an overall enterprise-wide compliance initiative or an even bigger GRC framework. A related shortcoming of past approaches has been to treat ECM solutions separately from the contract life cycle management process improvement initiative. Managers must
realize that, in and of itself, ECM is not a silver bullet. The true return on investment of an ECM initiative is best viewed and enacted within the broader context of the contracting process, with a view toward a fully integrated system.

- **Project-focused implementations**: Several organizations have treated their ECM solution implementation as a one-time project. They approached the implementation with the idea of using technology to achieve compliance with one or more specific regulations, but did not take this opportunity to analyze, redesign, and optimize the underlying contracting processes. When technology is used to automate suboptimal business processes, it merely results in bringing what is wrong in the processes to the surface much more quickly than manual processes do. Thus, while the approach of implementing ECM as a one-time project may be successful in the short run, this success—and ultimately compliance—cannot be sustained in the long run unless compliance is embedded in the culture of the organization by using repeatable, sustainable, efficient, and effective contract life cycle management processes.

- **Functional-group-focused implementations**: It is understandable that organizations need to learn how to walk before they can start running. Some of the early adopters of ECM implemented the solutions for the procurement function; others implemented it for sales or human resources or for managing real estate or intellectual property contracts. However, the ECM solution implementation was treated as a project with a definite start and a definite end; once the software application was installed and ready to use by the first functional group within the organization, members of the implementation team were sent back to their routine jobs of contract author or contract administrator. Instead, organizations should continue to roll out the chosen ECM solution to other organizational functional groups that were not included in the initial rollout. Only when ECM solutions are embedded deeply and across the entire organization can compliance be sustained.

- **Stand-alone implementations**: Compliance with regulations requires the ECM solution to talk to multiple applications, such as ERP, SRM, CRM, etc. However, most early adopters of ECM solutions did not integrate them with other enterprise-wide applications. This led to swivel-chair integration, where the end users would log in to one application to retrieve some data about a transaction, then either
toggle to the ECM solution on the same workstation or move to a
different workstation and enter the same data in the ECM solution.
This results in errors and discrepancy in data. Instead, organizations
should integrate their ECM solution with ERP, SRM, CRM, and
other enterprise-wide solutions to get the maximum benefit from
their investments.

- The paradox of compliance: Another frequently misunderstood area
  is the “paradox” of compliance; going above and beyond in regula-
tory compliance usually results in lower overall costs compared to
doing the bare minimum to comply. This is because there is a sig-
nificant overlap between multiple regulations (e.g., Basel II and SOX
Section 409 both require timely disclosure of material changes in
operations and financial condition). ECM frequently has been de-
ployed in the past with the objective of addressing a specific regu-
latory requirement rather than a host of similar, if not identical,
requirements in one consolidated effort. This obviously has proven
to be an expensive and inefficient approach.

- Compliance with the “letter of the law”: ECM applications are often
  underutilized when management waits for regulatory bodies to pro-
vide direction and a road map for implementing processes and sys-
tems to achieve compliance. This situation has left many organiza-
tions in the uncomfortable position of having to create their own
interpretation of what a given regulation implies. Instead of focusing
on complying with the letter of the law, organizations need to im-
prove the underlying business processes to comply with the spirit of
the law.

- Lack of use of proven implementation methodologies: Several or-
ganizations did not use proven project management, change man-
agement, and continuous improvement methodologies while imple-
menting an ECM solution. This led to inefficient and ineffective
implementation, long lead times, and not enough buy-in from key
stakeholders. Once the ECM solution was implemented, many orga-
nizations did not use a continuous improvement approach (such as
Six Sigma) to keep moving the organization and its contracting pro-
cesses toward greater efficiency.

- Lack of direction and support from senior management: A final
  area of underutilization of ECM is related to fundamental manage-
ment communications. Oftentimes, those responsible for ECM imple-
mentation lack the support, guidance, and clear direction from upper
management regarding the relevance of ECM solutions and processes to the broader organization. This often leads to suboptimal implementation and failure to realize the full potential of a corporate culture of continuous improvement in the contracting process, the establishment of incentives aligned with the organization’s goals, and the ultimate attainment of sustainable compliance. The very lack of communication that gave rise to this suboptimal result often gives rise to problems in related areas such as instilling changes in the organization’s culture as it relates to compliance as a whole.

