

The AuditNet® Monograph Series
Information Integrity:
The Next Frontier for Internal Auditors



by Madhavan Nayar
mnayar@infogix.com
Infogix, Inc.
www.infogix.com

AuditNet®

TABLE OF CONTENTS

AuditNet® Monograph Series - Guides for Auditors.....	3
I. Overview.....	4
II. The Audit Mission	6
III. Business Failures and Losses	8
IV. The Audit Challenge	11
<i>Accelerating Changes</i>	11
Increasing Complexity	12
The Information Mirror.....	14
V. Information Errors.....	15
Information Risks.....	15
Information Errors.....	16
Impact of Information errors	16
VI. Information Integrity.....	17
The Information Integrity Perspective.....	17
A Conceptual Framework.....	18
The Domains of Information Integrity	18
Attributes of Information Integrity	19
VII. Information Controls	20
Levels of Information Controls.....	20
Principles of Information Controls	21
Automated Information Controls.....	22
VIII. The Next Frontier.....	23
REFERENCES	24

AuditNet® Monograph Series - Guides for Auditors

This monograph series grew out of my desire to establish an online electronic communication network for auditors. Before online services, bulletin boards and the Internet many auditors were operating without the benefits of peer collaboration and information sharing on a major scale. The Internet, founded on the principle of sharing and communication, changed the interaction model between auditors. Auditors can now post messages in online discussion forums, upload and download audit work programs, checklists, surveys, questionnaires and other audit related material in warp speed. Small one-person audit shops can now communicate with others and feel like they are not paddling upstream with one oar when it comes to having access to audit resources. My vision of an online information communication network for auditors became a reality with AuditNet® as the foundation.

The AuditNet® Monograph Series or AMS provides auditors with guidance on different aspects of the audit process and other relevant topics to help them do their jobs. New auditors will seek these guides to learn some basics of auditing while experienced auditors will use them as a review. Each guide focuses on a specific subject.

If you have an idea for additions to the AMS please send a proposal via email to editor@auditnet.org .

Jim Kaplan, AuditNet®Founder and Principal

I. Overview

Information Integrity is the dependability and trustworthiness of information. More specifically, it is the accuracy, consistency and reliability of the information content, processes and system. The mission of the internal auditor is to assess and ensure the integrity of the business operation. Internal audit is a key element in the system of internal controls aimed at ensuring the viability, success and survival of a business.

The internal audit profession and the current set of audit standards and best practices have evolved over the past century. The internal audit practice consists of planning the audit based on materiality and risk exposure; performing the audit by assessing the systems, processes and people using audit guides, checklists and computerized audit test tools; and presenting the audit findings and recommendations to the audited departments and senior management.

The current approach to internal audit seems to have served well, until recently, the needs of management, investors and regulators. During the past two decades, however, we have seen an alarming number of massive financial losses and major business failures in countries with well-developed internal audit standards, practices and protocols. The exact causes of these losses and failures may be subject to interpretation and somewhat unique in each case. However, it appears that many of them can be attributed to some of the very same risks that internal auditors are supposed to have identified and prevented.

Auditors today face many challenges: accelerating changes in the business environment, increasing complexity of systems and technology and an expanding array of regulations and compliance requirements. The most important challenge, however, is a fundamental shift in the role of information. The 'physical' organization and operation – customers, suppliers, people, processes and resources- are becoming less and less visible, identifiable and accessible. Instead, they are represented by the information in corporate data warehouses, ERP systems and various data repositories. Information is rapidly becoming a surrogate for the real thing. Consequently, auditors have to define, analyze and assess the business through an 'information mirror', the representation of the physical environment in the information environment. The auditor's assessments, conclusions and recommendations will be only as good as the integrity of the information environment. The auditor, therefore, is a stakeholder in Enterprise Information Integrity.

The integrity of the information and information environment in most organizations today is often unclear, ill-defined or at best suspect. It will be necessary to have definitions and standards for Information Integrity and deploy an effective system of automated information controls to monitor, measure and maintain Information Integrity throughout the enterprise.

Information Integrity, as a concept and a field of knowledge, is still very early in its

evolution. The development, study and application of Information Integrity present a new frontier for the internal auditor. Perhaps it can dramatically change the audit paradigm and enable internal auditors to achieve their mission more effectively and efficiently in the 21st century.

II. The Audit Mission

The mission of the internal auditor in a business organization may be viewed as assessing and ensuring the integrity of the business operation. The dictionary defines 'integrity' as:

1. adherence to moral and ethical principles; soundness of moral character, honesty.
2. the state of being whole, entire, undiminished.
3. sound, unimpaired or perfect condition.¹

Integrity is an apt term in the context of the auditor's mission which generally concerns protection of assets, assessment of the efficient and effective use of resources, compliance with internal policies and external regulations, and assurance of the accuracy of financial and management information.

The history of internal auditing is perhaps as old as civilization itself.² The Mesopotamian civilizations, which existed about 3000 B.C., utilized elaborate systems of internal controls. Documents of that period contain ticks, dots and check-marks indicating the existence of the auditing function during those times.

The Bible contains an extensive discussion of internal audit functions in the modern sense.² It addresses limited access to assets, dual custody of liquid assets, surprise audits, care in selecting employees, and separation of duties. The Bible even explains the rationale behind such internal controls: the employees (i.e., agents) were likely to steal or misappropriate their master's monies if given an opportunity to do so.

The internal audit profession, as we know it today, has evolved over the past century. To a large degree, the profession is self-regulated and has taken the initiative to develop professional standards and codes of conduct. There are a number of national and international organizations as well, and cooperation among these has resulted in world-wide standards and best practices.

The scope of internal audit is broad and ranges from financial audit and compliance audit to assessment of results achieved (performance audit.) The assessment of the reliability of internal control systems is a major area of audit, and as organizations' operations are increasingly computerized, information systems (IS) audit has also become an important part of the internal audit work.

