

Corporate governance and business continuity and availability



Overview.....	3
Current requirements and future trends	3
Fundamental principles.....	4
Implications and impact on continuity of operations	5
Time frames.....	5
Benefits: Efficiencies and competitive edge gained with compliance	5
Changing business processes: E-mail	6
Compliance.....	6
Ensuring compliance	7
Risk of non-compliance	7
Legal considerations	7
Conclusion.....	7
Recommendations for business continuity and availability compliance	7
Bottom line	8
HP Business Continuity and Availability (BC&A) solutions	8
BC&A portfolio	9
Business continuity and availability consulting services.....	9
Data management and protection	9
Database management and protection.....	9
Server management and protection	9
Data center management and protection	9
Appendix A: North America regulations.....	10
Sarbanes-Oxley	10
Recommendations for business continuity and availability compliance	12
Health Insurance Portability and Accountability Act	12
Recommendations for business continuity and availability compliance	13
National Association of Securities Dealers	13
Securities and Exchange Commission	13
NASD Rule 3500 Series	13
3510. Business Continuity Plans.....	13

3510. NASD Rule Third Revision	14
3520. Emergency Contact Information.....	14
Recommendations for business continuity and availability compliance	14
Patriot Act	15
Gramm-Leach Bliley Act	15
Appendix B: EMEA regulations	16
Basel II Accord	16
Basel Committee’s Capital Accords and Sound Practices for the Management and Supervision of Operational Risk	16
Recommendations for business continuity and availability compliance	16
Turnbull Report	16
Appendix C: Asia Pacific.....	17
Monetary Authority of Singapore	17
Key principles	17
Recommendations for business continuity and availability compliance	17
Australia Prudential Registration Authority	18
Recommendations for business continuity and availability compliance	19
Appendix D: Audit standards	20
Organizations of the Treadway Commission: Internal control, integrated framework	20
Statement on Auditing Standards Nos. 55 and 78.....	20
Systems Auditability and Control Report.....	20
Control Objectives for Information and Related Technology.....	20
Key performance indicators—Measuring effectiveness	22
Appendix E: References.....	23
International, cross-industry standards.....	23
Standards and guidelines for financial and technology industries.....	23
Guidelines for publicly traded companies on stock exchanges.....	24
Regulations related to privacy, security, risk management, and corporate governance	24
Additional regulations and guidelines.....	24
Other file retention and protection requirements.....	25
Electronic Funds Transfer Act	25
Graham-Leach-Bliley Act of 1999	25
USA Patriot Act	25
Foreign Corrupt Practices Act of 1977	25
For more information.....	26

Overview

Corporate governance is the system by which companies are directed and controlled. It is the way that corporate boards and officers set policies and handle the affairs of a corporation. Initially, the focus of corporate governance was to protect shareholders of the corporation, but with increasing emphasis being placed on corporate governance and associated policies, current thinking defines corporate governance as a corporation's responsibility to stakeholders (irrespective of share ownership). This fundamental shift means increased importance on external influences (for example, new government regulations) and the need for corporations to be proactive in responding to governance variables, as opposed to a reactive mode in years past.

Corporate governance is primarily concerned with, but not limited to:

- Effectiveness and efficiency of operations
- Compliance with laws and regulations (primarily financial reporting)
- Vulnerability of the corporation and safeguarding of tangible and intangible assets (for example, cash reserves and branding)

This white paper focuses on reliability and availability (from an operational perspective), compliance with laws and regulations, and the safeguarding of assets and its implication to business continuity management programs and practices. Specific regulations by region, as well as applicable auditing standards, are discussed in detail in the addendum.

Current requirements and future trends

Without doubt, the regulatory scrutiny and prescriptive measures established on a global basis has increased significantly within the past five years.

Disasters such as the September 11, 2001 attack on the World Trade Center and the Pentagon caused government and commercial organizations to reevaluate their vulnerability to interruption of operations and to examine the societal impact and readiness of critical physical, telecommunication, and financial infrastructures. Not surprisingly, it was determined that levels of protection were low and the state of readiness not at an acceptable level. This event and others such as the blackouts that occurred in the Northeastern U.S., Eastern Canada, London, Sydney, Copenhagen, and Italy in August and September of 2003, raised awareness of the need for robust, efficient corporate governance within corporations. But although awareness was raised, budgetary constraints and resistance to change caused an initial slow uptake in the implementation of efficient corporate governance offices.

The primary driver of corporations making governance issues more of a priority were corporate scandals (Enron, Adelphia, Arthur Anderson, and so on) that shook the confidence of stakeholders and raised the ire of legislators on a global basis. The most senior executives knowingly provided false financial information, misused or misappropriated corporate assets, and abused their positions. While some of the most significant incidents occurred in the U.S., few of the world countries avoided similar types of corporate malfeasance, causing stakeholder losses and cries for government action. The perceived and actual failure of corporate governance and internal controls has led to the establishment of regulatory focus on ensuring sound internal controls are established for at least the financial elements (auditing) of the organizations.

The most significant legislative trend is the development of regulations that apply significant civil and criminal penalties to management who fail to use due diligence in protecting the corporate assets and the reporting of accurate information. Moreover, even without any penalties, there is a common theme throughout all standards and regulations of management being held accountable for ensuring stakeholders' assets are protected. The most senior levels of organizational management and boards

of directors are becoming personally responsible for ensuring adequacy of controls within their organizations. Few at the most senior management levels will be able to claim ignorance with any hope of protection from civil or even criminal penalties.

Less catastrophic than a disaster or corporate bankruptcy but no less of a societal concern is the right of individual privacy being violated through unauthorized disclosures and system security compromises. Sensitive personal information related to individual identity and health was recognized as requiring a higher degree of protection because of identity theft and issues of discrimination. European countries have had similar privacy laws for over a decade. Impacts on stakeholders exacerbated by poorly designed and maintained controls provided the impetus for regulatory intervention.

How does this affect business continuity management programs? Availability and integrity of information and continuity of services are key internal control concepts directly attributable to an effective business continuity management (BCM) program. What must a company do to ensure compliance with these controls concepts?

It is important to understand how regulators and auditors determine whether an organization is or is not in compliance. Auditors using a variety of audit methodologies review and determine both the presence and in some case efficiency of the controls. One such method, Control Objectives for Information and Related Technologies (CobiT), described in the addendum, can be used to define the parameters in evaluating the effectiveness of business continuity (BC) and disaster recovery (DR) processes.

