



A BC Overview of Sarbanes-Oxley, HIPAA and Graham-Leach-Bliley Acts

Jack Goldman, Business Protection Systems International, Inc.

What you should know about
legislation affecting our business.

©2003 Communication Technologies, Inc., All Rights Reserved.
Reprinted from *Continuity Insights* magazine. Contents cannot be reprinted without permission from the publisher.

WWW.CONTINUITYINSIGHTS.COM

IN A LITTLE OVER A YEAR, THREE FEDERAL AGENCIES issued final rules that will pose business continuity management (BCM) challenges to the vast array of companies that are covered by these rules. This article is an overview of those rules, the underlying statutory policies, the BCM implications and the compliance requirements that are mandated by the rules.

The Rules

On May 23, 2002, the Federal Trade Commission (FTC) issued a final rule under the Graham-Leach-Bliley Act (GLB), entitled *Standards for Safeguarding Customer Information*, that became effective one year later on May 23, 2003 (the Safeguard Rule). The Safeguard Rule was preceded by the adoption of the GLB *Privacy Rule* that established privacy standards for consumer and customer information and measures for consumers to restrict the use of that information by financial institutions. In general, the Safeguard Rule “requires each financial institution to develop a written information security program that is appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue” for the safeguarding of customer information. The Safeguard Rule is deceptive in its brevity and requires careful study to grasp the scope of the definitions and its impact on covered entities.

On February 20, 2003, the Department of Health and Human Services (DHHS) published the long-awaited *Final Security Regulations* under HIPAA that became effective on April 21, 2003, with a compliance deadline of April 21, 2005 (the Security Rule). The Security Rule requires covered entities that possess, process or transmit electronic protected health information (E PHI) to do the following:

- Ensure the integrity, confidentiality and availability of E PHI
- Protect E PHI against reasonably anticipated threats or hazards to its security or integrity and unauthorized use or disclosure
- Ensure that their employees comply with the Security Rule

The HIPAA *Privacy Rule* that became effective in April, 2003, applies to all forms of protected health information, including paper records. Finally, on June 5, 2003, the Securities and Exchange Commission (SEC) published final rules for Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) that will be effective on June 15, 2004, for all SEC reporting companies with a market capitalization in excess of \$75 million and on April 15, 2005, for all other companies that file periodic reports with the SEC (the *404 Rules*). The 404 Rules require CEOs and CFOs of public companies, as part of the company’s 10-K annual report, to provide a written internal control report and certification that assesses the effectiveness of the company’s internal controls system and

financial reporting procedures. In general, the annual internal controls report must acknowledge (1) management’s responsibility to establish and maintain an internal control structure and procedures for financial reporting and (2) management’s assessment of the effectiveness of the internal control structure and procedures at year’s end.

The 404 Rules also require the accountants who issue a report on the company’s financial statements to provide a written attestation on the internal controls assessment of the management. The framework that is used by reporting companies for management’s evaluation must be a broadly recognized internal control framework.

Compliance with each set of rules requires the establishment of an infrastructure that is designed to protect and preserve information, records and data from loss, destruction, alteration or unauthorized use and access. Covered companies are required to assess the risks in their business environments that may present compliance problems and to adopt controls to provide reasonable assurance that those risks are minimized—which can be accomplished through policies, procedures and control processes throughout the enterprise. Each of the rules provides for designated management employees to assume responsibility and accountability for compliance or certification of compliance. Noncompliance can result in civil or criminal penalties, liability and criminal prosecution for responsible companies and individuals. Although the rules stress the protection, preservation and retention of records and data, their principal purpose is the establishment of a control environment that will govern how transactions are to be carried out, recorded and reported in accordance with management’s authorization and applicable policies and procedures.

The GLB Safeguard Rule and HIPAA’s Security Rule mandate the adoption of processes that are designed for the protection and preservation of designated *personal information*. The 404 Rules under SOX require the adoption of internal controls that assure transactions are carried out as authorized by management and are correctly recorded and that the records of those transactions be preserved and protected from loss or alteration. Best practices compliance measures for all of the rules would include an effective internal controls environment and emphasis on appropriate business continuity (BC) methodologies. Consequences of compliance failures, in addition to the penalties mentioned above, can result in loss of reputation, loss of trust with the public and loss of enterprise value—all threats to BC. Each rule has specific requirements for compliance that are addressable through BCM processes. All of the rules stress the need for a strong sense of ethics to support compliance programs.