Audit professionals in most countries rely on certain concepts and frameworks such as control environment, internal control and internal audit.³ Control Environment provides the discipline and structure for achieving the objectives of the system of internal controls. Some elements of the control environment are integrity and ethical values, management philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices.

Internal control can be regarded as the system of processes that include all the

controls, financial or otherwise, effected by the supervisory board, senior management and other personnel to ensure that the following requirements are met: accomplishment of established goals and objectives, economical and efficient use of resources, adequate control of the various risks incurred and the safeguarding of assets, reliability and integrity of financial and management information, and compliance with laws and regulations, as well as policies, plans, internal rules and procedures.

Internal Audit is a special part of the internal control system. It is an independent assessment that provides objective information on the management and cost-effectiveness of business activities and operations, systems and built-in controls, economic and efficient and protective use of resources, integrity of financial and management reporting, and compliance with legal statutes and organizational policies and procedures.

The internal audit process in most organizations consists of planning of the audit, performing the audit, and follow-up on audit recommendations.

Planning for the audit is usually done by prioritizing the audit targets based on materiality and risk exposure. Materiality is a function of how reliable the system of internal controls is and procedures in place are considered to be. In addition, the auditors also try to take into account the vulnerability to loss through fraud, theft or mismanagement and the liquidity of cash and other assets managed. Damage to reputation and image is an extremely important risk, particularly for banks, insurance companies and other public institutions where the loss of credibility in the eyes of the public can have devastating consequences. Other criteria for selecting which areas should be audited include major changes in systems or organization, staff turnover, extent of decentralized approval authorities, the degree of computerization and any other known senior management or external auditor concerns.

The auditors review the internal control systems to ensure that they are working as intended. To do this, key system controls are identified in terms of economy, efficiency and compliance. Based on the evaluation of the existence and adequacy of these key controls, the auditors determine the level and type of audit testing required. The audit testing is done to ensure if the systems and procedures perform as they are specified to do. The testing may include that a sample of actual transactions are followed in detail on how they are processed. Sometimes the auditors also use sets of hypothetical transactions to do these kinds of tests. In order to clarify if a relevant and stable "audit trail" exist, computer audit programs or manual audit guides/or checklists are used in the analysis of the system and results in the identification of deficiencies or weaknesses and risks. The cause of the situation and the resultant effects are further investigated and recorded together with appropriate audit evidence to back up all conclusions reached. The audit report which documents the audit observations and recommendations is reviewed with the audited departments before it is finalized and submitted to senior management.

A good audit practice is to follow up on the extent of management action in

implementing measures which correct weaknesses identified in the audit report.

III. Business Failures and Losses

Internal audit is a rigorous discipline and a respected profession in the free economies of the industrialized world. Public corporations, government agencies, multinationals and other large organizations have policies, procedures and mandated internal audits consistent with the audit mission. Yet, during the past two decades, we have seen an alarming number of massive financial losses and major business failures in countries with well-developed internal audit standards, practices and protocols.

The exact causes of these losses and failures may be subject to interpretation and somewhat unique in each case. However, it appears that many of them can be attributed to some of the very same risks that internal audit is supposed to have identified and prevented. Let us look at some well-known examples:

Metallgesellschaft (December 1993). MG Refining and Marketing, a US subsidiary of Germany's Metallgesellschaft AG, had a program of selling long-dated fuel and oil supply commitments to end-users. These had embedded options designed to mimic for clients the optionality of holding physical supplies. MG used a "stack and roll" hedging program to hedge the long-term obligations with short-term futures. When oil prices dropped in the autumn of 1993, large variation margin calls on the futures caused liquidity problems. The firm turned to its banks for hundreds of millions of dollars in financing. Alarmed by the situation, Metallgesellschaft's supervisory board intervened, replacing the CEOs of both Metallgesellschaft and MG. They unwound outstanding positions at a \$1.3 billion loss.⁴

Orange County (November 1994): Orange County, California had an investment pool that supported various pension liabilities. The pool lost \$1.7 billion from structured notes and leveraged repo positions. The treasurer, Robert Citron, took the positions with oversight from the county's five-person board of supervisors. The riskiness of the pool's investments was publicly discussed when Citron ran for, and won, reelection in 1994. Members of the board of supervisors claimed that they did not receive critical information which would have indicated the risks that Citron was taking.⁴

Barings Bank (February 1995): Barings Plc lost £827 million because a Singapore-based trader, Nick Leeson, took unauthorized futures and options positions linked to the Nikkei 225 and Japanese government bonds. At the height of his activities, Leeson controlled 49% of open interest in the Nikkei 225 March '95 contract. Despite having to finance margin calls as the bank lost money, the Barings' board and management claimed to have been unaware of Leeson's activities.⁴

Daiwa Bank (September 1995): One of Daiwa Bank's US-based bond traders, Toshihide Iguchi, concealed \$1,100 million in bond losses over a ten year period. When management learned of the losses, they attempted to hide them from US regulators. Ultimately, Daiwa was forced to cease its US operations and was fined

\$340 million in a plea agreement with US prosecutors.⁴

Sumitomo Corp. (June 1996): Sumitomo's head copper trader, Yasuo Hamanaka, disguised losses totaling \$1,800 million over a ten year period. During that time, Hamanaka executed as much as \$20 billion of unauthorized trades a year. He was able to hide his activities because he headed his section and had trade confirmations sent directly to him, bypassing the back office.⁴

Cendant (April 1998): Executives at the former CUC International, now a part of Cendant Corp., "deliberately and fictitiously" manufactured about \$500 million in fake revenue over a three-year period in an attempt to ensure CUC's earnings matched analysts' expectations, according to an August 1998 report by Cendant's auditors. The irregularities came to light in April 1998. The disclosures sent Cendant stock into a tailspin and forced the resignation of Walter Forbes, former chairman and CEO of CUC, from his new post as Cendant chairman, along with eight other directors who had served under him at the former CUC. Based on hundreds of hours of interviews with more than 80 witnesses, the report cites "numerous" and "pervasive" instances in which CUC officials inflated earnings from 1995 to 1997. The report found that operating income at CUC had been inflated during the restatement period in 17 of 22 operating units. It said that while "numerous unsupported entries" were made by CUC subsidiaries, "the directions for the improper entries came from CUC corporate headquarters."⁵

