

4

Information Management Compliance (IMC)

In the first three chapters, we provided a framework for understanding Information Management and for identifying and managing business records. In this chapter we begin to explore the core concept of the book, Information Management Compliance (IMC).

What Is Compliance?

Although the term compliance is most often associated with the legal world, understanding it solely as a legal term is too narrow. In a broader context, and in the context used in this book, compliance simply means to act in accordance with any accepted standard or criteria. The “accepted standard” can refer to any kind of criteria, including business goals, performance measurements, laws, regulations, or quality targets.

In a general sense, there are two basic elements to compliance, namely:

1. Determining what the criteria should be
2. Developing techniques (often called *controls*) to ensure that the criteria are followed

Compliance is also a specific discipline that is practiced within dedicated departments in many regulated organizations around the world. These departments focus on ensuring that the organization complies with laws, regulations, codes, and other sources of compliance criteria. According to the International Compliance Association, organizational compliance departments have five key functions:¹

1. To identify the risks that an organization faces and provide guidance on the identified risks.

2. To design and implement controls to protect an organization from those risks.
3. To monitor and report on the effectiveness of those controls.
4. To resolve compliance difficulties.
5. To advise the organization on risks, rules, and controls.

How Compliance and Information Management Fit Together

Although the compliance concept can apply to nearly any activity or department, in this book we are concerned with how to achieve compliance in Information Management.

IMC involves:

1. The development of Information Management criteria based on legal, regulatory, and business needs.
2. The implementation of controls designed to ensure compliance with those criteria.

To put it another way, IMC is a fusion of the Compliance discipline with Information Management activities. Although it may seem natural on one level to bring these two areas together, at most organizations Compliance and Information Management typically exist within different departments and exhibit very different cultures. Also, they often take fundamentally different approaches to the problem they are designed to address. That is, Information Management programs often take a *best practices* approach, while Compliance often is based on a *risk management* methodology.

Combining the Two Approaches

As each of those two approaches has strengths and limitations, organizations should employ the best of both in developing their IMC programs.

Information Management programs are typically developed with the objective of achieving a reasonable level of assurance that information will be effectively managed, with a minimum of overhead. Organizations try to achieve that objective by implementing a series of recommendations and practices that are

generally accepted as highly effective yet not inordinately costly—commonly called *best practices*.

A weakness with this approach is that there really is no single set of best practices that is applicable to all organizations. Further, changes in the economy, operating environment, and technology can make current best practices obsolete.

On the other hand, Compliance tends to take a risk management–based approach. This approach involves identifying the risks that an organization faces; evaluating the potential for damage represented by each risk; and addressing these potentials in a systematic manner.

Common risk factors that an organization typically evaluate when building Compliance programs include:

- The nature and complexity of its business
- The diversity of its operations
- The scale, volume, and value of its business transactions
- The quantities or kinds of litigation
- Regulatory environment and oversight
- The nature and magnitude of risk-related activities

Risk management has its own pitfalls, as it depends on the ability of the organization not only to identify all possible risks but also to gauge the likelihood that a particular risk will occur and how often, and determine the appropriate amount of time and energy that should be spent protecting the organization against each risk. Making these judgments and calculations can be very difficult, particularly when addressing “soft” risks such as the chance that a company executive is going to indiscriminately destroy documents related to a trial. In addition, calculating the costs of efforts designed to prevent such eventualities, such as training programs and investments in “corporate culture,” is also difficult. See the discussion of Total Cost of Failure (TCF) in Chapter 12.

This characterization of Information Management and Compliance is intentionally simplistic and does not capture the complex mix of strategies that most organizations employ in their Information Management and Compliance programs. The intent is to illustrate the need for organizations to use both best practice and risk management strategies in the development of their Information Management programs.

The process of IMC starts with a body of best practices and continues by adapting these practices to an organization's specific needs according to their unique legal, regulatory, business, and risk environment.

