IT Auditing *and* Sarbanes-Oxley Compliance

Key Strategies *for* Business Improvement

Dimitris N. Chorafas

CRC Press
Taylor & Francis Group

IT Auditing *AND* Sarbanes-Oxley Compliance

Key Strategies *FOR* Business Improvement

IT Auditing *AND* Sarbanes-Oxley Compliance

Key Strategies *FOR* Business Improvement

Dimitris N. Chorafas

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20131031

International Standard Book Number-13: 978-1-4200-8618-8 (eBook - PDF)

Contents

Preface

Written as a contribution to the accounting and auditing professions, this book brings under one cover two key strategies for business improvement: information technology (IT) auditing and Sarbanes-Oxley (SOX) compliance. Superficially, these seem to be strange bedfellows, yet they belong together for several reasons, not the least being that they both require

- Ethical accounting practices,
- Focused auditing activities,
- A functioning system of internal control, and
- A very careful watch by the board's audit committee and chief executive officer.

From the Bubble Act of 1720 to the Sarbanes-Oxley Act of 2002, the history of financial legislation is the *child of crisis* and of the inevitable complaints of those who were harmed by malfeasance. When new laws are voted into effect, or when rules and regulations change, the impact is felt by both

- The accounting profession, because accounting is the gatekeeper of financial information, and
- Information technology, particularly that part of it addressing account keeping and financial reporting, hence the need for IT auditing.

The text has been designed to give the reader a practical knowledge of modern IT auditing, all the way to compliance issues. The practical examples and case studies included in this book have been written with the hope that they may assist in raising the professional standards. Therefore, not surprisingly, the readership is principally auditors, accountants, and information system specialists at large. Because not all readers are necessarily versatile in internal control and audit prerequisites, Part I focuses on those issues that are needed to provide a level playing field.

Chapter 1 introduces the reader to the concept of internal control and explains how and why internal control and information technology correlate. As the text

demonstrates, a similar statement can be made in regard to internal control and auditing.

Case studies on the contribution of internal control to sound governance, particularly in connection to operational risk, have been included in Chapter 2. Design reviews are examined under the aspect of an internal control instrument, and internal control is treated not only as a feedback channel but also as the process that, to be effective, must be endowed with analytical capabilities.

The theme of Chapter 3 is auditing functions. Auditing is the systematic verification of books of account, vouchers, and other financial and legal records for the purpose of determining accuracy and integrity of accounting and record keeping, including IT records. As such, auditing involves the in-depth examination of financial and other reports by challenging the "obvious" and through proper understanding of the business under audit.

Originally, the purpose of an audit was to trace fraudulent transactions and accounting errors. Late in the 20th century, new functions began to make their appearance. Auditing theory and practice have developed at a rapid rate to include the audit of internal controls, operational risks, and information technology. This requires auditors well trained not only in accounting but also in economics, finance, law, and technology—acting in two capacities as both controllers and advisers. The Sarbanes-Oxley Act is taken as an example of the change that has occurred in terms of audit objectives and of compliance.

Audits, Chapter 4 points out, can be internally conducted by regular employees of the organization or externally by hired professional auditors. As this text suggests, whether auditing is internal or external, the auditors should be investigative, comply with the laws of the land, and do their work with diligence, accuracy, and integrity.

Chapter 5 deals with the responsibilities of the board of directors in connection with internal control and audit. It documents the reasons why internal and external auditors should not report to line management but, rather, to the audit committee of the board. This is the best way to ensure the auditors' independence of opinion and the transparency of results.

Part II presents the reader with real-life case studies in which the author had a role to play. As the principles and conduct of business have changed over the recent years, and as financial operations (including their immediate and further-out ramifications) have become more complex, the purposes of audits are now covering a far wider scope than they formerly did.

The subject of how information technology should be audited, from IT policies to procedures, is treated in Chapter 6. The case of technology risk is deliberately brought into perspective so that the IT auditor is made aware that, while the effect of technology is generally positive, there are also cases where IT may be a drawback or even a source of errors and fraud. Left to its own devices, technology risk may morph into legal risk.

The case study in Chapters 7 and 8 is based on the IT audit of a well-known credit institution, undertaken at the demand of the board. Chapter 7 presents the

bad news. The external IT auditor was asked by the bank's chairman and CEO to present an independent opinion. To do so, he conducted personal interviews with all senior executives and key IT team members, and gave them the chance to develop and defend their own views while

- Probing for weak spots in the systems specialists' reasoning, and in their work;
- Guiding them back to basic issues if they strayed off the path; and
- Helping them to keep things simple by thinking clearly, realistically, and creatively.