Equitable Life of Great Britain (January 1999): Following an exhaustive inquiry that spanned more than two years and was subsequently compiled in an 818-page report, Equitable Life, which was founded in 1762, was found to have made exorbitantly large payments to holders of its with-profits policies (an insurance contract that shares in the profits of the insurance company) and nearly collapsed in 2000. To remain solvent, the company was forced to cut the pensions and retirement savings of policyholders. As a result, more than 1 million policyholders in the U.K. and more than 15,000 in other EU countries, notably Ireland and Germany, incurred massive losses to their pensions, savings and investments. Equitable Life launched a £4 billion (\$7.4 billion) legal action, seeking £2 billion from 15 ex-directors whom it claimed were negligent, and demanding a similar sum from former auditor Ernst & Young, claiming that it signed off on the company's accounts without warning of the problems that led to its collapse.⁶

Enron (December 2001): During the late 1990s and early 2000s, Enron was a trading powerhouse. The firm, which had started as a US natural gas pipeline company, started trading energies, then launched into new markets, including metals, paper, water, weather and bandwidth. For a time, it seemed that everything Enron touched turned to gold. The firm attracted some of the best talent, first from the energy industry, and then from Wall Street. In 2001, the Enron Empire collapsed. The firm's bankruptcy was the largest in US history, surpassed seven months later by WorldCom's bankruptcy.⁷

WorldCom (June 2002): In 2002, the Enron record was broken by the bankruptcy of

telecommunications firm WorldCom.⁸ In June of 2002, WorldCom announced that it would restate its financial results for all of 2001 and first quarter of 2002 to take almost \$3.8 billion in cash flow off its books, wiping out all profit during those times.⁹ Enron and WorldCom were just the two most prominent in a slew of bankruptcies and accounting scandals, which included Global Crossing, Tyco, Rite Aid, Xerox, and others.

Royal Ahold N.V. (February 2003): Management at Ahold, the world's third-largest grocer and owner of U.S. giant Stop and Shop, said in February 2003 that earnings for the previous two years were overstated by \$500 million at its U.S. Foodservice division, whose customers included restaurants, schools, and hotels. Ahold indicated that local managers booked much higher promotional allowances—provided by suppliers to promote their goods—than the company actually received in payments.¹⁰ In October 2004, Ahold settled Securities and Exchange Commission charges that its Columbia food distribution unit, U.S. Foodservice Inc., and other subsidiaries fraudulently inflated earnings by nearly \$830 million between 2000 and 2002.

The Ahold fiasco left securities regulators wondering whether the International Accounting Standards Board (IASB) model was any better than the U.S. Generally Accepted Accounting Principles (GAAP)—a system that critics say led to Enron, WorldCom, and many of the other high-profile frauds in the United States.¹⁰

Fannie Mae. (September 2003). The giant mortgage finance company used improper accounting methods that raised serious questions about the validity of its financial reports, government regulators reported. Though it didn't quantify the effect of what it called pervasive misapplication of accounting rules on the company's books, a report by the Office of Federal Housing Enterprise Oversight (OFHEO) cited one instance in 1998 where the company inappropriately deferred \$200 million of estimated expenses, which enabled management to receive full annual bonuses. Had Fannie recorded the expenses in 1998, no bonus would have been paid, the report said. Management at Fannie Mae "deliberately developed and adopted" inappropriate accounting policies, supported widespread violations of generally accepted accounting principles, tolerated lax internal controls and failed to properly investigate an employee's concerns about accounting, OFHEO's report said. The report also detailed numerous transactions over several years where it said Fannie Mae management intentionally smoothed out gyrations in its earnings to show investors it was a low-risk company. Fannie "maintained a corporate culture that emphasized stable earnings at the expense of accurate financial disclosures," regulators said in a letter to the company.¹¹

The findings echo those made the previous year about Freddie Mac, the other large government-chartered mortgage finance company. Regulators, who launched their Fannie Mae inquiry after the Freddie Mac problems came to light, found that Fannie Mae failed to follow the rules in accounting for complex financial instruments known as derivatives, which the company used to hedge against movements in interest rates. Much of rival Freddie Mac's accounting problems involved accounting for derivatives.

Parmalat (December 2003) Parmalat, an Italian company specializing in long-life milk admitted that the true level of its debt was €14.3bn (£10bn) - eight times more than it claimed. The questions began when Parmalat had difficulty making a €150m bond payment. The company, which had 36,000 employees, was supposed to have been sitting on €3.9bn in cash, so Italian bankers were puzzled by its predicament. Parmalat's problems quickly reached epic proportions after it made the extraordinary admission that the €3.9bn it thought it had in the bank did not exist.¹²

Investors have lost close to \$200 billion in the past half-dozen years in earnings restatements and stock meltdowns following audit failures. And the pace seems to be accelerating. Between 1997 and 2000, the number of restatements jumped 100%, from 116 instances to 233 in USA.¹³ Across the Atlantic, Europe is experiencing a similar phenomenon as evidenced by events concerning Equitable Life of Great Britain, Royal Ahold, Parmalat etc.

In the past, internal auditors have been able to provide reasonable assurance regarding the achievement of an organization's objectives because they either had the time to inspect and identify risks; processes, controls and problems were sufficiently isolated to prevent wide-scale losses and failures (due to the loosely coupled or discontinuous and physical nature of the business environment). However, these debacles demonstrate some fundamental shift in the business environment and the seriousness and urgency of finding new approaches and solutions.