- **Beyond document management**: Many early ECM adopters have treated ECM implementations as a document repository implementation only. While this is one of the key components of an ECM solution, such applications provide much more functionality, for example capability to author contract documents using clause and contract templates. Most current content management solutions do not provide this capability which is at the core of ensuring and enforcing compliance. The other capabilities offered by ECM solutions should be used to ensure that they institutionalize, industrialize, and embed compliance at all levels within organizations.

The prospect of implementing an ECM solution can be daunting, especially for senior managers with limited familiarity in the world of contract management applications. It is understandable that a number of issues could arise in the implementation of such an application that could have a far-reaching impact on almost all functions within an organization. However, through a combination of sound planning, careful team building, good consultative support, and periodic evaluation of value added, the process of ECM solution implementation can be achieved with minimal risk and disruption to operations and a near-seamless conversion to superior control over this critical area of an organization’s information management systems.

### 4.6 SUMMARY

The intimate, complex, and potentially powerful relationship between ECM applications and compliance management was described in this chapter. This relationship is based on the fact that contracts are the very currency of compliance—they represent communications between individuals, organizations, and agencies that, woven together, form the fabric of a company’s relationships. To
the extent that ECM serves to promote and foster sustained compliance, the organization and its stakeholders benefit. Suboptimal or ineffective ECM, on the other hand, leaves a company ill-equipped to address the challenges of compliance and prevents it from taking full advantage of the many benefits offered by a proactive culture of compliance.

The three major domains of compliance for an organization—regulatory, procedural, and contractual—were outlined. Also discussed were the interrelationships between these domains and the demands these relationships place upon an organization—both internally and externally. These demands arise from the need to interact with the various agencies involved in establishing and monitoring compliance policy, the divisions within an organization that must work effectively to achieve sustained compliance, and the various vendors, customers, and business partners with which a company must interact in a compliance-friendly environment. The role of ECM in streamlining these relationships was emphasized, including the role of ECM as a tool in contract creation, approval, execution, monitoring, and analysis, utilizing appropriate templates, reporting mechanisms, and notifications of compliance activities as they relate to predetermined standards.

In point of fact, the extent to which ECM is utilized and implemented by an organization has a dramatic impact on every aspect of operations and financial performance. Underutilization or nonutilization of appropriate ECM applications leaves a company’s compliance framework incomplete, elevating regulatory risks, reducing competitiveness, and leaving opportunities for growth unrealized. The benefits of proactive implementation and utilization of ECM applications as part of an overall compliance initiative are numerous. They include enhanced contract visibility without sacrificing security, increased revenue and reduced costs, and streamlining of a company’s procedures, operations, and processes to achieve optimal efficiency and financial return.

The benefits of ECM implementation to an organization are best realized when ECM is viewed as part of an integrated compliance IT and management architecture versus viewing ECM and compliance as isolated—the silo perspective—or a mere repository for documents and data. Clearly, to be effective as a compliance-enhancing tool, ECM cannot operate in a vacuum, nor should it be viewed as a one-time fix. ECM-based compliance initiatives are of greatest benefit to an organization when they are implemented into an existing IT system and corporate culture with the recognition that “you must walk before you can run.” Only then, by embracing deeper and more powerful elements of ECM so that it works seamlessly with other IT applications (e.g., a company’s ERP, SRM, and CRM platforms), will a network of IT applications permit previously un-
available levels of control and continuity for an organization’s contracts and communications. Moreover, such a compliance system offers a new and powerful ability for an organization to address and respond to compliance requirements from multiple agencies and sources in a single coherent framework.

By properly implementing ECM into a company’s ongoing enterprise applications, policies, operations, and procedures, ECM can be a valuable and proactive force in positioning a company to deal effectively with the challenges of compliance today and tomorrow and in increasing the overall value of the enterprise for its stakeholders through instilling a compliance-friendly corporate culture.