Covered companies are required to assess the risks in their business environments that may present compliance problems and to adopt controls to provide reasonable assurance that those risks are minimized.

| BC Overview |

Characteristics of the GLB Safeguard Rule

The Safeguard Rule requires all companies that meet the definition of a “financial institution” to “develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards” to protect “customer information” from loss, unauthorized disclosure or misuse. Customer information is any information (in electronic or other form) identified with the customer (individuals and not businesses) that is maintained by or for a financial institution and derived from the relationship between the financial institution and the customer. The Safeguard Rule delineates five separate elements of the information security program:

1. Designating an employee to coordinate its information security program to ensure accountability and achieve adequate safeguards
2. Identifying reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in unauthorized disclosure, misuse, destruction or other compromise of such information (Three separate areas of risk are mentioned for assessment in each area of operations.)
3. Designing and implementing information safeguards to control the identified risks and regular monitoring to test the effectiveness of the safeguards
4. Overseeing service providers (defined as any business that receives, maintains, processes, or is permitted access to customer information in the course of its services)
5. Evaluating and adjusting the information security program in light of testing and monitoring results and material changes in business, operations or other known circumstances

The Safeguard Rule requires a typical BCM program with each financial institution having the ability to design its information security program in a manner that is appropriate to its size, complexity, the nature and scope of its activities and the sensitivity of the customer information concerned. The individual elements of the process would consist of risk assessment, policy and procedure development, assignment of responsibility and accountability, security, backup and recovery measures, testing and maintenance, and communication and education within the organization. Since regulated financial institutions currently operate under contingency planning mandates, the information security program that is required by the Safeguard Rule can be a subset addition to an existing BCM program. Neither the Safeguard Rule nor the

GLB Act contains any formal structural or technology requirements for an information security program.

Characteristics of the HIPAA Security Rule

The Security Rule, in contrast to the Safeguard Rule, is lengthy and highly structured. Covered entities (entities that possess, transmit or process EPHI) must adhere to four fundamental requirements of the Security Rule through the following:

1. Ensuring the integrity, confidentiality and availability of EPHI
2. Protecting EPHI against any reasonably anticipated internal or external threats or hazards to its security or integrity
3. Protecting EPHI against uses or disclosures that are not permitted by the HIPAA Privacy Rule
4. Ensuring that members of the covered entities' workforce comply with the Security Rule

Three terms, *integrity*, *confidentiality* and *availability* have specific applicability. *Integrity* means that EPHI is not modified or destroyed without proper authorization; *confidentiality* means that EPHI is not disclosed or made available for any purpose without authorization; and *availability* relates to the need for EPHI to be accessible and usable when needed by authorized persons.

The Security Rule does not specify what security measures covered entities must employ to implement the standards and

implementations that are specified in the rule. In selecting appropriate security measures, a covered entity must take into account (1) its size, complexity and capabilities; (2) its technology infrastructure and capabilities; (3) the costs of the security measures; and (4) the probability and criticality of potential risks to EPHI. Cost is not a factor that will excuse compliance, but may be considered one of the factors in deciding which security measures to use. The rule specifies three categories of security safeguards. The first, *Administrative Safeguards*, are implemented through nine standards; the second, *Physical Safeguards*, are implemented through

Noncompliance can result in civil or criminal penalties, liability and criminal prosecution for responsible companies and individuals.

The Committee of Sponsoring Organizations (COSO) has released for industry review a draft of their Enterprise Risk Management document. A copy can be downloaded from www.erm.coso.org.

Several states are in the process of implementing laws/regulations similar to the governance requirements of SOX, including California and Massachusetts. Many of these potential state laws are looking to expand the SOX requirements to all businesses, including those in the private sector. BCM planners should be aware of what the various States are doing in this arena.

Chart 1

	Graham-Leach-Bliley Safeguard Rule	HIPAA Security Rule	Sarbanes Oxley 404 Rules	California SB 1386
Effective Date	May 23,2002	April 21,2003	June 5,2003	July 1,2003
Compliance Deadline	May 23,2003	April 21,2005	June 15,2004 (for public companies with market cap.of \$75 million or more) June 15,2005 (for other SEC reporting companies)	
Covered Entities	Financial Institutions as defined in the Bank Holding Company Act that possess, process,transmit private customer information	Organizations that possess, transmit,process electronic protected health information (EPHI)	Publicly owned companies that file periodic reports with the SEC	Any public or private entity that has unencrypted electronic personal information of California residents
Purpose	Protect Customer Information from unauthorized disclosure or use	Protect EPHI from unauthorized disclosure or use	Provide senior management assessment of effectiveness of company's "internal controls for financial reporting" and attestation by independent auditors	Protect California residents from Identity Theft
Operative Mechanism	Information Security Program <ul style="list-style-type: none"> • Responsible employee selection • Risk assessment • Information safeguards and controls • Oversight of "service providers" • Testing and monitoring 	Security Safeguards <ul style="list-style-type: none"> • Risk assessment • Policies and procedures to control access • Physical security measures • Contingency plan • Appointment of security officer • Training and communication to increase awareness • Audits and maintenance of audit trails • Agreements with "business associates" • Testing and evaluation 	Internal Control Framework (COSO Framework or equivalent) <ul style="list-style-type: none"> • Control environment— compliance and ethics • Risk assessment and analysis • Control activities—policies, procedures,control mechanisms to limit risks • Information and communication • Monitoring of operations and control activities to determine continuing effectiveness of internal controls 	None Specified (GLB or HIPAA type security measures should be acceptable) Encryption of personal information eliminates need for other compliance measures
Criminal Consequences of Noncompliance	Fines and imprisonment for up to 5 years	Fines to \$250,000 and imprisonment for up to 10 years	Fines up to \$5 million and prison sentences for up to 20 years for deliberate violations	Civil liability to any injured California resident