IV. The Audit Challenge

Auditors today face many challenges: accelerating changes in the business environment, increasing complexity of systems and technology and an expanding array of regulations and compliance requirements. The most important challenge, however, is a fundamental shift in the role of information. The 'physical' organization and operation – customers, suppliers, people, processes and resources – are becoming less and less visible, identifiable and accessible. Instead, they are represented by the information in corporate data warehouses, ERP systems and various data repositories. Information is rapidly becoming a surrogate for the real thing. Consequently, auditors have to define, analyze and assess the business through an 'information mirror', the representation of the physical environment in the information environment. The auditor's assessments, conclusions and recommendations will be only as good as the integrity of the information environment. The auditor, therefore, is a stakeholder in Enterprise Information Integrity.

Let us look at these challenges in more detail:

Accelerating Changes

"We are entering an age of acceleration. The models underlying society at every level, which are largely based on a linear model of change, are going to have to be redefined. Because of the explosive power of exponential growth, the 21st century

will be equivalent to 20,000 years of progress at today's rate of progress; organizations have to be able to redefine themselves at a faster and faster pace," said Ray Kurzweil, inventor, entrepreneur, author and futurist.¹⁴

This rapid acceleration of change is manifested by the revolutionary trends in the business environment.

- Globalization of manufacturing
- Business process outsourcing
- Transnational mergers and acquisitions
- Privatization of many public sector activities
- Deregulation
- Rapid growth in access and use of the internet
- Emergence of internet-based businesses such as internet banking, e-commerce, etc.
- Doubling of the total volume of information every 24 months¹⁵

An important consequence of these changes is the necessity of relying on information from third-parties to operate, manage and monitor the business. This creates new challenges for the internal auditor.

Even more important is the fact that the pace of these changes is only going to accelerate even further in the future.

Increasing Complexity

Changes in technologies, new business models, increased business activity, mergers, consolidations, privatization, deregulation, etc. have resulted in significantly increasing the complexity of the business environments and the associated information systems and technologies supporting them. This complexity manifests itself in many forms affecting everything from the day-to-day operations of the business to senior management's strategic plans. Economies of scale, scope and skills appear to be wiped out by 'economies of complexity'.¹⁶

Complexity is a hidden cost of doing business.¹⁶ Complexity has created a many-headed monster for management. Excessive complexity typically grows over many years and fossilizes into structures, cultures, systems, and personnel that are not easily altered and examined. In the same measure, complexity poses significant challenges to internal audit's ability to provide assurance on the achievability of organizational objectives. For example, Citibank uses 28 different applications to support its deposit account process. It is almost humanly impossible to examine the integrity of each of these systems through traditional internal audit methods such as inspection of sampled data on a continuous basis. Much of Enron's debacle can be attributed to auditors' inability to understand and evaluate the complex structure of its special purpose entities (SPEs).¹⁷ For example, Enron securitized some of its assets through SPEs – examination of such transactions under FAS 140 is common

knowledge for the auditor community. However, such transactions became fairly complex and sources of confusion when Enron leased back some the assets that it off-loaded through the SPEs.

Modern enterprises operate in a connected economy. They constantly generate, use, store, and exchange information and materials with customers, partners, and suppliers. Enterprises are also required to exchange key performance information with the regulatory agencies and the shareholders. The connected enterprise can only be successful if it provides and receives the accurate information it needs in order to do business effectively. Trustworthy information reduces uncertainty in the decision-making process, enhances confidence, and improves operational effectiveness.

The internal audit community needs a framework and a set of tools to understand and examine the information flows within a complex environment in order to provide assurance over compliance and business objectives. The existing framework and tools are not adequate as evidenced by the number of business failures.

Expanding Array of Regulations and Compliance Mandates

Business failures, new political and economic policies and recognition of new types of threats and risks have resulted in a complex web of new regulations, standards and compliance mandates.

The Securities and Exchange Commission (SEC), in its recent study on Off-Balance Sheet Accounting, discussed the critical need to make accounting standards less complex.

Many of the material weaknesses noted in the first Sarbanes-Oxley Section 404 reports relate to misapplication of complex accounting standards.

The American Institute of Certified Public Accountants' (AICPA) recent task force found that current GAAP is too complex and not necessarily useful to the users of private company financial statements.

Financial Executive Institute's (FEI) Committee on Corporate Reporting (CCR) has frequently noted that the complexity of accounting standards is simply outpacing our ability to keep up.

As companies comply with the reporting requirements of Sections 302 and 404 of the US Sarbanes-Oxley Act, SAS70, Patriot Act and Basel II, internal auditors are coming to grips with their role and involvement in these initiatives.

"Compliance can be a time-consuming distraction of the internal auditor's focus from day-to-day responsibilities," said Dave Richards, president of The Institute of Internal Auditors. He added, "If this prevents the internal auditors from completing the audit plan, it leaves companies wide open to a vast array of other risks that should be