In contrast, the text of Chapter 8 reflects an adviser's job: a positive contribution by the external information technology auditor to the IT solution the institution needed to remain competitive. This part of the mission was characterized by intramural discussions in which the company's executives played a major role by coming up with suggestions. The Socratic method was at the kernel of IT auditing in this phase, while in the first phase (Chapter 7), the focal point was the bank's IT people, books, and deliverables.

The constructive approach followed in Chapter 8 continues in Chapter 9, which analyzes the underlying reasons for failures in IT projects and how they can be avoided. The case studies in this chapter are drawn from different industries. The intent is not to make the reader an instant expert in IT audit. Rather, the thoughtful discussion is intended to help the reader gain a general feel for what goes into an IT audit, including company politics.

Part III takes a different approach altogether. Its method is pedagogical, which has much to be said for it, but which differs from the case studies at the general management level presented in Part II. The chosen approach has been Cicero's method, which has the advantage of getting more deeply into an issue and focusing on questions, but also puts limits on their coverage.

Two themes have been chosen for Part III, each including technical issues for which an IT auditor can exercise his or her skills. Chapters 10 and 11 concentrate on some of the most critical technical questions concerning any information technology, where auditing functions must penetrate to the core of the subject matter. First the chosen subject is presented as "matter of fact"; then questions are raised—similar to the queries an IT auditor should be asking—to guide the reader's hand. In each chapter, the questions being asked on the IT auditor's behalf pertain to issues under discussion; this is not an all-weather-type IT inspection.

Chapter 10 discusses auditing problems closely related to system reliability and response time, i.e., issues that have complex technical and financial ramifications. It needs no explaining that—neither through paper records nor through remembrance—managers and professionals cannot hope to have all of the various data of their business at their fingertips at all times. Modern business relies upon information technology for support in a great number of daily operations, and this support

is conditioned by availability, reliability, and response time. Therefore, all three must be subject to established corporate standards, and they have to be regularly audited.

As Chapter 11 demonstrates, a similar statement is valid about the ways and means employed by the firm for enhancing security. An audit that centers on IT security must be polyvalent and, as such, it is characterized by a number of critical issues that include abiding by top management's security policies, sizing up situations where security is in doubt, appraising administrative controls, identifying weaknesses that hackers can exploit, assessing security risks despite all of the measures being taken, and planning and corrective action.

Part IV follows the conceptual framework of Part III in terms of conducting an examination, but its focal point is managerial auditing, with a focus on compliance. The Sarbanes-Oxley Act, which is presented to the reader in Chapter 3, constitutes the background scenario. Chapter 12 explains that the better approach to compliance rests on clear and unambiguous top-management policies and evidently involves a fair amount of IT.

The same chapter also brings to the reader's attention methods of approach that help to promote effective compliance. One is the corporate memory facility (CMF). All decisions, along with their rationales and their outcomes, must be registered and mined to serve in a wide variety of applications, ranging from compliance to decisions regarding extension of credit, contemplated investments, prevailing trends, profitability of operations, and more. Most evident, the CMF must be audited.

Moreover, as Chapter 12 documents, any implementation of information technology that does not employ a high quotient of knowledge engineering is one that costs too much and delivers too little. Therefore, the IT audit must examine the company's use of agents and expert systems. The results will be a reliable reference source on the state of the art of the firm's information technology.

While closely linked to the central theme of Chapter 12, Chapter 13 presents the reader with a "what if" scenario. This scenario is primarily related to the Sarbanes-Oxley Act and secondarily to technology, taking as a reference the actions of Enron, WorldCom, and Enron's banks. What if SOX legislation had passed the U.S. Congress in the late 1990s or even 2000? How might this have influenced the financial statements of Enron and WorldCom? What about the credits that banks extended to them, and the new financial instruments they designed for them? What kind of role might technology have played in averting these bankruptcies?

Behind these queries is the issue of compliance and, with it, management intent and management policies. The strategy of the aforementioned companies was one of deception, and it is safe to bet is that no tactical moves could correct such strategic flaws. In the end, both companies proved to be empty sacks, and as Benjamin Franklin wrote in his autobiography, "It is hard for an empty sack to stand upright."

Because all issues treated in this book's 13 chapters have a touch of normal human frailties as well as strengths, it has been a deliberate choice to use constructive criticism—but criticism nevertheless—in connection with the case studies. Like any other audit, an IT audit must establish in a factual and documented way which new problems confront the organization in regard to its information technology and its functions. Changes in both the operational risk factors and the impact of the unexpected must, in fact, be expected.