Additionally management must also consider the following. Do the controls ensure data integrity? If there is an interruption of services, can the organization continue or resume operations without materially affecting the financial position of the organization? Is the data managed and protected sufficiently to minimize loss potential, without compromising timely and accurate reporting of financial results? Is individual privacy protected even during a major incident? Has senior management been engaged in the programs to have sufficient knowledge of their effectiveness?

Fundamental principles

To understand the objectives and implication of regulations, you must recognize the fundamental principles on which they are based. These principles have been the basis for control for decades, for example, principles such as data confidentiality, integrity, and availability and controls such as separation of functional responsibility and clear definition of roles and responsibility. This assumes a fundamental understanding of physical, logical, and operational risks and their implications to the enterprises operations, data, facilities, and personnel. It mandates that basic check and balance, identification and management of risk, and assurances that assets are managed as intended.

Finally, it is ensuring the trust the public and vested individuals have in the accuracy of information representing their interests in the organization and the principles under which that organization is governed is warranted.

It is when these basic concepts are abused and compromised that the need for regulatory guidance and intervention is required.

How companies help ensure they are in compliance with regulations and standards is typically through a review process by audit organizations or other outside independent reviewers. Most times, the auditors utilize one of several widely accepted internal control review methodologies. While the specificity within each assessment methodology varies, they have a common objective of ensuring effective internal controls. Business continuity and disaster recovery are considered key controls in all audit standards.

The effectiveness of the BCM program and its business continuity and disaster recovery planning methodologies is evaluated against best practices and standards that focus on critical elements

supporting continuity of operations, availability of information and staff, and maintaining the integrity of information.

Implications and impact on continuity of operations

The regulations have very specific impact on continuity of operations. There is a broad presumption that data protection and system availability are fundamental to effective internal controls. Compliance with regulations assumes an effective business continuity program.

Time frames

Current regulations already mandate data protection and privacy and presume continuity of operations as part of demonstrating effective internal controls. Considering the ever-increasing government focus on ensuring investor protection and mandating effective corporate governance, an increase in both the number, frequency of publication, and scope of the regulations should be anticipated.

The META Group reported in May 2002 a prediction that “regulatory pressures would force more than 30% of Global 2000 (G2000) firms to adopt a formal risk management (RM) model such as CobiT or CRAMM (UK government’s Central Computer and Telecom Agency Risk Analysis and Management Method), and that by 2005, more than 40% of G2000 firms would adopt RM and a balance risk/reward reporting process.” They also predicted that because of the increasing use of “supercritical” real-time 24 x 7 business systems, there would be an increased emphasis on the use of high availability (HA) solutions. This has implications that affect traditional operational processes and the underlying methodologies utilized to build new applications (HA requirements must now be considered before development as opposed to an additive at the end of the process). Also, resiliency will increasingly be engineered into the normal day-to-day architectures of larger network/web-centric organizations. Some of the implications caused by these conditions include:

- Technology—Emphasis on resilience of design and data integrity and protection
- Services—Increased use of outsourcers to diversify risk
- Solutions—Emphasis on data resilience solutions, high availability, and geo-diversity to provide protection against regional incidents
- BCM—Movement toward solutions capitalizing on the business demand for more information and having zero tolerance for interruptions of business processes and the efficiencies and business advantages from having access to large volumes of data and meeting the expectations of today’s e-commerce customers and trading partners

Benefits: Efficiencies and competitive edge gained with compliance

- Reduced risk exposure
- Increased stakeholder confidence
- Increased efficiency by having a proactive policy towards compliance
- Ability to build internal operational efficiencies caused by compliance constraints and controls
- Increased value to possible partners by showing compliance
- Reduced data administration costs
- Architectural changes provide geo-diversity
- 99.999 availability plus protection from site loss

Changing business processes: E-mail

To minimize risk and exploit synergies between corporate governance and continuity, organizations must be aware of how business processes have evolved and changed. It is essential to understand the criticality of different business processes when performing a business impact analysis (BIA); e-mail is a good example of this.

Not too many years ago, e-mail was not considered mission-critical and therefore was not considered worth protecting. But now e-mail has supplanted all paper-based and verbal communications as the most critical single element of the corporate communications infrastructure. The vast majority of organizations now consider e-mail a viable and trusted medium for taking orders, giving approvals, formalizing contracts, and discussing sensitive human resource issues. The corporate e-mail system now contains a massive amount of information that once was stored only on paper.

Governmental and legal scrutiny regarding e-mail has increased, and now e-mail is as admissible in courts as paper-based records.

Recent research has found that approximately 60% of the critical business information that the typical e-mail user requires for his or her job is stored within the e-mail system. E-mail system storage growth increases by 40% or more each year because of the growing use of e-mail, increased use of attachments, and increased user reliance on the tool.

Although enterprises in the financial services and health care industries face the most difficult data retention requirements, all enterprises in all industries are required to maintain records in e-mail and other electronic media. Complicating the issue is that there are thousands of data retention requirements in the United States and elsewhere.

Poor records retention practices expose organizations to a host of legal problems, potentially heavy fines, and a loss of reputation.

Without an appropriate archiving system from which e-mails can be methodically searched and extracted, a court order can order that all servers and backup tapes can be seized for analysis.

Compliance

To become compliant, HP suggests that the following issues be considered and addressed.

First, recognize that simple tape backups are not an effective method for ensuring that regulatory or legal requirements can be met, nor are these backups an effective method for gaining access to the volume of information housed in the organization's messaging system. Traditional backups are more difficult to manage than a properly implemented archiving system, require more IT intervention, and can create more e-mail downtime in the event of a server failure or other technical problem.

To better enable record protection and effective access, the system should be able to:

- Enforce corporate data retention policies—Permits data to be retained as long as necessary but no longer.
- Have no requirement for involvement—Automation lessens overhead and reduces errors.
- Index all content—Assists meeting demands imposed by a regulatory audit or court actions.
- Safely allow authorized end user access without IT assistance.
- Protect archived data from tampering—A key requirement of many of the content management regulations imposed by government is that data is tamper proof and provides an audit trail when accessed.
- Archive only required e-mail—Allows focus on those messages the organization has deemed necessary rather than creating an archive of clutter, spam, informal communications, newsletter, and the like.

Ensuring compliance

- Establish and enforce a corporate retention strategy.
- Store records in a system and on protected media that enables authorized access and provides access to an audit trail and timely retrieval of archived records.

Risk of non-compliance

Fines, while insignificant in relationship to the overall profit of the organization, should be considered “a shot over the bow” as a warning that penalties that are more significant might be imposed.