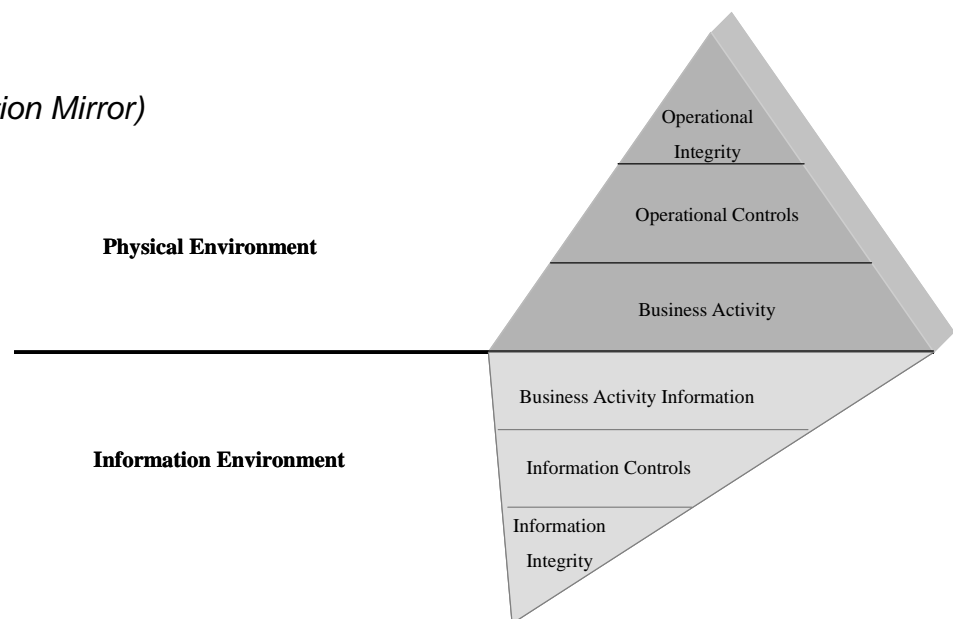
assessed and monitored.”¹⁸

The Information Mirror

With the advent of the industrial revolution, some 200 years ago, it became necessary to establish a system of operational controls to monitor business activity. The resources of the industrial age were tangible things that could be mined, processed, bought, sold, managed and easily understood,¹⁹ and the ‘physical’ organization and operation – customers, suppliers, people, processes and resources- were visible, identifiable and accessible. The task of the internal auditor was comparatively simple and straightforward.

With the advent of the information revolution, it became possible to process and store large quantities of data at a much faster rate. This allowed gathering of much more detail data about the physical environment. Today customers, suppliers, people, processes and resources are represented by the information in corporate data warehouses, ERP systems and various data repositories. Information is rapidly becoming a surrogate for the real thing. Consequently, the auditor has to define, analyze and assess the business through an ‘information mirror”, the representation of the physical environment in the information environment (*Fig. 1*)

(*Fig. 1. The Information Mirror*)



V. Information Errors

Information Risks

All business enterprises, especially large organizations within the financial services industry, receive, process, produce and store an amazing array of information to support and manage their operations, satisfy regulators and make important decisions. They use sophisticated information systems and state-of-the-art information technologies. However, their information environments are inherently susceptible to the risk of information errors. They are impacted by certain extrinsic and intrinsic risk factors.

The extrinsic risk factors are *Change, Complexity, Communication, Conversion* and *Corruption*.

1. **Change.** No organization is immune to changes in people, organizational structure, regulations, hardware and software. All such changes increase the probability of system failures and information errors.
2. **Complexity.** Information environments in organizations are becoming more complex due to increasing data volumes and processing speeds, distributed software and system interfaces and new functions and features demanded by business and regulatory imperatives. Complexity, by definition, introduces the potential for failure. Increased complexity increases the probability of information errors.
3. **Communication.** Widespread deployment of the internet and distributed processing and the availability of high-speed, high bandwidth communication links require the information environments of most organizations to share data across the enterprise and among partners. All such communications are susceptible to failed, incomplete or duplicate transfer of information and therefore information errors.
4. **Conversion.** Conversion of data from one format to another, from one medium to another or one system to another is an integral aspect of every information environment. All such conversions are susceptible to information errors due to deficiencies and defects in software and processes.
5. **Corruption.** Errors are introduced due to accidental system and process failures as well as deliberate and fraudulent alteration or tampering of systems, processes and data. All information environments are prone to accidental failures. Many are susceptible to fraudulent intrusions. Hence information error due to corruption is an inherent risk.

The intrinsic risk factors are *Design Errors, Development Errors, Deployment Errors, Detection Errors* and *Data Errors*.

1. **Design Errors:** Design errors are caused by incomplete or incorrect specification of requirements, faulty design reviews and walkthroughs and unanticipated environmental or other changes.
2. **Development Errors:** Development errors are caused by poor development methodologies and incomplete or incorrect testing.
3. **Deployment Errors:** Deployment errors are caused by inadequate or incomplete controls.
4. **Detection Errors:** Detection errors are caused by manual or automated controls which fail to detect information errors or which wrongly identify errors when they do not exist.
5. **Data Errors:** Data errors are caused by erroneous input and incorrect or incomplete edit and validation controls.

Information Errors

We are accustomed to information errors. We experience them firsthand in our dealings with our bank and insurance company or over the Internet. We read about them in newspaper headlines. We see and hear about them on television and radio.

Reports in the media are but tiny bubbles on the tip of a very large iceberg. Only a small fraction of the information errors that actually happen are reported. No company or organization wants its name associated with a mistake. For every error reported, there probably are hundreds more that are detected and corrected, but not reported. And for every error detected, there are many more that go undetected.

The fact is, information errors are a pervasive and insidious aspect of our personal, corporate, and social lives in the Information Age. Yet our attitude toward information errors can be described in three words: *awareness, skepticism and resignation*.

We are all **aware** that information errors occur. Most of us would like to believe or profess that they do not occur in *our* systems, in *our* databases, or in *our* companies. The fact is that they are everywhere.

We are **skeptical** that those errors can be prevented, or that there can be radically new ways to deal with them.

We are **resigned** to the presence of information errors. We accept it as a cost of doing business or as part of living in the Information Age.

Impact of Information errors

The reason for our resignation about information errors is our lack of recognition of

how much it is costing us. To the best of our knowledge, there are no comprehensive studies or reports about the economic impact of information errors. We do know that dozens of companies go bankrupt with clean financial statements, and that an increasing number of public companies have had to restate their financial performance. Restated financial statements result in dramatic drops in the market capitalization and have cost shareholders tens of billions of dollars in recent years.

Information Integrity is a significant element of the cost of operations. We know that every person and every department in every organization performs a variety of activities and commits various resources to verify information and to prevent, monitor, and detect information errors. And when errors do occur, it is enormously expensive to research the causes and correct the problem.

The economic impact of information errors is huge!

Take the telecom industry, for example. The telecom industry has a term for revenue lost due to erroneous or missing data. They call it "revenue leakage". In fact, most telephone companies have vice presidents and departments for "Revenue Assurance". Conservatively, telephone companies lose between 5% and 10% of their revenue due to revenue leakage.²⁰ That means an AT&T may be losing at least \$3 billion annually because of information errors.