Chart courtesy of Jack Goldman.

four security standards; and the third, *Technical Safeguards*, are implemented through five security standards. Not all of the security standards that are included within the security safeguards are required. Those that are designated as "addressable" may be omitted if, after assessment, it is determined that implementation of that safeguard is not reasonable and appropriate for the covered entity and the reasons for the nonimplementation are documented. Implementation of "required" safeguards is mandatory.

From a BC perspective, the security safeguards require covered entities to assess and develop measures to mitigate potential identified risks and vulnerabilities from within and outside the organization. Policies and procedures governing

access to EPHI are to be implemented to control access to systems and information by personnel and by outside parties as well. Physical security measures are required to be developed, documented and implemented throughout the information technology (IT) infrastructure. A contingency plan that will set procedures for backup and recovery, emergency operation, recovery priorities and testing and revision also is required. Additional requirements include appointment of a security officer, communications and training within the organization to create awareness of the security measures, periodic evaluation of the technical and nontechnical components of the security program, audits of systems and use and maintenance of audit trails, and entering

Congressman Oxley Weighs in on the Sarbanes-Oxley Act

| BC Overview |



The Sarbanes-Oxley Act celebrates its first anniversary. (L to R) William J. McDonough, Senator Mike Enzi (WY), Senate Banking Committee Chairman and coauthor of the Sarbanes-Oxley Act of 2003 Paul Sarbanes (MD), Michael G. Oxley (OH), and William H. Donaldson.

Congressman Michael G. Oxley (R-OH), coauthor of the Sarbanes-Oxley Act of 2002, takes a moment to discuss the Act with *Continuity Insights*:

“A year after its enactment, we’re really beginning to see the impact of the corporate responsibility reforms approved by Congress in response to corporate misdeeds. The new law has already been invoked in at least two cases.

“But the impact of the law goes much further than that. In addition to the reforms set out by the Act, there are many steps being taken by securities regulators and in the business community to defend the honor of upright businesses all across America. An important aspect of the Act is what I’ve seen referred to as the trickle-down effect. This is the idea that although Sarbanes-Oxley only applies to public companies, it is raising the bar for private and nonprofit businesses as well. These secondary benefits will be a very important part of the law’s legacy. Healthy free markets thrive on a steady diet of transparent and accurate information. In elevating the standards for public companies, we’re boosting the principles under which the entire business community operates to the benefit of all investors.

“In a September hearing, our Committee heard testimony from SEC Chairman Donaldson and the chairman of the accounting board created by Congress on their ongoing work to implement the law’s provisions. In Sarbanes-Oxley, Congress gave the Commission and the accounting board needed flexibility to deal with unforeseen issues that will inevitably arise as the Act is implemented.

“I applaud both the SEC and the Public Company Accounting Oversight Board (PCAOB) for their willingness to work with all parties to ensure that the goals of the law can be met in a most efficient and unduly burdensome manner; however, it will take a great effort on the part of everyone in the business community to deliver on the promise held out by the Act.

“I am pleased to see reports that some companies are even taking extra steps, going beyond what is required of them by the new regulations, to protect their employees, their investors and uphold their reputations. I commend such pioneering in the business community.”

agreements with “business associates” that will provide assurances that EPHI will be protected as required by the Privacy Rule. The Security Rule also places emphasis on documentation of policies, procedures, access controls and other compliance communications and appropriate records retention measures.

Characteristics of the 404 Rules

An understanding of the 404 Rules starts with the definition of the term *internal control over financial reporting*. It denotes a process designed by or under the supervision of senior management and effected by the board of directors and senior management to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with generally accepted accounting principles (GAAP) and includes policies and procedures that do the following:

- Pertain to the maintenance of records that accurately and fairly reflect the transactions and dispositions of assets of the company
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of GAAP financial statements and that receipts and expenditures are being made only in accordance with management’s and the board’s authorizations
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of assets that could have a material effect on the financial statements

In the annual evaluation of internal controls over financial reporting, the SEC acknowledged that the COSO Framework (the 1992 report of the Committee of Sponsoring Organizations of the Treadway Commission on Internal Control—Integrated Framework, as supplemented in 1994) satisfied its criteria for purposes of management’s annual internal control evaluation and disclosure requirements.