Sources of IMC Criteria

In Information Management, there are two broad categories of compliance criteria:

1. Criteria imposed on an organization from an *external* source such as a regulatory body. These include the following criteria:
 - **Laws**, such as Sarbanes-Oxley
 - **Regulations**, such as IRS and SEC Rules
 - **Industry standards** required by agreement or contract, such as ISO standards that must be followed when manufacturing products for export
2. Criteria voluntarily adopted or developed by an organization *internally*. These include such criteria as:
 - **Methods** developed internally or by industry associations, such as Total Quality Management™ or Six Sigma™, which companies adopt in order to improve internal operations
 - **Voluntary standards and codes** such as website accessibility standards for people with disabilities, published by the World Wide Web Consortium
 - **Operating procedures** developed and refined by an organization over its operating life because they are the most efficient, reflect the company's values, or simply because "that's the way we do things"

Establishing Your Compliance Criteria

Determining all of the criteria that your organization should (or must) comply with can be complex, especially if your organization is international (or subject to multiple jurisdictions) or is involved in many different lines of business. Table 4-1 shows some common examples of compliance criteria and the organizations that they affect.

Table 4-1: Organizations and Sources of Compliance Criteria

Type of Organization	Sources of Compliance Criteria
Commercial entities	Federal, state, and local laws and statutes governing business operations, such as tax laws and commercial codes
Government agencies	Government standards for performance, accountability, and reporting, such as those created by the U.S. Office of Management and Budget (OMB)
Public companies	Federal, state, and local laws governing the conduct of public companies, such as the Sarbanes-Oxley Act
Manufacturing companies	ISO 9000 series standards regarding manufacturing practices
Companies online	Web “privacy seals” such as TRUSTe, and privacy standards such as the Platform for Privacy Preferences, promulgated by the World Wide Web Consortium
Information technology companies	Technical standards, such as Department of Defense standards for electronic recordkeeping systems, and quality standards for suppliers to pharmaceutical companies

COMPLIANCE IS A PROCESS, NOT A PROJECT

Implementing new technology that has Information Management significance requires close attention to the ongoing compliance of the technology with criteria that support the goals of your Information Management program.

For example, many organizations embarking upon imaging projects (i.e., converting paper records to digital images) discover that there is far more to scanning and imaging than meets the eye. In fact, if done properly, the process may consist of numerous stand-alone activities—from proper document preparation, to the development of a comprehensible indexing regime, to a post-scan review to ensure complete capture and usability of the image. To get it right, organizations need to develop policies and procedures based on industry best practices or standards. These policies become the “compliance criteria” for making sure that employees know what to do to get it right every time, at every step of the process.

Continued

COMPLIANCE IS A PROCESS, NOT A PROJECT (*Continued*)

Thereafter, organizations must ensure that employees continue to get it right. Continued vigilance may require monitoring the actions of the employees, auditing to ensure that the captured images are of a high quality, and retraining employees regularly.

Unfortunately, companies have not been doing a good job in educating their employees on their IMC responsibilities. A 2008 Kahn Consulting survey indicated that, on average, only 15% of an organization's employees understand their responsibilities and how to fulfill them.²

If organizations think that the "imaging project" is over when the technology "goes live," they need to think again, because this attitude will likely mean an IMC breakdown is in their future.

In other words, compliance is a process, not a project.

Organizational Liability

YOU MAKE THE CALL

Which of the following information management compliance failures are true and which are false?

- A. Federal agency is ordered to shut down its websites because of a lack of security controls that allows original government records to be altered, deleted, and so forth.
- B. The Federal government will spend *billions* of dollars just looking for relevant information in a class action lawsuit.
- C. Stolen army computers containing army secrets can be purchased at a market across from the base in an Arabic country.
- D. Secret communications intercepted from known terror suspects, preceding the September 11 terror attacks, are purged before they are reviewed because of storage limitations.
- E. All of the above.

If you answered E you are correct. All are true.

A corporation can only act through natural persons, and it is therefore held responsible for the acts of such persons fairly attributable to it. Charging a corporation for even minor misconduct may be appropriate where the wrongdoing was pervasive and was undertaken by a large number of employees or by all the employees in a particular role within the corporation...or was condoned by upper management.

On the other hand, in certain limited circumstances, it may not be appropriate to impose liability upon a corporation, particularly one with a compliance program in place, under a strict respondeat superior theory for the single isolated act of a rogue employee. There is, of course, a wide spectrum between these two extremes, and a prosecutor should exercise sound discretion in evaluating the pervasiveness of wrongdoing within a corporation.