For other industries, there are no published estimates of losses due to information errors. Our own investigation indicates that, on an average, organizations spend between 1% and 5% of their revenue in activities and resources aimed at preventing, monitoring, verifying, detecting, and correcting errors.²¹ This means that a company with \$30 million in annual revenue would incur a minimum of \$600,000 in costs assuming a 2% impact; a company with \$1 billion in revenue would routinely spend at least \$20 million.

Even a single digit percentage reduction in these costs could mean significant increases in corporate profits.

VI. Information Integrity

The Information Integrity Perspective

Information Integrity (I*I) is the dependability and trustworthiness of information. Information errors are symptoms of lack of Information Integrity or caused by Information Integrity failures. Our perception of information errors, however, is usually quite different. Auditors and accountants view information errors as security, audit, and control issues. Software engineers view them as the result of inadequate software testing or poor development processes. We invest a large amount of resources, hardware, software, people, and time for backup and recovery of our data

and systems. And we have almost everyone – from loading clerks to senior executives – manually verifying all kinds of information. When errors are detected, we often blame it on human failure.

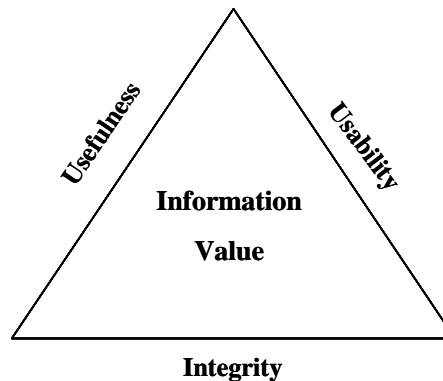
Even our language for discussing and describing the problem and the solution is arbitrary, inconsistent, imprecise, and confusing. We use the words data and information interchangeably. We use accuracy, consistency, quality, and integrity without any common understanding of what they mean.

We need a new framework which establishes a common language, and is based on a rigorous conceptual foundation and sound principles.

A Conceptual Framework

The conceptual framework outlined here establishes Information Integrity as a dimension of information value and then delineates the attributes and domains of Information Integrity.

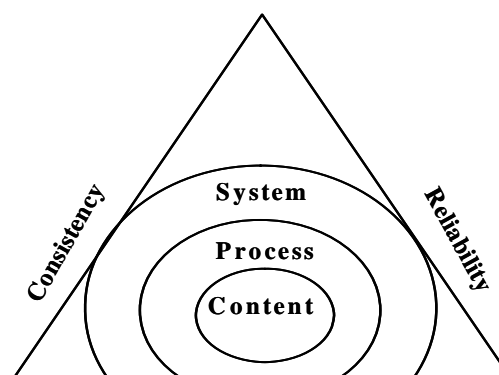
The value of information has three dimensions: its usefulness, its usability, and its integrity (*Fig. 2*).



(*Fig. 2. Information Value Dimensions*)

Usefulness of information is its suitability to purpose. Usability of information concerns its form and accessibility. Information Integrity, often erroneously confused with data quality, is directly concerned with the accuracy, consistency, and reliability of information with its supporting processes and systems. While all three dimensions of information *value* are important, the one most critical to good decision-making and the one over which we tend to have the least control is Integrity.

The Domains of Information Integrity



(*Fig. 3. Information Integrity Domains*)

A distinguishing feature of I*I is its focus on all of the environments or domains that ultimately govern the integrity of information (*Fig. 3*). The issue is not simply “bad data,” but the underlying systems and processes that produce unreliable or inaccurate content. Accordingly, the three domains of I*I are: content, process, and system. The integrated relationship among these three domains is the overall context of Information Integrity.

Information Content is the set of data elements (or groups) provided to the user(s) to enable the attainment of a task’s objectives. The content includes many forms, e.g., numeric, text, graphics, audio, and video.

Process is an organized set of logical functions designed to transform an input into a specified output. Examples of processes include claims processing and financial reporting.

System refers to the organized set of physical and logical components (human, electronic, mechanical, or other) configured to achieve a specific purpose. Computer applications, organizational units and governments are all examples of systems.

Attributes of Information Integrity

What specifically do we mean when we say information possesses or lacks integrity? There are three dimensions or attributes: *accuracy*, *consistency*, and *reliability*. In general, these attributes apply to each of the domains of content, process, and system and can be objectively evaluated and measured. Together, they determine the “trustworthiness or dependability of information.”

Accuracy can be assessed by identifying an established standard and by determining an acceptable tolerance for deviations from that standard. Information that conforms to the standard within an acceptable tolerance is deemed to be accurate.

Consistency can be evaluated by identifying the degree to which repeated instances of the same information occur in space, over time, and in relation to one another at the same point in time (pattern consistency). We expect the same set of inputs,

givens, assumptions and conditions to result in the same content again and again. To the extent this does not happen, we lose confidence in the information.