About the Author

Since 1961, **Dr. Dimitris N. Chorafas** has advised financial institutions and industrial corporations in strategic planning, risk management, computers and communications systems, and internal controls. A graduate of the University of California, Los Angeles, the University of Paris, and the Technical University of Athens, Dr. Chorafas is also a Fulbright scholar.

Financial institutions that have sought his assistance include the Union Bank of Switzerland, Bank Vontobel, CEDEL, the Bank of Scotland, Credit Agricole, Österreichische Länderbank (Bank Austria), First Austrian Bank, Commerzbank, Dresdner Bank, Demir Bank, Mid-Med Bank, Banca Nazionale dell'Agricoltura, Istituto Bancario Italiano, Credito Commerciale, and Banca Provinciale Lombarda.

Among multinational corporations, Dr. Chorafas has worked as a consultant to top management for General Electric-Bull, Univac, Honeywell, Digital Equipment Corporation, Olivetti, Nestlé, Omega, Italcementi, Italmobiliare, AEG-Telefunken, Olympia, Osram, Antar, Pechiney, the American Management Association, and a host of other client firms in Europe and the United States.

Dr. Chorafas has served on the faculty of the Catholic University of America and as a visiting professor at Washington State University, George Washington University, University of Vermont, University of Florida, Georgia Institute of Technology, University of Alberta, Technical University of Karlsruhe, Ecole d'Etudes Industrielles de l'Université de Genève, École Polytechnic Fédérale de Lausanne, Polish Academy of Sciences, and Russian Academy of Sciences.

More than 8,000 banking, industrial, and government executives have participated in his seminars in the United States, England, Germany, Italy, other European countries, Asia, and Latin America.

Dr. Chorafas is the author of 145 books, some of which have been translated into 16 languages.

Acknowledgments

My debts go to a long list of knowledgeable people who contributed to the research that led to this text. Without their contributions, the book the reader has in hand would not have been possible. I am indebted not only for their input, but also for their constructive criticism during the preparation of the manuscript.

Let me take this opportunity to thank John Wyzalek for suggesting this project, and Ari Silver for the editing work and production effort. To Eva-Maria Binder goes the credit for compiling the research results, typing the text, and making the camera-ready artwork.

Dr. Dimitris N. Chorafas
Valmer and Vitznau

MANAGEMENT CONTROL

I

Chapter 1

Internal Control and Information Technology

1.1 Internal Control Defined

Internal control (IC) is a formal system of safeguards established by top management to provide a feedback on the way a financial institution, industrial organization, or any other entity observes the board's and senior management's policies, plans, directives, and rules as well as the law of the land and regulatory requirements. This is in contrast to the *grapevine*, which is a feedback channel of hearsay. IC should be seen as a process:

- Promoting transparency,
- Enhancing communications, and
- Affecting all levels of personnel.

The competitive advantage of internal control is that it enables board members to supervise, and senior executives to manage, by tracking exposure to deviations from guidelines, programs, established courses of action, and regulations. Such deviations may increase in credit risk, market risk, operations risk, settlement risk, legal risk, or other exposures relating to transactions, assets, and liabilities as well as to fraud and other events due to breaches of security.

Beyond risks, internal control goals include the preservation of assets, account reconciliation, and compliance. Without any doubt, laws and regulations impact

on IC, whose able management requires policies, organization, technology, open communications channels, reliable information, access to all transactions, quality control, experimentation, and corrective action. The major aims of IC aims are to

- Promote personnel accountability and
- Keep open the arteries of corporate communications.

The development, implementation, and proper functioning of an internal control system require the existence of clearly stated internal bylaws and directives; a rigorous sense of supervisory activity; compliance with government regulations; and an organization that is flexible, dynamic, and appreciative of the need for management control (Chapter 5). Advanced technology is required to support IC efforts.

Not everybody, or every company, has the same definition of what is and is not internal control. This is documented by the opinion of 76 talented people in the financial industry, including central banks, commercial bankers, investment bankers, brokers, and representatives of trade associations that participated in the research. "The internal control definition," said the executive vice president of a New York brokerage, "should reflect the necessary segregation of duties, and it should stress the quality of management—two issues well beyond pitch-up reports."

In the opinion of David L. Robinson, of the Federal Reserve Board, internal control should in principle be content-neutral; but a system designed to serve IC should be commensurate with the complexity of the banking business that it supports. This is a sound principle to follow in regard to organization and structure, particularly when it is enriched with concrete and measurable objectives.