Federal Prosecution of Business Organizations, U.S. Department of Justice³

Organizations, as well as individuals, can be tried and convicted for breaking the law. There are many reasons why an organization could be found liable. In many cases, a company is taken to task because it failed to employ adequate policies, supervision, training, discipline, corrective action, or other controls designed to diminish the likelihood of wrongdoing. In these cases the problem is seen to be so systemic that the organization must be punished in order to provide restitution to those damaged by its failure, and to ensure that its practices change.

A legal principle or doctrine called *respondeat superior* is commonly used by the courts to determine whether or not an organization should be held liable for the illegal acts performed by, or the damages caused by, its employees. Under this doctrine, an organization can be held “vicariously liable,” providing that an employee’s actions “(i) were within the scope of his duties and (ii) were intended, at least in part, to benefit the corporation.”⁴ Many cases where organizations were held liable for the Information Management failures and bad acts of its employees are explored throughout this book.

When federal prosecutors are faced with fraud and other criminal activity within corporations, they consider a number of factors when deciding whether to prosecute the corporation in addition to the individuals directly responsible for the wrongdoing.

These factors, which are provided in a manual for U.S. federal prosecutors (quoted above),⁴ include:

1. The nature and seriousness of the offense.
2. The pervasiveness of wrongdoing within the corporation, including the complicity in, or condoning of, the wrongdoing by corporate management.
3. The corporation's history of similar conduct.
4. The corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents.
5. The existence and adequacy of the corporation's compliance program.
6. The corporation's remedial actions.
7. Collateral consequences, including disproportionate harm to shareholders and employees not proven personally culpable.
8. The adequacy of the prosecution of individuals responsible for the corporation's malfeasance.
9. The adequacy of remedies such as civil or regulatory enforcement actions.

A Case Study in IMC Failure: Morgan Stanley —

The importance of establishing a culture of information management compliance is particularly important in heavily regulated industries, such as the securities industry. The example of Morgan Stanley provides a microcosm of how not to address (and how to address) compliance issues.

The Coleman Case

Probably the most well known of Morgan Stanley's compliance problems arose out of the suit by financier Ronald O. Perelman against the investment bank arising out of its advice to the appliance maker Sunbeam in Sunbeam's purchase of Perelman's camping goods business, the Coleman Company. The focus shifted from the plaintiff's allegations of fraud to Morgan Stanley's discovery violations.

The plaintiff sought information from Morgan Stanley's internal files, including electronic mail, from the outset of the litigation. Although Morgan

Stanley instructed its personnel to preserve paper files relating to the suit, it continued its normal practice of recycling, and thus overwriting, its e-mail tapes after 12 months, despite an SEC regulation requiring that all e-mails be retained in an easily accessible format for two years. The court found that several certifications that Morgan Stanley made in the course of producing e-mails were false. For example, when it produced 1,300 pages of e-mails pursuant to a court order in May 2004, and certifying that it had produced all relevant e-mails, there were over 2,100 backup tapes that had not been searched.

Morgan Stanley continued to find additional backup tapes after certifying that it had found all relevant material, up through February, 2005. It also subsequently reported flaws in the coding for the search protocols they had written, resulting in an additional 7,000 e-mails to be reviewed. The court summarized Morgan Stanley's deficiencies as follows:

In sum, despite MS & Co's affirmative duty arising out of the litigation to produce its e-mails, and contrary to federal law requiring it to preserve the e-mails, MS & Co. failed to preserve many e-mails and failed to produce all e-mails required by the Agreed Order. The failings include overwriting e-mails after 12 months; failing to conduct proper searches for tapes that may contain e-mails; providing a certificate of compliance known to be false when made and only recently withdrawn; failing to timely notify CPH [plaintiff] when additional tapes were located; failing to use reasonable efforts to search the newly discovered tapes; failing to timely process and search data... or notify CPH of the deficiency; failing to write software scripts consistent with the Agreed Order; and discovering the deficiencies only after CPH was given the opportunity to check MS & Co's work and the MS & Co's attorneys were required to certify the completeness of the prior searches. Many of these failings were done knowingly, deliberately, and in bad faith.⁶