Legal considerations

Electronic records now have legal validity; the courts cannot deny their use simply because they are in electronic form. During the legal discovery processes, e-mails are subject to review. Technical difficulty in providing electronic records is not accepted as an argument. Every commercial or government agencies requires the production and retention of a record.

Conclusion

Recommendations for business continuity and availability compliance

To achieve maximum efficiency in integrating compliance issues with continuity projects, organizations must take a proactive approach towards compliance. Initially, organizations must create a robust BC plan that minimizes risks and accounts for all the variables that can significantly impact an organization in the event of a disaster. To do this, organizations should:

- Complete a risk analysis to determine the vulnerability of the systems and data
- Mitigate the risks where possible
- Complete a business impact analysis to identify the financial and other impacts to the organization caused by the loss of systems, data, or both; identify the dependencies on locations, data, equipment, networks, and staff
- Determine the Recovery Point Objectives (RPOs) that establish the maximum data loss that can occur and still enable financial reporting to be accurate and timely
- Identify the data management and technology solutions to minimize data loss and maximize data availability
- Determine the Recovery Time Objectives (RTOs) that establish the window of time for recovery from downtime and identify the processes and technology solutions to meet these objectives
- Brief the organization management and obtain approval
- Document the BC solutions, processes, and actions into plans
- Test the solutions and validate the data
- Maintain the BC plans within a formal documentation process that considers changes in the organization and ensures a current state of the plans
- Have the processes validated by an independent reviewer on an annual basis

After organizations have established sound BC methodologies, the synergies between governance and continuity can be exploited. Some things to consider are:

- Can continuity and governance be accomplished by a unified approach (for example, backup and restore of electronic records)?
- What business processes are critical (e-mail could be an example)?
- Are the BC/DR plans current?

- How recently were they rehearsed?
- What are management's expectations regarding timeline and amount of compliance?
- How do recent regulations affect your e-mail and instant messaging systems? What underlying implications does this have in maintaining business process? (for example, directory integration in the event of a disaster.)
- Does your off-site backup location meet requirements for distance, staffing, and accessibility?
- Is your backup location on a different power grid? Does it emulate your production infrastructure? Are there redundant, yet diverse carrier connections?
- How recently have the business owners reviewed the RPOs and RTOs? Are they based on relevant business processes and not just IT metrics?
- Do your organization's processes support compliance objectives?
- Does your current technology support the storage growth and records management requirements of regulations?
- Are your audit trails sufficient?
- Who is responsible for enforcing and maintaining compliance? How many departments are involved?
- How do these regulations affect your security procedures?
- Beyond saving the information, how quickly can you retrieve a necessary file?
- Can the system withstand an external test while operations continue?

Bottom line

The assessment of BC and DR plans has long been included in the audit approach of various regulatory and standards organizations. The financial services industry experienced the most attention to DR planning even before September 11. Regulatory agencies such as the Office of the Comptroller of Currency regularly audit controls to ensure the integrity of transactions and the protection of sensitive customer information.

Regulation aside, transaction integrity, service and IT asset availability, and the security and availability of sensitive customer information are top-of-mind business imperatives across most industries. Exploring enterprise-wide practical contingency options that meet specific regulatory, contractual, and customer demands will prove valuable for recovering from any disaster or business interruption.

Although many organizations struggle with meeting regulatory requirements, few embrace the true benefits that result from exercises necessary to not only identify risks to the financial reporting process, but also mitigate those same risks. A comprehensive BC effort, including a rigorous BIA and risk assessment, supplemented by a business continuity plan, can identify risks that, if left unchecked, could compound the impact to an organization after a disaster.

HP Business Continuity and Availability (BC&A) solutions

Your business depends on information technology more than ever before. In this IT-driven environment, availability of key application services and information is critical to maintain your business processes, and the consequences of any outage are far-reaching. A service interruption can mean lost customers, decreased revenue, and production downtime. Businesses need their key business processes—and the IT infrastructure that enables them—to be adaptive, reliable, and resilient. These factors, combined with the need to satisfy present and future regulatory environment, means that organizations must take an adaptive approach to their availability and continuity requirements. HP has a long legacy of meeting these challenges and offering clients solutions that are both adaptable and resilient.

BC&A portfolio

Business continuity and availability consulting services

- Risk assessment
- Business impact analysis
- Business continuity strategy definition
- High availability/disaster-tolerant solution infrastructure design
- Business continuity plan development
- Business continuity plan rehearsal
- Business continuity program management

Data management and protection

- Backup and recovery technologies
- Backup and recovery services
- Electronic vaulting services
- Data replication technologies
- Data replication services

Database management and protection

- Oracle RAC and RACGuard

Server management and protection

- ProLiant (clustering)
- HP-UX (serviceguard suite)
- Alpha (OpenVMS)
- NonStop

Data center management and protection

- Business recovery services for the office
- Business recovery services for the data center

Appendix A: North America regulations

Sarbanes-Oxley

The purpose of the Sarbanes-Oxley Act (SOX) of 2002, and related regulations, is to ensure that the corporate scandals that erupted over the last five years do not happen again. This is primarily achieved by making executives and officers of all public corporations (of any size, including small businesses) and certain investment firms bear personal liability for the maintenance of company records, essentially making the defense of executive “ignorance” not admissible in the courts of law.

The law even extends into foreign audit firms doing business in the U.S. or with U.S. companies. Although Securities and Exchange Commission (SEC) Rule 6835 has for some time required management (that is, the board of directors) to generate report that includes an analysis of any and all terms deemed material to the financial performance of a corporation, SOX extends the rule’s scope, responsibility, and punitive measures.

Sections 302 and 404 of the SOX most closely apply to data protection and continuity of operations. And while the data integrity and continuity is implied by the stated objectives of the act, it is not explicitly stated. One can conclude that not being able to report accurate financial statements within the prescribed timeframes would cause an organization to not be in compliance with the act. With corporations creating teams devoted to SOX compliance triage, there must be synergy between both corporate and IT audit teams. Indeed, auditing, legal, and IT departments will embrace IT portfolio management, focusing on risk management dimensions of information assets, existing and planned systems, and technology solutions to center compliance efforts on areas of greatest risk and concern.

A proper risk assessment should include lesser known operational and IT risks resulting from, among other things, inadequate DR or BC plans. These deficiencies would affect the availability of the following financial related processes and functions:

- Capturing and authorizing transactions
- Processing cutoffs
- Ability to roll up disclosure data
- Fair value information pricing
- Trading position and current market exposures

In an ideal world, these processes and their related risks and controls would already have been assessed if a BCM structure existed, was being considered, or was under development.