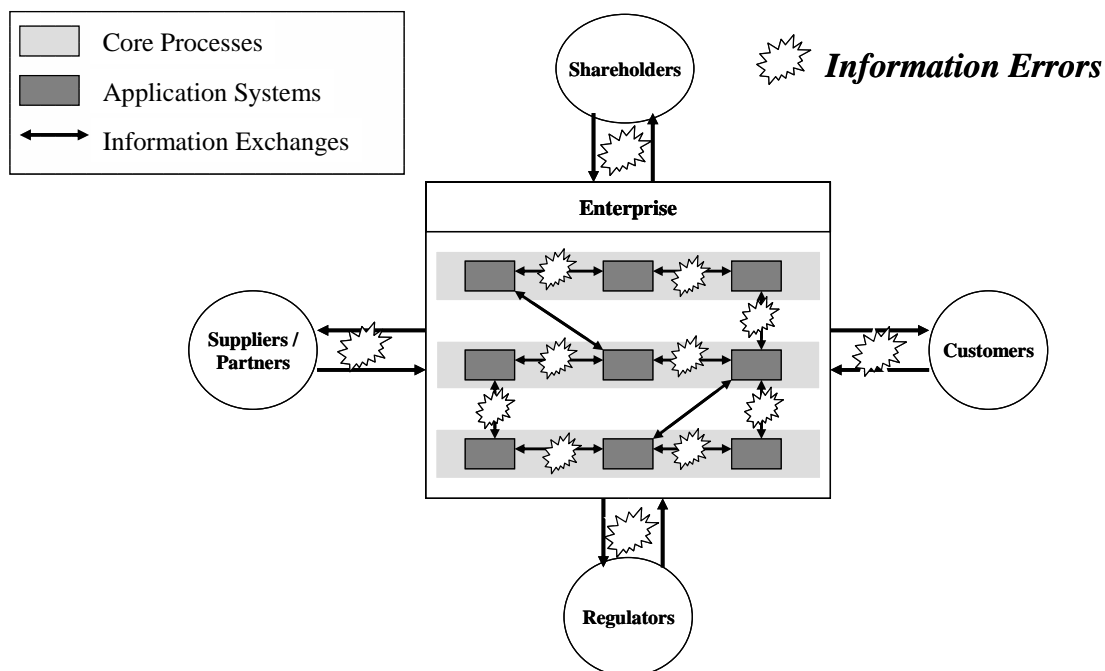
Reliability can be determined by examining its completeness in relation to a given specification; by assessing its currency or relative newness; and by establishing its verifiability, the degree to which its origin and history can be traced. We learn that we can rely on information and the sources of our information when experience shows us that it is up to date (current), in adequate detail and coverage (complete), and when we know the source (verifiable).

VII. Information Controls

The increasing dependence on information and the inherent risk of information errors make it an imperative that organizations deploy an enterprise-wide, integrated system of information controls to achieve the organizational Information Integrity objectives. This section discusses the four levels of information controls within an enterprise, the principles of information controls and the features and benefits of automated information controls.

Levels of Information Controls

Figure 4 shows the Enterprise Information Model (EIM), a simplified representation of the enterprise information environment. The EIM consists of the key external entities that the enterprise interfaces with, the business processes within the enterprise, the application systems that comprise the business processes and the information exchanges among these elements. The key external entities include customers, suppliers, business partners, regulators and shareholders.



(Fig. 4. Enterprise Information Model)

The business processes vary depending on the industry. For example, in retail banking they may include the deposits business (e.g.: checking, savings, money markets, time deposits); the residential mortgage business (including home equity lines); consumer finance (e.g.: auto, credit lines and term debt); as well as the card issuer processing business. The application systems include the software, databases, and reports etc. that are used to process information for a particular purpose.

With reference to the EIM, there are four levels of information controls:

- **Level 1 Controls** monitor and ensure the integrity of the information exchanged between the enterprise and the key external entities. Depending on the industry and the nature of the business, some or all of these information exchanges may be the most critical for the enterprise.
- **Level 2 Controls** monitor and ensure the integrity of the information exchanged among the business processes. Because of the extrinsic risk factors discussed earlier, these information exchanges are susceptible to information errors and must therefore be monitored through appropriate information controls.
- **Level 3 Controls** monitor the information exchanges between the application systems within business processes. Depending on the degree of integration of applications (e.g. ERP implementation) and the frequency and scope of changes, these information exchanges may be at risk to a greater or lesser degree.
- **Level 4 Controls** monitor the integrity of the application systems which are subject to the intrinsic risk factors discussed earlier.

Principles of Information Controls

The effectiveness of information controls depends on how well they follow certain basic principles:

- **Independence:** The controls must be independent of the domain they are intended to control. This contradicts the conventional wisdom that applications and systems are more efficient and effective when they have built-in controls. It is true that integrated applications such as ERP systems have very effective internal controls; however, they are subject to the intrinsic risk factors like all

other systems. More importantly, the interfaces between the applications are susceptible to information errors and therefore must be **auditability**: Information controls should produce audit trails that are necessary and sufficient to verify the results.

- **Concurrency**: The control regime should operate concurrently with the controlled domain. Depending on the information process, this may mean that some controls are exercised periodically while others are operated continuously or in real time.
- **Standardization**: Controls that are consistent in their design, deployment and operation are more effective than a myriad of unique controls.
- **Automation**: Automated information controls are more efficient because they eliminate manual intervention and process delays. They are more effective because they produce consistent and predictable results.

Automated Information Controls

Effective automated information controls prevent information errors, ensure Information Integrity and yield many important benefits to the enterprise such as:

1. **Operational Efficiency**: Operational efficiency is increased through automation of manual verification, standardization of information controls and elimination of unnecessary delays in processes. Operational efficiency translates to better resource use, reduced cycle time, and increased customer satisfaction.
2. **Increased Profitability**: Automated information controls increase profitability by reducing operational costs in many different ways: elimination of manual labor, prompt detection of errors, faster resolution of errors, and lower refunds and write-offs. Profitability is also increased by protecting an organization's revenue through prompt detection and prevention of revenue leakage and the capture of unbilled revenue.
3. **Regulatory Compliance**: Automated information controls, because they are consistent, standardized and verifiable, simplify and speed up internal and external audits. They also ensure that the information provided to the regulators is accurate, consistent, and reliable.
4. **Protection of Reputation**: Some information errors can be catastrophic because they can result in damaging headlines in the media, severe penalties from the regulators or significant erosion of the market value of the business. Automated information controls help detect and prevent catastrophic Information Integrity failures.

VIII. The Next Frontier

There are no signs that the Information Revolution is going to slow down. There are no signs that the deluge of digital data is going to let up. In many respects, our predicament with information today is very similar to our predicament with our natural environment back in 1950's.

Back then, the industrial revolution had left us a legacy of toxic waste dumps, contaminated water, and polluted air. Our life, living, and livelihood were at risk. We have paid an enormous price to deal with the damage.