As a result of Morgan Stanley's actions, the court imposed a number of sanctions upon the company. First, the court elected to have a statement read to the jury detailing Morgan Stanley's discovery conduct. It also took the unusual step of reversing the burden of proof of some aspects of the case—Morgan Stanley was required to establish that it was *not* aware of fraudulent conduct and did not conspire with Sunbeam to defraud the plaintiff, instead of the

plaintiff being required to establish that Morgan Stanley did. The plaintiff would be allowed to argue that Morgan Stanley's concealment of its role in the underlying transaction could be considered evidence of malice, or evil intent, which could form the basis for punitive damages.

Even after the entry of this order, the plaintiff discovered more discovery problems. For example, other software problems, hitherto unmentioned, had further reduced the number of e-mails processed by Morgan Stanley. Further evidence of misleading and false statements and certifications were established by the plaintiff. More than 6,800 additional backup tapes were found. The court therefore granted, in part, the plaintiff's later motion for default judgment.

The net effect of these orders resulted in a \$1.58 billion jury verdict against Morgan Stanley. Although ultimately reversed by Florida appellate courts on other grounds, the case represents an example of how discovery issues can overshadow (and overwhelm) the underlying substantive issues in a case.

The IMC failures in the Coleman case magnified its impact. Because Morgan Stanley did not know where all of its backup tapes were, they were continually discovering new tapes. This continuing pattern of finding new tapes, along with their obfuscation, wore out the patience of the court and was a significant factor in the award of punitive damages (which accounted for over \$800 million of the judgment).

The opinions do not even touch on the direct costs to Morgan Stanley in undertaking the search. Untold man-hours were spent searching for the tapes and loading the tapes into the archive. If there was no record retention policy (the court opinions do not mention one), then the company and its attorneys would be forced to wade through useless information with no business value, or information that may have had value at one time but should have been disposed of. Dealing with backup tapes themselves as an archival medium imposes additional costs. Tapes are designed for recovery of computers, not long-term information storage. Trying to find relevant information on a tape is an arduous, time-consuming process.

Other E-Mail Challenges

Similar allegations by the Securities and Exchange Commission resulted in the payment by Morgan Stanley in 2006 of a \$15 million fine as a result of Morgan Stanley's failure to search for and produce e-mails in response to several SEC investigations between 2000 and 2005.⁷ The SEC alleged that Morgan Stanley

overwrote backup tapes and “made numerous misstatements regarding the status and completeness of its productions; the unavailability of certain documents; and its efforts to preserve requested e-mail.”

Failure to Monitor for Possible Insider Trading

About the same time, the SEC settled a proceeding against Morgan Stanley for failure to monitor trading by its employees with possession of material nonpublic information regarding Morgan Stanley’s clients. For example, as a result of miscoding and mislabeling, Morgan Stanley failed to monitor about 434,000 employee or employee-related accounts for trading in so-called “Watch List” securities. Thus, the SEC found that:

Despite the legal requirements to do so, Morgan Stanley, for years, failed to maintain and enforce adequate written policies and procedures to prevent the misuse of material nonpublic information by Morgan Stanley or persons associated with it. Due to a systemic breakdown in this critical compliance function, Morgan Stanley failed to conduct any surveillance of a massive number of accounts and securities. Moreover, Morgan Stanley’s written policies failed to provide adequate guidance to Morgan Stanley personnel charged with conducting surveillance, and there were inadequate controls in place with respect to certain aspects of Watch List maintenance.⁸

System Compliance Problems

In 2007, the SEC settled a proceeding with Morgan Stanley in which Morgan Stanley agreed to disgorge profits in the total amount of about \$6.4 million, and pay a \$1.5 million penalty, in connection with discrepancies found by the SEC in some of its trading systems.⁹ In some cases, the system embedded markups and markdowns in certain retail orders. In other cases, the operation of the system resulted in delays, in violation of their duty to execute certain orders immediately.