The COSO Framework has five basic elements:

1. Control Environment—the tone of the organization and its people toward compliance and ethical standards and that



Senator Sarbanes and Congressman Oxley.



Congressman Michael G. Oxley, House Financial Services Committee Chairman and coauthor of the Sarbanes-Oxley Act of 2002.

| BC Overview |

everyone is responsible for internal controls.

2. Risk Assessment—assessing financial, operational and regulatory risks to the organization and how the risks are to be managed.
3. Control Activities—policies, procedures and control mechanisms to minimize or eliminate identified risks (including risks of ethical lapses within the organization).
4. Information and Communication—identification, capture and communication of pertinent information to enable responsibilities to be carried out and how the information is communicated throughout the organization as well as into and out of the organization (how clear and timely is the message communicated).
5. Monitoring—a process that assesses the quality of the system's performance over time, monitoring of operations and reporting of internal controls deficiencies upstream to senior management and the board.

All of these elements are fundamental to a BCM program, and the process for internal controls reporting amounts to a BCM project. With an effective internal controls program that meets the COSO Framework, reporting companies will have fewer challenges in complying with other SOX requirements:

- Section 302 quarterly CEO and CFO disclosure controls certifications
- Section 409 real-time disclosures of material changes
- Section 906 representations by certifying officers
- Reduced exposure to disclosures of material weaknesses in internal controls in annual assessments and attendant negative consequences
- Reduced exposure to noncompliance with the Foreign Corrupt Practices Act of 1977

(COSO has released for industry review a draft of their Enterprise Risk Management document.)

Recent State and Congressional Compliance Measures

HIPAA and GLB explicitly allow states to adopt their own privacy and security measures. Many states have responded by enacting laws that mirror and even surpass federal privacy regulations for HIPAA- and GLB-protected information. One recent noteworthy addition is California's Senate Bill 1386, a measure designed to reduce the national explosion of identity theft. It became effective on July 1, 2003. SB 1386 requires any organization that possesses unencrypted electronic personal information of California residents (a person's name and, in addition, any combination of either a social security number, credit or debit card number, bank account number, driver's license number, in combination with any password, access code, or security code that would permit access to a person's financial account) to provide written notification to them of any unauthorized disclosure or misuse of the information. This law affects public agencies and all businesses, wherever located, as long as they possess personal information

of California residents. In June, 2003, Senator Feinstein introduced a similar bill in the U.S. Senate, called NORPDA (Notification of Risk to Personal Data Act). Under SB 1386, any organization that has unencrypted personal information of California residents must adopt measures to protect the security of the information from unauthorized disclosure or use. Measures that would comply with the GLB Safeguard Rule or the HIPAA Security Rule should be adequate SB 1386 compliance measures. (Laws such as California SB 1386 also apply to all businesses that deal with entities in California, whether or not they are located in California.)

Common BC Connections and Conclusion

A broad common public policy is served by all of these rules and laws—safeguarding information and assets from unauthorized access or misuse. There is a common connection with each of the rules and information. It is a grave mistake to view compliance as a data backup or records management challenge. Each of the rules includes a compliance structure that consists of the following:

- An assessment of internal and external risks (including operational, financial and regulatory risks)
- Control activities to mitigate and contain the risks
- Emergency or contingency plans to operate during and to recover from disruptive incidents
- Communications throughout the organization to promote an environment that encourages compliance and ethical conduct
- Monitoring, testing and maintaining the control systems to ensure appropriate measures are taken to promote continued compliance

These are basic elements of enterprise-wide BCM programs. Compliance with these measures is a serious matter. Noncompliance can result in civil damages and penalties, prosecution, imprisonment and criminal fines. It is possible that compliance lapses may result in serious consequences under more than one of the rules simultaneously.

One overriding benefit that compliance measures under a COSO Framework or similar structure will provide is a more resilient enterprise. This alone is justification for all covered organizations to make the effort and devote the time, funds and resources to comply with all of these rules and laws that are applicable.

Jack Goldman is a corporate lawyer with Miller & Holguin (Los Angeles, CA) and CEO of Business Protection Systems International, Inc. (Riverside, CA). He can be reached via e-mail at jgoldman@businessprotection.com or jgoldman@millerholguin.com.

WWW.CONTINUITYINSIGHTS.COM