A senior executive at the European Monetary Institute (EMI), predecessor of the European Central Bank (ECB), looked to an IC system as the process (including all controls, financial or otherwise) effected by a credit institution's board of directors, senior management, and other key personnel to provide reasonable assurance that corporate objectives are achieved, including

- Safeguarding of assets
- Accomplishment of established goals
- Effective and efficient use of resources
- Adequate control of various risks incurred
- Reliability and integrity of financial reporting and of internal management information
- Compliance with laws and regulations, as well as with policies, plans, internal rules, and procedures

The definition of internal controls by the Institute of Internal Auditors (IIA) states that the term stands for actions taken by management to plan, organize, and direct the performance of sufficient operations so as to provide reasonable assurance

that corporate aims will be achieved. IIA's bullet points are very similar to those listed above by EMI.

The Committee on Working Procedures of the American Institute of Certified Public Accountants (AICPA) defines internal control as comprising the plan of organization—and of all coordinate methods and measures adopted within the business—with the objectives of safeguarding its assets, checking the accuracy and reliability of its accounting data and of its budget, promoting operational efficiency, and encouraging adherence to subscribed managerial policies.

Managers and executives from different branches of industry, who participated in this research, underlined the need for better tools than currently available to make internal control proactive, including IT-based tools and methods. "Most current tools are post-event," said Clifford Griep, of Standard & Poor's in New York, "but internal control must be proactive. It must deal with pre-transaction approval."

Some of the IC definitions recorded during the research meetings were broader than others because they incorporated budgetary control and feedback on standard costs, quality of work being done, operating results, statistical analyses, and more. The dissemination of such outputs was also a consideration. Additionally, some institutions divided internal control into two distinct but complementary parts. AICPA, for example, distinguishes between

- Accounting controls and
- Administrative controls.

Moreover, a number of financial institutions and regulators take IC as being part of risk management, while others make exactly the opposite statement. In reality, as Figure 1.1 demonstrates, up to a point, internal control, audit, accounting, and risk management overlap. But at the same time, each one of these functions has its own domain of specific characteristics.

Whatever the adopted IC definition and organizational solution may be, the surge in interest for internal controls is a direct result of senior management's decision to be in charge of the company's fortune. Top-tier control systems enable early detection of problems that, left alone or remaining undetected, lead to crises. A first-class IC also makes feasible more timely and effective damage control.

In conclusion, internal control is a dynamic system with feedback (and sometimes feed-forward) characteristics, covering all types of exposure, addressing fraud, assuring transparency, and promoting reliable financial reporting. The chairman, board members, chief executive officer (CEO), and senior managers are responsible and accountable for the proper functionality of internal control. Because even the best solutions and systems do not last forever, internal control must be regularly audited by internal and external auditors to ensure its rank and condition. Auditors should respond to the board's query about its status in the organization in a factual and documented manner. The audit committee (Chapter 5) must ascertain that

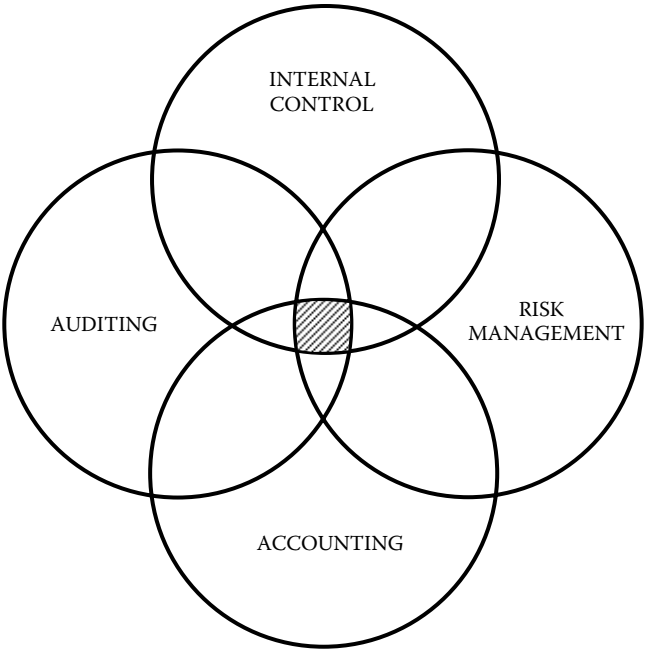

Figure 1.1 Internal control, internal auditing, risk management and accounting have a common core.

there is no cognitive dissonance at any level in connection to IC goals or duties and the way that these duties are carried out.

