Running head: DATABASE AND COMPLIANCE

The Effect of Compliance on Database Integrity, Security and Administration

Patti Jessup

July 10, 2007

Abstract

The dawn of the 21st century saw advances in technology that allowed consumers and businesses to communicate and complete routine and complex transactions using a new vehicle – the internet. This new medium quickly became the status quo for millions of consumers to procure everything from mortgage loans to prescription refills. However, every cloud has a silver lining and a dark side. The dark side quickly materialized in the form of corporate mismanagement scandals, identity theft and privacy violations. New compliance regulations began to take shape in an effort to mitigate these issues. These regulations touch every aspect of a business from financial reporting to firewall configurations.

Companies and organizations scrambled to find ways to automate and monitor their businesses in an effort to comply with these regulations. Some companies found themselves responsible for complying with multiple regulatory requirements. The corporate governance industry was born and continues to thrive today.

Data Management is a key component of the governance roadmap. A company or organization's data must be protected from unauthorized access both internally and externally, and its integrity certified by key executives. The following table highlights the importance of data security and privacy common to many of the regulations now facing organizations.

Common Regulation Controls

Mandate	Processes and Risk Management	Content and Records Management	Data Security and Privacy	Training
Cross Industry				
Sarbanes-Oxley Act	x	x	x	x
HIPAA		x	x	x
California Senate Bill 1386			x	x
International Accounting Standards	x	x	x	x
EU Data Privacy Directive			x	x

Federal Sentencing Guidelines				x
Industry Specific				
Basel II	x			x
Gramm-Leach-Bliley			x	x
SEC17A-3/4		x		x
FDA 21 CFR Part 11	x		x	x
Freedom of Information Act		x		x
USA Patriot Act		x	x	x

Many companies do not recover from a data breach and no company wants to make headlines because they just lost the credit card numbers of their customers or they have to re-state earnings due to invalid reporting. An organization's data must be verified for integrity and protected on an ongoing basis in order to prevent the occurrence of such events. These requirements are a primary focus in compliance regulations.

"Database security once only the concern of the database administrator is now a key topic among executives. "With multiple industry regulations continuing to be the dreaded thorn in the side of most database administrators and security practitioners, the notion of database compliance is a significant challenge. When coupled with the growing difficulty in making a concrete distinction between data and databases, database compliance issues have created a horde of unanswered questions." (Foster, 2006).

Today, databases store most of the world's data. They have become the favored storage vehicle for nearly every type of application. Database has become synonymous with data. Companies are increasingly investing in methods and best practices to meet compliance regulations and to protect their data from loss and breach. The database administrator is out of the computer room and into the boardroom.

Top 3 Compliance Regulations

Compliance regulations span every level from state to federal. However, there are 3 compliance acts that effect most major industries and organizations.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act was enacted July 30, 2002 as a response to recent corporate scandals at Enron, WorldCom and Tyco. The act centers on financial reporting and accounting practices of publicly traded companies.

Sarbanes-Oxley addresses the duties of the Chief Executive Office (CEO), the Chief Financial Officer (CFO), and the Auditor. The Act details the reporting requirements along with the rules and regulations for financial reporting. This Act makes management personally responsible for ensuring the credibility of the financial reporting provided to its stakeholders. When misleading information is discovered, it carries stiff penalties for the CEO, CFO, and Auditor [3]. The SEC and the PCAOB (Public Company Accounting Oversight Board) enforce this legislation, with sections VIII, IX, and XI of the Act detailing penalties for non-compliance with the Act. There are eleven sections defining auditor and corporate responsibilities, including expectations for financial disclosures, strong penalties for white-collar crimes, and protection for “whistleblowers”[4, 5]. The three most obvious sections of relevance for the CIO are 302 and 404 because they deal with the internal controls that a company has in place to ensure the accuracy of their data. Section 409 is also important because material changes affecting financial disclosures must be reported on a rapid and current basis. This means systems must be able to provide timely information within days, not weeks, of an event. Although initially scheduled for implementation in 2004, the compliance dates for several sections of SOX have been extended, specifically section 404 that deals with compliance on proof of internal controls. Depending on a company’s status as an "accelerated filer”, a nonaccelerated firm, or a foreign private issuer, the compliance date is the first fiscal year ending on or after November 15, 2004