Section 302 is currently in effect. Executive certification requires the certifying officers to state:

- They have read the financial report.
- The report does not contain or omit any untrue statement.
- The report represents the financial condition of the company.
- They are responsible for establishing and maintaining “disclosure controls and procedures” and have ensured the financial information has been disclosed to them.
- They have evaluated the effectiveness of the issuer’s disclosure controls and procedures within 90 days.
- They have reported to the auditors and the audit committee (a) all significant deficiencies in the design or operation of internal controls which could adversely affect the company’s ability to record, process, summarize, and report financial data; (b) any material weaknesses in internal controls; and (c) any fraud, whether material, that involves management or other employees who have a significant role in the issuer’s internal controls.

- Whether there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.
- The report materially and accurately represents the financial condition of the company.

Not having a business continuity plan that proves the ability to continue financial reporting following an interruption is a significant deficiency in the design or operation of internal controls that could adversely affect the company's ability to record, process, summarize, and report financial data.

The risk analysis of internal controls must consider pervasive IT controls. Computer operations, physical and logical security, program change, systems development, Internet, business continuity, and similar controls are examples of pervasive IT controls. These IT controls are pervasive because they affect the achievement of financial control objectives across multiple processes through the related application systems at the process level.

Section 404(a) Sarbanes-Oxley Act of 2002 and the Securities Exchange Commission's related implementing rules¹ require the management of a public company to assess the effectiveness of the company's internal control over financial reporting, as of the end of the company's most recent fiscal year. Section 404 also requires management to include in the company's annual report to shareholders management's conclusion because of that assessment about whether the company's internal control is effective.

According to the SEC, implicit in the rule is an understanding that a company's senior management "bears express responsibility for **designing, establishing, maintaining, reviewing, and evaluating**" the company's disclosure controls and procedures and ensuring that reports are "**timely, accurate, and reliable.**" Executives, who proceed without a comprehensive evaluation of their information system vulnerabilities and an appropriate response to that evaluation, do so in violation of these provisions and at their personal risk.

There is a presumption in financial reporting that public companies will be able to meet their reporting deadlines and have available all material information needed for fair presentation and disclosure, including the update of accounting estimates with current and reliable information.

Under Sarbanes-Oxley, the allowed time to file quarterly reports will fall from the current 45 days to 35 days in 2005, and annual reports will have to be filed within 60 days of the close of the year, rather than 75. Disclosures of "material events" and insider trades must be filed within two days. Should the event causing an interruption of operations occur just before preparing the reports, the organization will have 10 less days for their quarterly reports and 15 less days for the preparation of the annual report to recover their financial systems and any data lost during the incident. Without the appropriate recovery time objectives, available recovery resources and testing that validates both the quality of the data and effectiveness of the system the organization might not be able to make the dates.

The risk and business impact analyses of the business continuity management program establish the operational risks, interdependencies, and impacts associated with critical business processes. The two foundations of BCM establish the basis for the recovery objectives for critical business processes and IT assets, as well as risks to which the organization might be vulnerable. After the risk and business impact analysis is completed, the organization can evaluate whether changes are needed to their business continuity and disaster recovery plans. The plans must be maintained in a current state and validated through testing to ensure the company can fulfill its obligations to shareholders under SOX requirements.

¹ Refer to "Final Rule: Managements Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports" (Securities and Exchange Commission Release No. 33-8238, June 5, 2003).

A company must meet the financial reporting presumption, and on a program level, an organization's business continuity methodology and approach must be agreed to by management as the foundation for mitigating financial and reputation risk posed by business interruption.

The results of the analyses focus the organization on the data and applications that support the critical business processes. The data management processes include backup, recovery, and restoration. The company must be able to restore or restart the processing in a manner that does not violate the integrity and completeness of transactions or data.

The loss of transactions and data obviously could affect the accuracy and completeness of processing.

The criticality of applications derived from the business impact analysis help define the appropriate timing and frequency of the backup process. The cost/risk/benefit evaluation of how much data or transaction a company can afford to lose without negatively impacting the business is considered in the frequency, method, and reliability of the data management process.

Recommendations for business continuity and availability compliance

In relationship to compliance with Section 404, business continuity and disaster recovery plans facilitate the ability to continue to accurately and timely file its required financial and other filings with the SEC under the commissioner's rules and regulations.

This means:

- Financial data must be protected to maintain its integrity and availability.
- Internal controls, in this case availability, must ensure both integrity of the data and the timeliness of reporting.
- Auditors will assess business continuity and disaster recovery programs to ensure they provide for protection of financial data and the timely processing and reporting of financial information. There are no provisions to delay financial reporting caused by an incident that interrupts business, technology operations, or both. There are no provisions to allow less than the most current and accurate data should the company's financial data be lost. There are no provisions, and in fact, some prohibitions to utilize manual processes in lieu of automation under emergency conditions. The uses of spreadsheets as a temporary recovery solution is no longer acceptable because human intervention can circumvent the controls designed into the financial systems.

Health Insurance Portability and Accountability Act

The American Health Insurance Portability and Accountability Act (HIPAA) signed by President Clinton on August 21, 1996 as part of on-going health care reform initiatives. The purpose of Title II, the Administrative Simplification section of the law, is to improve the efficiency and effectiveness of the health care system by standardizing the electronic data interchange of certain administrative and financial transactions. HIPAA requires the Department of Health and Human Services (DHHS) to develop standards and requirements for the maintenance and transmission of individually identifiable health information. HIPAA also provides for civil and criminal penalties for noncompliance.

The security regulations resulting from HIPAA became final on February 20, 2003. The new federal security standards cover how personal health information is electronically maintained or transmitted. It is a legal nightmare, requiring massive training efforts and millions of dollars to bring affected organizations into compliance. While these standards became law, it does not take effect until April 21, 2005, according to the Centers for Medicare & Medicaid Services (CMS), part of the U.S. DHHS. According to the CMS, the new security standards will affect 2.6 million "covered entities," a group that includes the whole swath of the health care industry, from individual doctors to hospitals to major insurance plans. While it does not mandate specific technologies or procedures that should be used to meet the security standards, the CMS does define what information must be protected and what the industry should strive to do. The wording is intentionally general and leaves it to the complying organization to interpret and implement

According to the deputy director of the office of HIPAA standards at CMS, the security standards could become the de facto standard for Protected Health Information (PHI) even though they are not effective until 2005. The privacy rules cover paper and oral communications, as well as electronic health information. Most importantly, the standards not only cover privacy; they also cover integrity and availability.