But, we have also turned a severe adversity into an exciting opportunity. We have developed a whole new science, whole new technologies, and a whole new industry - the environmental science, technology and industry. Today, we are at the threshold of a similar phenomenon: the information equivalent of the environmental crisis.

We must acknowledge and understand information for what it is: a basic, universal, and shared resource. We must acknowledge that information is useless, even dangerous, if it does not have integrity. We must develop a body of knowledge about I*I that applies equally well to banking, engineering and medicine. We must synthesize our current knowledge about I*I – knowledge from disciplines as diverse as accounting, auditing, aerospace, engineering, ethics, food safety, law, library science, robotics, and software, for example – and develop a new I*I discipline.

We must coalesce today's fragmented industry and create a new market space – much like the environmental industry – to produce and deliver a whole array of new products and services, based on scientific theory and sound specifications and standards. We must bring together academia, industry, and government to collaborate and coordinate research and education, and create scientific and technical knowledge about I*I.

The new science and technology will change the way we address I*I. It will help us create new products and services to measure and improve I*I. We will be able to formulate effective and efficient standards and legislation for I*I. Together, the new products, services, standards, and legislation will enable society to have confidence in information.

The development, study and application of Information Integrity present a new frontier for the internal auditor. Perhaps it can dramatically change the audit paradigm and enable internal auditors to achieve their mission more effectively and efficiently in the 21st century.

REFERENCES

- ¹Webster's Encyclopedia Unabridged Dictionary of the English Language. 2001, Random House Value Publishing.
- ²Gupta, Praveen P. "Spiraling Upward – History of Internal Auditing and the Institute of Internal Auditors." Internal Auditor, June 1991.
- ³"Central Bank Audit Practices: Sigma Papers No. 24." Organisation de Coopération et Développement Economiques (OECD.) May 20, 1998.
- ⁴"Risk Glossary", Financial Risk Management (FRM.) 2007 www.riskglossary.com.
- ⁵"Cendant closes fraud case." CNNMoney.com. August 27, 1998.
http://money.cnn.com/1998/08/27/companies/celandant_folo/
- ⁶Woolfe, Jeremy. "Equitable, Ahold prove it: Europe has scandals, too!" WebCPA.com. July 10, 2006. <http://www.webcpa.com/article.cfm?articleid=20810&pg=acctoday>
- ⁷"Enron Debacle", Financial Risk Management (FRM.) 2007 www.riskglossary.com.
- ⁸Risk Glossary, "United States Financial Regulation," www.riskglossary.com. 2007.
- ⁹"World Class Scandal at WorldCom." CBSNews.com. June 26, 2002.
<http://www.cbsnews.com/stories/2002/06/26/national/main513473.shtml>
- ¹⁰Starkman, Dean. "Ahold Settles Lawsuit for \$1.1 Billion." Washington Post. November 29, 2005. Page D03.
- ¹¹Hilzenrath, David S. "Report Slams Fannie Mae: U.S. Regulators Find Accounting Failures At Housing Financier." Washington Post. September 23, 2004: Page A01.
- ¹²"Parmalat: Timeline to Turmoil." BBCNews.co.uk. September 28, 2005.
<http://news.bbc.co.uk/1/hi/business/3369079.stm>
- ¹³"Accounting Failures Aren't New--Just More Frequent." Business Week Online. January 28, 2002. http://www.businessweek.com/magazine/content/02_04/b3767713.htm
- ¹⁴Kurzweil, Ray, and Chris Meyer. "Understanding the Accelerating Rate of Change." Perspectives on Business Innovation. KurzweilAI.net. May 1, 2003.
- ¹⁵School of Information Management and Systems at the University of California at Berkeley (2000), *How Much Information?* White paper.
www.sims.berkeley.edu/research/projects/how-much-info/

¹⁶Jagersma, Pieter Klaas. "Managing Business Complexity." Management Site: for and by professionals. <http://www.managementsite.com/461/Managing-Business-Complexity.aspx>.

¹⁷"Key Issue Briefing: Complexity." Business Leadership Forum. 2007.
http://www.forum.executiveboard.com/BLF/1,3204,0-0-Public_Display-126126,00.html

¹⁸"Enron and Special Purpose Entities." FindLaw: Legal News and Commentary.
<http://news.findlaw.com/hdocs/docs/enron/sicreport/chapter1>

¹⁹"Compliance Compromises Audits." DarkReading.com. November 22, 2006.
http://www.darkreading.com/document.asp?doc_id=111207

²⁰Cleveland, Harlan. "Information as a Resource." *Futurist*. December 1982.

²¹Young, D. (2000), "Finding the Money", *Wireless Review*, July, pp. 37-39, 58.

²¹Deloitte & Touche (1998), *First Revenue Assurance Survey*, White paper. Kloss, L. (2002), "Information Integrity: Our Achilles' Heel", *Journal of AHIMA*, AHIMA.

²²Bariff, M. & Watson, C. (2002), *Information Integrity (I*I) Conceptual Framework*, White paper.

ADDITIONAL RESOURCES

Bariff, M. (2002), "Your Business is Ready for Success, but is Your Information?", *E-Business Strategies Magazine*, Issue 5, p. 23.

Mandke, V. & Nayar, M. K. (2000), "Information Integrity Imperative for Competitive Advantage in Business Environment Characterized by Uncertainty", *Proceedings of 16th World Computer Congress 2000*.

Mandke, V. & Nayar, M. K. (2002), *Global Product and Local Markets – Criticality of Information Integrity for Competitive Advantage*, White paper.

Nayar, M. K. (1999), *Information Integrity Imperative*, White paper.

Nayar, M. K. (2000), *Information Integrity Space*, White paper.

Prabhaker, P. (2003), "Information Integrity: An Edge", *Siliconindia*, pp. 50-51.

Walter, P. (2002), "No more 'as is' information", *E-Business Strategies Magazine*, Issue 4, p. 23.