An interesting aspect of the Commission’s order was its description of the interaction between system programmers and compliance personnel. Although compliance officials had discovered some initial programming problems (which were corrected), Morgan Stanley “had no procedure requiring

Compliance's approval of changes to the market-making system by Information Technology personnel. As a result, Compliance's knowledge and understanding of specific programming changes, and their intended and actual effects, was either incomplete or non-existent." Although the programmers provided comments in plain English in their code, no one in either the Compliance, IT, or the business units reviewed the comments, which the SEC found might have prevented some of the failures.

To Morgan Stanley's credit, the SEC described several incidents where discovered problems were promptly acted upon. In December, 2004, an employee discovered some discrepancies in prices that should have been identical. Although the differences were sub-pennies, the employee brought the issue to the attention of an attorney, "who advised that the cause needed to be understood and resolved promptly." The employee made efforts to do so. About a week later, a trader noticed an unusual amount of profit (\$400,000) made in a few minutes of unusually volatile trading. He immediately brought the matter to the attention of his manager and system support personnel. By that afternoon, the problem was pinpointed, and the system code was changed to eliminate any markups or markdowns on the affected retail orders. Morgan Stanley also "immediately cancelled and rebilled the affected trades." In addition, Morgan Stanley "performed an internal investigation into the matter and enhanced its supervision and controls over the relevant trading technology." These remedial efforts were considered by the SEC in its settlement of the dispute.

In the settlement itself, Morgan Stanley agreed to the appointment of an independent compliance consultant to "conduct a comprehensive review of [Morgan Stanley's] automated retail order handling practices to ensure that [Morgan Stanley] is complying with its duty of best execution to retail customers' orders." The consultant would make recommendations for changes and improvements to Morgan Stanley's policies and make a report to the SEC. If Morgan Stanley disagreed with any of the changes, it would have to propose an alternative to achieve the same purpose. An independent distribution consultant would also be appointed to develop a plan to distribute the \$6.4 million disgorgement.

Conclusions

The above examples may unfairly portray Morgan Stanley as a poster child for information management compliance failures. In fact, as a multi-billion-dollar

enterprise heavily dependent upon information systems for its day-to-day operations, the company should probably be commended for having as few failures as it has. In particular, the actions taken upon learning of its system problems in December, 2004 indicate that a culture of compliance has taken strong root at Morgan Stanley.

The advent of the personal computer and its widespread use in business have brought information management issues to even the mom-and-pop business. The danger is that complacency can develop from an overreliance and unquestioning acceptance of the results of computer systems.

The lesson learned is that compliance failures can impose very real costs upon a company, and not only in direct monetary outlays; they can affect a company's reputation and may subject the enterprise to higher levels of regulatory scrutiny. The objective of this book is to help companies develop a culture of compliance where compliance issues do not occur, but if they do, they can be caught and fixed before they become compliance problems.

Notes

- ¹ International Compliance Association, "Compliance and the Regulatory Environment." Online at http://www.int-comp.org/doc.asp?docId=6920&CAT_ID=676
- ² "GRC, E-Discovery, and RIM: State of the Industry—A Kahn Consulting, Inc. Survey in association with ARMA International, BNA Digital Discovery and E-Evidence, Business Trends Quarterly, and the Society of Corporate Compliance & Ethics." Online at www.kahnconsultinginc.com/library/surveys.html
- ³ "Federal Prosecution of Business Organizations," Department of Justice Memorandum to Heads of Department Components and United States Attorneys, January 2003.
- ⁴ Ibid.
- ⁵ Ibid.
- ⁶ *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, No. 502003CA005045XXOCAI (Fla. Cir. Ct., March 1, 2005)
- ⁷ U.S. Securities and Exchange Commission, "Morgan Stanley Sued for Repeated E-Mail Production Failures; Morgan Stanley Agrees to Pay a \$15

Million Penalty and Undertake Reforms in Settlement,” Litigation Release No. 19693, May 10, 2006.

⁸ Order, In the Matter of Morgan Stanley & Co., Inc. and Morgan Stanley DW Inc., Admin. Proceeding File No. 3-12342 (Securities and Exchange Comm., June 27, 2006).

⁹ Order, In the Matter of Morgan Stanley & Co., Inc., Admin. Proceeding File No. 3-12631 (Securities and Exchange Comm., May 9, 2007).