Recommendations for business continuity and availability compliance

To become HIPAA compliant, HP recommends that you:

- Identify the risks associated with a disclosure of information specified within this act.
- Follow the basic BCM principles to ensure availability of protected information, while maintaining a protected state.
- Ensure that information is protected at alternate locations, during the restoration of data in a recovery effort and at the workstations. Essentially utilize the same operational safeguards within the secondary location that are present within the primary production environment.

National Association of Securities Dealers

On August 30, 2002, the National Association of Securities Dealers (NASD) issued a proposed business continuity plan rule. It provides that each member must have a written business continuity plan and conduct an annual review of its plan. Each plan must address each of the types of risks enumerated by the rule.

The New York Stock Exchange also filed during the same period. The planning requirements for both organizations are for the most part identical.

Securities and Exchange Commission

[Release No. 34-47441; File No. SR-NASD-2002-108] March 10, 2003

Self-Regulatory Organizations; Notice of Filing of Amendment Nos. 1, 2, and 3 to a Proposed Rule Change by the National Association of Securities Dealers, Inc. Relating to Business Continuity Plans and Emergency Contact Information March 4, 2003. Pursuant to section 19(b) (1) of the Securities Exchange Act of 1934 ("Act") 1 and Rule 19b-4 there under, the National Association of Securities Dealers, Inc. ("NASD"), on August 7, 2002, filed with the Securities and Exchange Commission ("Commission"), a proposed rule change to require its members to establish and maintain business continuity plans.

NASD Rule 3500 Series

On April 7, 2004, the Securities and Exchange Commission (SEC) approved the new NASD Rule 3500 Series, which requires members to establish emergency preparedness plans and procedures.

3510. Business Continuity Plans

(a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to continue its business in the event of future significant business disruptions.

(b) Each member must update its plan in the event of any material change to the member's operations, structure, business, or location. Each member must also conduct an annual review of its business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business, or location.

(c) The elements that comprise a business continuity plan are flexible and may be tailored to the size and needs of a member.

Each plan, however, must at a minimum, address:

- Data backup and recovery (hard copy and electronic)
- All mission-critical systems
- Financial and operational assessments
- Alternate communications between customers and the member
- Alternate communications between the member and its employees
- Business constituent, bank, and counter-party impact
- Regulatory reporting
- Communications with regulators

Each member must address the categories in the preceding list to the extent applicable and necessary to enable the member to continue its business in the event of a future significant business disruption. If any of these categories are not applicable, the member's business continuity plan need not address the category. The member's business continuity plan, however, must document the rationale for not including such category in its plan. If a member relies on another entity for any one of these categories or any mission-critical system, the member's business continuity plan must address this relationship.

(d) Members must designate a member of senior management to approve the plan, and he or she will be responsible for conducting the required annual review. The member of senior management must also be a registered principal.

(e) For purposes of this rule, the following terms shall have the meanings:

(1) "Mission-critical system" means any system that is necessary, depending on the nature of a member's business, to ensure prompt and accurate processing of securities transactions, including, but not limited to, order taking, order entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities.

(2) "Financial and operational assessment" means a set of written procedures that enables a member to identify changes in its operational, financial, and credit risk exposures.

3510. NASD Rule Third Revision

NASD Rule 3510 is intended to require not only that members conduct a planning process to create a written business continuity plan, but also that the plan resulting from this process be reasonably designed to enable members to continue their business in the event of a future significant business disruption.

3520. Emergency Contact Information

Each member shall report to NASD, through such electronic or other means as NASD might require, prescribed emergency contact information for the member.

Each member must promptly update its emergency contact information, through such electronic or other means as NASD might require, in the event of any material change.

Recommendations for business continuity and availability compliance

To become compliant with the above, HP recommends that within your plan you address:

- Data backup and recovery (hard copy and electronic)
 - Assumes data is evaluated to determine its criticality, the recovery point objectives are identified, and the restoration solutions will support the recovery time objectives. The backup data is not exposed to the same incident as the primary site data.
- All mission-critical systems

- Assumes a business impact analysis is conducted to identify mission-critical and non-critical systems. Management has reviewed and understands the potential impacts and approved the recovery time objectives.
- Financial and operational assessments
 - Assumes identification of financial and operational impacts and interdependencies
 - Alternate communications between customers and the member
 - Assumes alternative means to continue emergency communication between customers and the member organization without access to normal communication vehicles
- Alternate communications between the member and its employees
 - Assumes emergency communications processes between the members and its employees
 - Business constituent, bank, and counter-party impact
 - Assumes understanding of the impact on business constituents, banks, and counter-parties
 - Regulatory reporting
 - Requires formalized process to report the impact of the incident to the regulators following a loss and communications with regulators
 - Requires vehicles and processes to facilitate immediate communication with regulators

Patriot Act

The Patriot Act, passed in the wake of the September 11, 2001 terrorist attacks, requires financial services companies to verify customer identities, submit suspicious-activity reports to the U.S. Department of the Treasury's Financial Crimes Enforcement Network, and check customers against crime databases established by law enforcement agencies.

Gramm-Leach Bliley Act

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule, and Pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the **Financial Privacy Rule** and the **Safeguards Rule**. These two regulations apply to financial institutions, which include banks, securities firms, insurance companies, and companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts, and an array of other activities. Such non-traditional financial institutions are regulated by the Federal Trade Commission (FTC).

The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether they are financial institutions, who receive such information. For a summary overview of the Financial Privacy Rule, the Safeguards Rule requires all financial institutions to design, implement, and maintain safeguards to protect customer information.

The Safeguards Rule applies to financial institutions that collect information from their own customers and to financial institutions—such as credit reporting agencies—that receive customer information from other financial institutions.

The **Pretexting** provisions of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting."

Appendix B: EMEA regulations

Basel II Accord

Basel Committee's Capital Accords and Sound Practices for the Management and Supervision of Operational Risk

The Bank for International Settlements (BIS) is an international organization on banking policy, including the U.S., and includes the Basel Committee on Banking Supervision, which is named for Basel, Switzerland, where it is based.

The Basel Committee issued the Basel Capital Accords in April 2003. Section 5 of the accords addresses operational risk, defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.” It provides a formula for determining the amount of capital a bank must hold for operational risk. For a bank to qualify for a lower reserve, it must prove the adequacy of its risk management framework.

“Sound Practices for the Management and Supervision of Operational Risk,” issued by the Basel Committee in February 2003, details the required contingency and business continuity plans in its Principles 7 and 10.