1.2 Internal Control and Service Science

The development of *service science* as a polyvalent but integrative field of management in the 21st century has greatly increased the need for effective internal control. The better way to appreciate the notion of service science is to start with a most basic query: What is meant by *service*? An orderly way of answering will look at fundamental issues underpinning the sense of conception, design, organization, and provision of a service, including its

- Nature
- Product characteristics
- Market offering
- Execution
- Profitability
- Feedback control

A couple of practical examples help in guiding the reader's mind. In 1882, journalists Charles Dow, 31, Edward Jones, 27, and Charles Bergstresser, 24, started Dow Jones & Co.—a service company. Its object was to pick up news and gossip and peddle them to brokers, bankers, investors, and speculators. Seven years later, in 1889, Dow Jones launched the *Wall Street Journal* (WSJ), another service product that came to life as a four-page stock-and-bond paper priced at 2 cents.

Throughout history, new services have been designed to cover a market need beyond what is addressed by existing services. One of the best recent examples is the emergence of Google on the Internet. Down to the bottom line, however, what counts most is *culture*. The offering of first-class services boils down to the people the firm employs, the responsibilities it assigns to them, the training it provides them with, and the way it rewards them for putting the firm's service interests above their own. Today, the component parts of service science are more complex than they used to be in previous centuries. They include

- Strategic planning
- Product and market studies
- Business partners
- Technical skills
- Analysis and experimentation
- Supply chain and logistics
- Quality assurance
- Internal control
- Information technology (IT)

Information technology became a branch of the service industry in the second half of the 20th century. Originally confined to number crunching and accounting, its domain has tremendously expanded. Among tier-1 firms, IT brings the concept of service orientation from the boardroom to the rank and file. Top-level IT tools promoting service science include

- Models
- Experiments
- Knowledge artifacts

(Because of its great importance in information technology, reference to *knowledge artifacts* is made in several parts of this book. This term, as well as the term *agents*, is defined in Chapter 12, to which the reader is referred in case he or she is not familiar with the aforementioned two concepts.)

Information technology assists internal control in delivering its messages, without delays, free of distortions, and at the right time. To enhance internal control, the better-managed companies use a wide range of methods, tools, and techniques, increasingly supported by real-time systems, sophisticated software,

data mining, simulation, analytics, and interactive visualization of engineering, financial, and other reports.

In terms of service science, IT makes a significant contribution to *logistics*, which has been an established discipline since Alexander's time, more than 2300 years ago. The blending of IT with logistics, including its implementation on the Internet, has delivered the benefits of supply-chain management involving (in a way) both the real and virtual worlds. Indeed, many experts look at this present-day version of logistics as the forerunner of service science.

Real-enough-time *management reviews* provide another example. The way an article in *Business Week* had it, Boeing could not have accomplished all of its Dreamliner's design and supply requirements on its own. Traditionally, the aerospace company micromanaged design and production of a jet's components, an approach that caused the budget of its previous plane, the 777, to double in cost, from $6 billion to $12 billion.

With the Dreamliner, many of the details of the plane's design have been handled by suppliers in Japan, Italy, and the United States. Tokyo-based Mitsubishi Motors created the wing, while Italy's Alenia Aeronautica produced the rear fuselage and horizontal stabilizer. Outsourcing, however, is subject to centrifugal forces, hence the need for

- Real-enough-time project control by management and
- Online real-time supply-chain-linked business partners.

In the case of Boeing's example, one of the keys to pulling off integrative supply-chain management was the company's careful attention to managing *cultural change*.* This made close collaboration with business partners and customers feasible while also improving the quality of deliverables, shrinking development time, and helping to keep costs down.

Part of the cultural change to which the preceding paragraphs refer center on the orientation of the user organization in implementing advanced IT solutions. Many participants in this research commented that it becomes increasingly difficult to derive returns from information technology investments if the chief information officer (CIO) is not at the same time

- A business innovator,
- A service-level designer, and
- An agent of disruption and renewal.

This is a demanding task, but it is also a personal opportunity. In the new order, which is slowly but surely defined by service science, the CIO becomes more than anything else a chief process innovation officer, whose responsibility is to think hard about all company processes, analyze the extent to which they further the

* *BusinessWeek*, May 14, 2007.

firm's competitive position, and project new IT solutions that bring the company ahead of the curve (more on this in Section 6).

1.3 The Proverbial Long, Hard Look

Building a sound system for internal control is synonymous with taking a long, hard look at how the business should be planned, conducted, and controlled. This has been the majority opinion of the cognizant people who contributed to the study leading to this book. Is a tough setting of internal control working against the growth in business? Lev Borodovski, of Crédit Suisse First Boston, mentioned a principle he learned at Fidelity, his former employer: "If it is done properly, internal control does not suppress business. It helps it."

Timothy Stier, of the Office of Thrift Supervision (OTS), sees internal control under the twin aspects of risk management and compliance, because there is regulatory risk. "We view internal control as the process that makes up for risk management by providing the nuts and bolts," said Curtis Wong, of the Federal Deposit Insurance Corp (FDIC). The FDIC places greater emphasis than ever before on internal and external audits, which

- Are part of internal control and
- Contribute to better risk management.