As a global accord, it is applicable to all multinational financial institutions and focused on operational risks with the objective to ensure continued financial viability by maintaining an appropriate capital level consistent with the risk profile of the organization. The lower operational risk profile allows the organization to maintain a lower capital reserve. The higher the operational risk, the higher percentage of capital reserve. Again corporate governance is considered in the operational risk profile of the organization. The consequences of a high-risk profile are the requirement to set aside funds that otherwise might be used for corporate initiatives and growth.

Again like SOX, the identification of sources of risk and consequences of impact provide the basis for effectively managing organizational risk through implementation of sound business practices. Basel II identified four groups of principles to establish an effective risk management program within the organization. The first group, “Developing an Appropriate Risk Management Environment,” provided three principles to establish the environment. The second group, “Risk Management: Identification, Assessment, Monitoring and Mitigation/Control,” identified four principles. And within those, “Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption,” is most relevant to this white paper.

The third group, “Role of Supervisors,” consists of two principles and the fourth group, “Role of Disclosure,” presents the tenth and last principle.

Recommendations for business continuity and availability compliance

To become Basel II compliant, HP recommends that you be able to demonstrate your business continuity plans, provide the ability to continue operations, and limit losses in the event of a severe business disruption.

Turnbull Report

The Turnbull Report was published in September 1999 and was aimed at businesses taking risk more seriously. Endorsed by the London Stock Exchange, it firmly places responsibility for managing risk in the lap of senior directors. Listed organizations must now demonstrate to shareholders that they have assessed the risk attached to all assets and activities and that they have taken action to limit or remove their exposure to risk in each area. Of course, as with any regulation or sector-specific guidelines, companies that do not comply with the Turnbull Report face the threat of a backlash in stakeholder confidence—from customers to investors—and, in theory, could even be de-listed.

Appendix C: Asia Pacific

The Asian community, like their American and European counterparts, is driven to business continuity through regulatory requirements. The lack of regulations (with the exception of Australia and Singapore) with regard to business continuity and disaster recovery continues to inhibit organizations from budgeting for corporate-wide business continuity management programs, with the exception of the financial institutions industry, where the central banks across Asia, such as Singapore and Hong Kong, have issued supervisory policies and guidelines. The financial industry also recognizes the need for regulation and compliance from a global perspective; hence, the incentive to comply with the requirements listed in the Basel II Accord. Countries such as Korea and Japan are beginning to follow. However, enforcement of policies is also limited.

Monetary Authority of Singapore

Business continuity management awareness and support is increasing in Asia-Pacific countries. Singapore, one of the leading countries supporting the BCM process, began developing standards, encouraging compliance, promoting awareness, and supporting education of BCM professionals.

Singapore published "Guidelines on Business Continuity Planning-Monetary Authority of Singapore (MAS)," on January 10, 2003. The guidelines are closely aligned with the NASD guidelines published in August 2002.

The Monetary Authority of Singapore (MAS) consultation paper proposes seven principles on business continuity planning in response to financial institution requests for guidance. Financial institutions are encouraged to consider and adopt these principles.

MAS will, in the course of its supervision of institutions, review the BCP implemented, taking into consideration the institution's alignment with the principles and their risk profile and role in preserving the systemic stability of the financial system. BCP is an important contributing factor in MAS' overall supervisory assessment of the institutions.

Key principles

- Principle 1: Board and management should take responsibility for the BCP preparedness of their institution.
- Principle 2: Institutions should embed BCP into their business-as-usual operations, incorporating sound practices.
- Principle 3: Institutions should test their BCP regularly, completely, and meaningfully.
- Principle 4: Institutions should develop recovery strategies and set recovery time objectives for critical business functions.
- Principle 5: Institutions should understand and appropriately mitigate interdependency risks of critical business functions.
- Principle 6: Institutions should plan for wide-area (zonal) disruptions.
- Principle 7: Institutions should practice separation policy to mitigate concentration risk.

Recommendations for business continuity and availability compliance

To become compliant, HP recommends that you consider the following:

- The board and management should take responsibility for the BCP preparedness of their institution. Senior management and the board must ensure the BC plans and resources will work as planned, limit interruptions and loss of revenue, and ensure confidence in the organization.
- Embed BCP into their business-as-usual operations, incorporating sound practices. BCM is an integral part of business processes, technology architecture, and data administration.

- Test BCP regularly, completely, and meaningfully. This means the plans are proven by testing the applications, infrastructure, systems, and networks, exercising the teams, and ensuring deficiencies are corrected in a timely manner.
- Develop recovery strategies and set recovery time objectives for critical business functions. This assumes the organization understands the risks and potential business impacts and has addressed the risks and management has approved the recovery time objectives.
- Understand and appropriately mitigate interdependency risks of critical business functions. Analyze interdependencies and identify critical relationships between internal business functions, outsourced services, and trading partners.
- Develop solutions that consider potential for wide-area (zonal) disruptions. Consider geographically diverse solutions that distribute staff, equipment, facilities, and data.
- Establish and practice a separation policy to mitigate concentration risk. Ensure the primary and alternate facilities, equipment, data, and staff is sufficiently geographically distant to limit the possibility that a wide-area incident will affect both facilities.

Australia Prudential Registration Authority

The Australian government views the importance of having a business continuity management standard to ensure continuity of operations in the event of problems arising because of internal or external events to minimize the financial, legal, reputation, and other consequences of the disruption.

The objective of the Australia Prudential Registration Authority (APRA) is to ensure that institutions implement a holistic business approach to BCM that is aligned with the nature and scale of its operations using plausible scenarios. With the increase resilience to business disruptions arising from internal and external events, APRA desires to ensure that critical systems can be restored in a timely manner. It also aims to meet financial and service obligations to depositors and policy holders.

Overview of APRA guidelines

- Risk management framework: Integrate BCM into the risk framework and treat it as a business function and not within IT.
- Materiality: Apply on a whole of business basis to critical business functions, resources, and infrastructure.
- Risk assessment: Use plausible scenarios that can lead to short-, medium-, and long-term disruption.
- Business impact analysis: Conduct a BIA that addresses all business units, including subsidiaries, outsourcing, and service providers, to define critical business functions.
- Recovery strategy: Conduct cost and benefit analysis to determine the resources needed to implement the strategy. Business insurance is not to be used as a comprehensive BCM framework.
- Business continuity plan: Outline the procedures to enable recovery, resumption, and return to normal processing.
- Communication plan: Plan to notify key internal and external stakeholders, including regulators, staff, customers, counterparts, service providers, and media.
- Outsourcing: BCM must be included in any outsourcing agreement that is undertaken by the institution.
- Alternate sites: Alternate sites should be located at a sufficient distance from the primary site to ensure the risk of both being impacted.
- Review and testing: Testing should be undertaken annually (at a minimum) and should cover all business areas and individual components.
- Training: Institutions should implement a general training program to build awareness of the BCP with the staff assuming responsibility for execution.
- External audit: APRA might request an external auditor of the institution to provide an assessment of the BCM arrangements.