In regard to the OTS reference, like any other credit institution, the savings and loans have two exposures that may get out of control and bring an entity to bankruptcy. One is credit risk. Figure 1.2 provides a snapshot of the building blocks that should enter into the able management of credit exposure. Notice that the functions briefly described by all of them can be significantly improved through IT. The other major exposure is interest rates: a market risk.

After the well-known problems of the later 1980s, OTS has instituted an excellent procedure for interest-rate risk control. The 1100 thrifts it supervises must report daily their liquidity position ±100, ±200, ±300, and ±400 basis points over and below the current rate; the ±200 bp is the main reference. (A basis point is 1/100, or 1 percent). In this case, too, IT plays a pivotal role. Being in charge of credit risk and market risk is not an option. It is a matter of regulatory compliance. In both cases, internal control and IT are instrumental in enabling the institution to comply with this directive by regulators (Chapter 13).

However, as Section 1 brought to the reader's attention, because all systems can malfunction, and because they decay with time, both internal control and IT must be regularly audited. Well-governed companies see to it that this is written in their bylaws, and they also appreciate that IC's proper functioning is part of the board's and of senior management's desire to confront their responsibilities.

It takes teamwork to understand where the risks occur, and nobody can say that the worst stories that have happened to others in the past "couldn't happen to

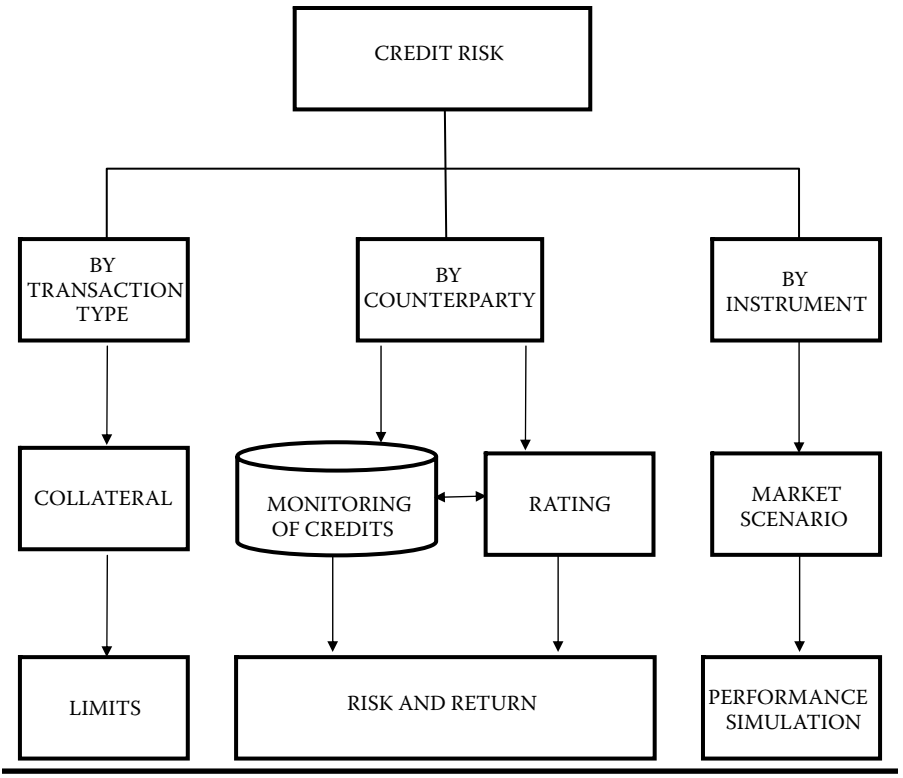

Figure 1.2 Building blocks of credit risk management.

us" in the future. Bear Stearns* probably thought so until adversity hit two of its hedge funds on June 20, 2007. Market risk is omnipresent, and any entity operating transborder is exposed to credit risk by counterparties it scantly knows.

Credit risk from unwillingness or inability to perform by counterparties as well as market risks from changes in foreign currency exchange rates, interest rates, leverage, and other reasons impact the entity's

- Cash flows,
- Financial position, and
- Results of operations.

Companies often manage their exposure to such market risks through derivative financial instruments. But even if derivatives are employed as risk management tools, and not for trading purposes, there are different types of exposures (frequently

* In early March 2008, after Bear Stearns ran out of both money and credit, JP Morgan Chase took it over, with the Federal Reserve acting as midwife and guarantour. The price was a paltry $2 per share, upped to $10. By late May 2008 the acquisition was completed and Bear Stearns ceased to exist.

covert) associated with assumed positions, which internal control should make transparent and bring to senior management's attention.