- **Accountability:** Where institutions use service providers, it is the responsibility of the institution to ensure compliance, not the service provider.
- **Application:** APRA guidelines apply to institutions on a business basis including any service providers located outside of Australia.
- **Notification requirements:** Institutions must notify APRA as soon as possible from the event and no later than 24 hours of the incident.
- **Transitional arrangements:** Institutions must confirm compliance with the standard in their upcoming annual risk management declaration. Areas of noncompliance should be reported to APRA with an action plan for recertification.

Recommendations for business continuity and availability compliance

The guidelines from APRA constitute a holistic and methodical means for an effective business continuity program. To be compliant, HP recommends that you follow the APRA guidelines, concentrating on how much protection for your institution must have.

Institutions should define their BCM policy and objectives, define their levels of business impact (intangible and tangible), build recovery strategies to address the most likely scenarios that could impact the institution, and implement a comprehensive business continuity plan.

Appendix D: Audit standards

Organizations of the Treadway Commission: Internal control, integrated framework

The internal control, integrated framework of the Organizations of the Treadway Commission (COSO) defined internal control as:

A process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Internal control is a process because it is planned, executed, and monitored by the board of directors and management of an entity as part of the management process and because it is the sum of a series of actions that permeate an entity's business processes.

COSO assumes that internal control can provide only reasonable, not absolute, assurance regarding the achievement of internal control.

Statement on Auditing Standards Nos. 55 and 78

Statement on Auditing Standards (SAS) No. 78 amends SAS No. 55 by replacing its definition and description of the internal control structure with that prescribed in the COSO report. While COSO tends to refer to all information systems, operational as well as financial, SAS No. 78 emphasizes only those systems and controls relevant to financial reporting objectives.

SAS No. 78 adopts COSO's five components—control environment, information and communication, control activities, risk assessment, and monitoring—and provides a greater understanding to those trying to make operational the concepts in an effective system.

Systems Auditability and Control Report

The Systems Auditability and Control Report (SAC Report, The Institute of Internal Auditors Research Foundations, 1991 and 1994) defines internal control as a means of to provide reasonable assurance that the overall objectives of the organization are achieved in an efficient, effective, and economical manner. The system of internal control is described as a set of processes, functions, activities, subsystems, procedures, and organization of human resources that provides reasonable assurance that the organization's goals are achieved and risk is acceptable. The SAC Report specifically focuses on those objectives impacted by the organization's information systems.

Control Objectives for Information and Related Technology

Control Objectives for Information and Related Technology (CobiT) was developed by the CobiT Steering Committee and Information Systems Audit and Control Foundation to bridge the gap that exists between business control models and the more focused control models for IT.

CobiT provides two control concepts: control and IT control. CobiT internal control is defined the same as COSO defines it. However, the control objectives under CobiT are defined in a process-oriented manner following the principles of business re-engineering.

The IT control concept is adapted from the SAC Report and defined as "a statement of the desired results or purpose to be achieved by implementing control procedures in a particular IT activity." This control is activated at the IT activity level.

The CobiT IT domain consists of four parts: planning and organization, acquisition and implementation, delivery and support, and monitoring. Thirty-four IT processes are identified within each of the four domains. The central control objective is to link IT domains, processes, and activities to the entity's operational processes and activities. The IT objective is to facilitate the accomplishment of business objectives.

Business objectives requirement for information include the following:

- Quality requirements (quality, cost, and delivery)
- Fiduciary requirements, as defined by COSO (effectiveness and efficiency of operations, reliability of information, and compliance with laws and regulations)
- Security requirements (confidentiality, integrity, and availability)

The CobiT's control objectives go beyond the business objectives defined by COSO or SAS Nos. 55 and 78—for example, IT Control Objective DS4: CobiT's Delivery and Support, Ensure Continuous Service. Control over the IT Control Objective, **"Ensure Continuous Service,"** has the business goal of **ensuring IT services are available as required and ensuring a minimum business impact in the event of a major disruption.**

DS4 defines critical success factors as:

- A no-break power system is installed and regularly tested.
- Potential availability risks are proactively detected and addressed.
- Critical infrastructure components are identified and continuously monitored.
- Continuous service provision is a continuum of advance capacity planning, acquisition of high-availability components, needed redundancy, existence of tested contingency plans, and the removal of single points of failure.
- Action is taken on the lessons learned from actual downtime incidents and test executions of contingency plans.
- Availability requirements analysis is performed regularly.
- Service level agreements are used to raise awareness and increase cooperation with suppliers for continuity needs.
- The escalation process is clearly understood and based on a classification of availability incidents.
- The business costs of interrupted service are specified and quantified where possible, providing the motivation to develop appropriate plans and arrange for contingency facilities.

It defines key goal indicators as:

- No incidents causing public embarrassment
- Number of critical business processes relying on IT that have adequate continuity plans
- Regular and formal proof that the continuity plans work
- Reduced downtime
- Number of critical infrastructure components with automatic availability monitoring

Key performance indicators—Measuring effectiveness

- Number of outstanding continuous service issues not resolved or addressed
- Number and extent of breaches of continuous service, using duration and impact criteria
- Time lag between organizational change and continuity plan update
- Time to diagnose an incident and decide on continuity plan execution
- Time to normalize the service level after execution of the continuity plan
- Number of proactive availability fixes implemented
- Lead time to address continuous service shortfalls
- Frequency of continuous services training provided
- Frequency of continuous service testing

Appendix E: References

International, cross-industry standards

- AS/NZ 4360 Risk Management Standard; Business Continuity. Addendum currently under international peer review.
- AS/NZ 4390 Records Management Standard.
- AS/NZ 4444 Information Security Standard; includes business continuity section.
- ISO 17799 Code of Practice for information security management; includes business continuity management section. It provides a comprehensive set of defined risks and controls (formerly BS 7799 now revised to BS 7799-2002).
- ISO 9002 quality assurance standard; addresses risk management and continuity planning issues for compliance.
- NFPA 1600 (under review into 2004; clearly a benchmark potentially a requirement) benchmark for continuity and emergency planners' strong focus on crisis communications. Potential international implications with broad support in the U.S. public sector.