The principles that internal control and IT must be audited are honored by every well-governed company, although this is a recent development. By and large, until two or three decades ago, internal and external audits used to be verifications of the accounting system and of what was written in the company's books. Only enlightened persons had taken the position that internal control, too, must come under the microscope.

This is true of all entities, including the state. In a 1928 Supreme Court decision, Justice Louis Brandeis wrote in the case of *Olmstead v. United States*, "If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy." This concept is fully applicable to every company regarding

- Its accounts,
- Its compliance with laws and regulations, and
- The way in which its internal control system operates.

"The role of bank managers is not only to assure the proper function of their institutions, but also to see to it that auditors obtain a consistent and coherent image of status and results," suggested Alain Coune, of the International Monetary Fund (IMF). Coune added that this has become part of both internal control and audit. Quantification has been enriched with qualification by the Sarbanes-Oxley Act (see Chapters 3, 12, and 13).

This dual approach is vital because an organization's control environment is the corporate atmosphere in which accounting operates, internal control exists, financial statements are prepared, and critical functions are audited. In the opinion of a senior audit executive, a well-studied internal control puts a saddle on a horse that never had one. A strong control environment reflects management's consciousness of and commitment to an effective system of internal control that

- Does not guarantee the absence of fraudulent financial reporting,
- But reduces the chance that management will override internal and regulatory accounting controls. (As we will see in Chapter 13, this is only partly true.)

A weak control environment undermines the effectiveness of a company's internal accounting system, and may reflect a predisposition toward misinterpretations or errors in financial statements. In contrast, an effective internal control structure enlarges the bandwidth of internal communications and improves the understanding of the organization's policies and objectives.

For instance, banks usually take a one-way street to risk management because they find it difficult to integrate different skills into one system. They either hire rocket scientists who are good in mathematics but know nothing of trading, or they hire

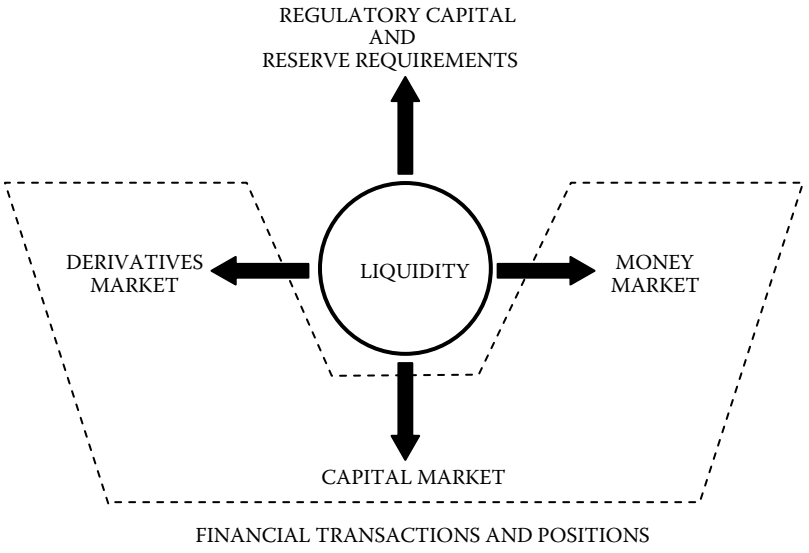

Figure 1.3 Four different dimensions of liquidity to be controlled intraday with results reaching top management through internal control.

ex-traders who grasp what makes sense in risk control, but who have no background in mathematical analysis. Contrary to this one-way street, organizations should be keen to merge trading and analytical skills, thereafter auditing the deliverables.

If the proverbial long, hard look is not very often in fashion in management circles, there exist some excellent positive examples. One of them is the conclusion reached by a 2005 blue ribbon banking committee under Gerald Corrigan, former chairman of New York Fed. In its conclusion, the committee differentiated between

- *Disturbances* as isolated problems and
- *Shocks* with systemic aftereffects.

Controls must be in place to register both and to differentiate between them. Frequently, the direct effect of shock is an increase in volatility, which, among other aftereffects, impacts negatively on investors' risk appetite. Another example is the disappearance, or near disappearance, of liquidity. As Figure 1.3 suggests, this impacts on financial transactions and positions.

- In the short run, there is no way to tell the difference between brief illiquidity problems and insolvency.*
- Therefore, liquidity must be controlled intraday through market data and feed-forward simulation.

* As Gerald Corrigan said in October 1987 to Alan Greenspan. See Bob Woodward, "Maestro: Greenspan's Fed and the American Boom," Simon and Schuster, New York, 2000.

The Corrigan Committee study also associated shocks with unexpected *tail risks* (of the assumed distribution of exposures) as well as to risk concentrations and risk contagion. These are issues addressed by a new generation of internal controls (see Section 4) that make good use of experimentation and whose information is boosted through stress tests.

(The Corrigan study identified relatively recent red zone shocks that greatly impact on financial stability: emerging market debt, of the mid-1980s; stock market crash of October 1987; debt instruments crisis of 1994; Asian Tigers crash of early to late 1997; Russian bankruptcy of August 1998; and LTCM's descent into the abyss in September 1998. The stock market crash of March/April 2000 provides another systemic risk example.)

1.4 Classical and New Internal Controls

Classical internal control issues included authorization for transactions, safeguards over assets and records, segregation of duties, documentation standards as well as verification duties, which tended to integrate internal control with auditing. Internal accounting control for industrial companies, merchandising firms, banks, and brokers included books and records of the firm's assets and liabilities, as well as segregated entries of customer property. The dual targets of such control have been

- Capital protection and
- Management compliance with existing rules and regulations.

The service economy has amplified these duties. As we saw in Section 2 on service science, in recent years the range of activities has been extended to cover new responsibilities that require both quantitative and qualitative judgments, for instance, on the degree of independence of different banking functions, including their relationships with

- Corporate governance rules and
- A growing range of compliance activities (Chapter 12).

Risks, too, must be controlled both quantitatively and qualitatively. Examples of quantitative measures are policies that pay adequate attention to risk limits and that ensure a rigorous process for measuring, evaluating, and instantly reporting exposures. In contrast, among other aims, qualitative controls put a premium on a strong control environment and make certain that the organization as a whole abides by ethical values.

One of the basic reasons why internal controls today play a more important function than ever is that the products and services offered by many service companies, credit institutions, and securities firms are becoming

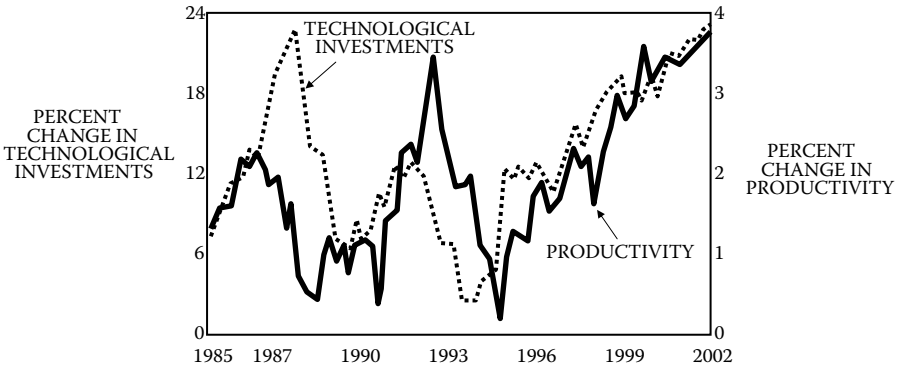

Figure 1.4 A pattern of non-farm labor productivity vs. technological investments in the United States. (2-Year annualized percent change. Statistics by bureau of economic analysis, Bureau of Labor Statistics).

- More complex and
- More exotic in their nature.

Precisely because of the growing complexity characterizing financial instruments and transactions, internal controls must produce not only words and numbers, but also patterns permitting one to judge, among other factors, individual and cumulative exposure. Patterns make it possible for every manager to be more confident when evaluating outstanding risk. As an example, Figure 1.4 presents a seven-year pattern of non-farm labor productivity versus technological investments in the United States.

Internal control and corporate governance correlate, because IC is a matter of *referential integrity*, addressing such questions as: How do we make sure our operations are clean of malfeasance and of conflicts of interest? How do we keep them clean? and other more personal queries. William McDonough, the former chairman of New York Fed, once said that corporate governance depends on more than a company's compliance with rules.

To a substantial extent, internal control is a matter of *management intent*. Management's *vigilance* and *virtue* make the difference between the chemists and alchemists of financial reporting and, by extension, the dependability of financial systems. Says Michael White in the biography of Sir Isaac Newton:

> The intellectual as opposed to the motivational foundations of chemistry and alchemy overlapped.… Chemists and alchemists dealt with the same compounds, even used the same apparatus and shared inherited knowledge; what lay between them was *approach* and *intent*.* (emphasis added)

* Michael White, *Isaac Newton, The Last Sorcerer* (London: Fourth Estate, 1997).