Standards and guidelines for financial and technology industries

- Basel Committee—13 countries with 30 working groups set framework for appropriate risk management environment with guidelines on risk identification, measurement, monitoring, and control; focus on international banking supervision.
- CobiT Control Objectives for Information and Related Technology.
- COSO Committee of Sponsoring Organizations of Treadway Commission—International framework to help management better control business activities using assessing internal controls and consistent monitoring.
- FFIEC Information Systems Examination Handbook.
- FFIEC Handbook Volume 1 at <http://www.ncua.gov/ref/ffiec/vol1bm.pdf>.
- FFIEC Handbook Volume 2 at <http://www.ncua.gov/ref/ffiec/vol2bm.pdf>.
- Related glossaries, presentations, and resources at <http://www.ffiec.gov/ffiecinbase/index.html>.
- OCC policies on bank examinations at <http://www.fdic.gov/regulations/information/information/s3c29.pdf>.

From now on, all specific BC requirements for financial institutions will probably come from the Federal Financial Institutions Examination Council (FFIEC), rather than its individual member agencies (FDIC, FRB, Treasury Department, OCC, OTS, and NCUA).

According to the FFIEC, "The loss or extended interruption of business operations, including central computing processing, end-user computing, local area networking, and nationwide telecommunications poses substantial risk of financial loss and could lead to failure of an institution. As a result, contingency planning now requires an institution-wide emphasis."

The FFIEC criteria are based in part on previous agency-specific BC regulations:

- OCC Circular 177, Corporate Contingency Planning, 1989
- OCC 97-23, Interagency Statement on Corporate Business Resumption and Contingency Planning, <http://www.occ.treas.gov/ftp/bulletin/97-23a.pdf>
- FFIEC Policy SP-5, Joint Statement, 1997
- NCUA letter 109
- FDIC FIL-68-97 <http://www.fdic.gov/news/news/financial/1997/fil9768.html>

- FDIC FIL-67-97
- FFIECR-67

Guidelines for publicly traded companies on stock exchanges

- **Turnbull Guidelines (UK)**—Address business continuity, risk management, and appropriate internal controls for companies listed on the London Stock Exchange, which first mandated requirements of this type. Stock exchanges around the globe are watching the impact this has when the compliance date has been reached and what the domino effect will be.
- **NYSE (proposed) Rule 446**—Addresses business continuity, risk management, and appropriate internal controls for companies listed on the New York Stock Exchange. NASD has required that all of its members implement risk management and business continuity programs.
- **Sarbanes-Oxley Act (2002)**—Requires auditors (internal and external) to provide a detailed report on a company's internal controls to the SEC. This will be published in the annual reports in its entirety.

Regulations related to privacy, security, risk management, and corporate governance

- HIPAA (U.S.)—Includes seven specific BCM points with 2003 compliance by large corporations. Includes federal civil and criminal penalties.
- Expedited Funds Availability Act (U.S.)—Demonstrated BC plans to ensure prompt availability of funds (federally chartered financial institutions).
- Gramm-Leach-Bliley Act (U.S.)—Wide range of organizations providing financial services beyond banks (for example, auto dealers, retail stores, financial planners, tax preparers, and insurance and real estate industries) requiring appropriate controls in place for a strong focus on client privacy. An unusual addition to this act is that it also includes vendors and suppliers to the institutions identified.
- Presidential Decision Directive (PDD) 63 (U.S., 1998)—Calls for an effort to ensure the security and continuous availability of critical infrastructures (physical, IT, and telecommunication) by 2003.
- Telecommunications Regulations 2000 (UK).
- Australian Commonwealth Criminal Code (December 2001 update)—Establishes criminal penalties for officers and directors of organizations that experience a major disaster and fail to have a proper business continuity plan in place.
- Telecommunications Act of 1996 (U.S.).
- Foreign Corrupt Practices Act (FCPA)—Addresses internal controls and criminal penalties.

Additional regulations and guidelines

- Computer Fraud and Abuse Act of 1986, revised 1996
- Computer Security Act of 1987, Public Law 100-235
- Federal Financial Institutions Examination Council (FFIEC): Information Systems Examination Handbook
- Federal Reserve Commercial Bank Examination Manual, Section 4060 Computer Services
- Federal Deposit Insurance Corporation, BL-22-88: Contingency Planning for Financial Institutions
- Federal Reserve Board, Policy Statement, SR89-16: Interagency Policy on Contingency Planning for Financial Institutions SP-5
- Federal Reserve Board, Policy Statement, SR97-15 (SPE): Corporate Business Resumption and Contingency Planning SP-5
- Federal Reserve Board, Policy Statement, SR98-9 (SUP): Assessment of IT in the Risk-Focused Framework

- Federal Reserve Board, Policy Statement, SR00-3 (SUP): Information Technology Examination
- Frequency Updates, Risk Assessments, and Controls
- Federal Reserve Board, Policy Statement, SR00-4 (SUP): Outsourcing of Information and Transaction Processing, Risks, Risk Management, Penalties, International Considerations
- Information Technology Governance Institute: Control Objectives for Information Technology (CobiT)
- Office of Management and Budget, OMB Circular A-130
- Office of Management and Budget, OMB Bulletin 90-08
- Office of the Comptroller of the Currency, (OCC), BC 177, Corporate Contingency Planning
- Office of Thrift Supervision, (OTS), TB 30, Interagency Policy on Contingency Planning for Financial Institutions
- U.S. Department of the Treasury, Internal Revenue Service Manual 2.1.10
- U.S. Department of the Treasury, Internal Revenue Service Manual 1.2.7.9
- National Institute of Standards and Technology, Special Publications 800-34, Contingency Planning Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology

Other file retention and protection requirements

Electronic Funds Transfer Act

<http://www.occ.treas.gov/netbank/ebguide.htm>

The Electronic Fund Transfer Act (EFTA) establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services.

Graham-Leach-Bliley Act of 1999

<http://www.ftc.gov/privacy/glbact/glb-faq.htm>

This act includes record retention requirements to prove compliance with privacy regulations.

USA Patriot Act

<http://www.ustreas.gov/press/releases/po3034.htm>

This act includes record retention requirements to prove compliance with Section 326, Customer Identification Program (CIP).

Foreign Corrupt Practices Act of 1977

<http://www.usdoj.gov/criminal/fraud/fcpa/>

This act holds management personally responsible for the “reasonable protection of information systems” and provides for civil and criminal penalties for both corporations and their officers.

For more information

- <http://www.hp.com/go/businesscontinuity>
- HP Business Continuity & Availability Solutions Brochure, HP 2004
- HP Business Continuity Services Brochure, 2004

© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

5983-1677EN, 03/2005