> (accelerated) or July 15, 2005 (others). Part of the justification for this extension has been the uncertainty about the real impact of SOX and the unexpected amount of process and systems changes anticipated to achieve compliance [6, 7]. (Kaarst-Brown & Kelly, 2005)

Of all the emerging compliance regulations, SOX compliance has had the largest impact on corporate governance. "The Sarbanes-Oxley Law of 2002 ("SOX") has been called the most significant new securities law since the Securities and Exchange Commission was created in 1934. SOX places substantial additional responsibilities on officers and directors of public companies, and impose very significant criminal penalties on CEOs, CFOs and others who violate various provisions of SOX." (Braun Esq & Stahl PhD, 2005). Even privately held corporations who aspire to become public in the future, must be aware of the basic requirements of operating a public company under SOX regulations and prepared to accept this responsibility upon public offering.

In 2005, Pillsbury Winthrop Shaw Pittman LLP estimated $35 Billion had been spent on SOX section 404 Compliance to date. AMR Research estimated SOX compliance spending for just 2005 at $6.1 Billion. ((North, 2005)

Health Care and Insurance Portability and Accountability Act (HIPPA)

HIPPA was one of the first significant attempts to mandate a standard of care in the field of health care with regard to electronic transmission of patient data. Hospitals, Insurance Companies, Physicians, Laboratories and employers who provide health plans are all subject to HIPPA compliance.

> HIPAA information security regulations require covered entities to do the following to protect "individually identifiable health information." 6
>
> • Ensure the confidentiality, integrity, and availability of all electronic protected

health information the covered entity creates, receives, maintains, or transmits

• Protect against any reasonably anticipated threats or hazards to the security or integrity of such information

• Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or otherwise required

• Ensure compliance by its workforce.

HIPAA is a broad ranging act and has spawned significant regulation. Importantly, because it affects so many different entities, we can expect that the standards required by HIPAA will have a significant meaningful impact on non-health care related industries. (Braun Esq & Stahl PhD, 2005)

Failure to comply with HIPAA electronic data, security or privacy requirements can result in monetary penalties of up to $25,000 per year, for each standard violated. The penalty for using private information for commercial or malicious purposes is punishable by 1 to 10 years in prison, plus fines of $50,000.00 to $250,000.00

Gramm-Leach-Bliley (GLB)

In 1999, Congress passed the Gramm-Leach-Bliley (GLB) Act to regulate the use and disclosure of personal information (nonpublic) regarding customers who obtain or seek products or services from financial institutions.

At first glance GLB seems to apply only to financial institutions; however, its broad definitions encompass any entity that engages in financial transactions (i.e. brokerage dealers, registered investment advisors, mortgage lenders, collection agencies, credit counselors, tax attorneys, certified public accountants).

From the standpoint of maintaining the privacy of customer information, GLB generally

prohibits a financial institution from disclosing non-personal public information to a nonaffiliated third party, either directly, or through an affiliate, unless the institution has disclosed to the customer, in a clear and conspicuous manner, that the information may be disclosed to a third party; has given the consumer an opportunity to direct that the information not be disclosed; and described the manner in which the consumer can exercise the nondisclosure option.

Financial institutions must also prepare and make public *privacy statements* which describe the institution's policies with regard to disclosing non-public personal information to affiliates and non-affiliated third parties; disclosing non-public personal information of persons who have ceased to be customers of the institution; and the categories of non-public personal information the institution collects. The institution is required to disclose clearly and conspicuously those policies and practices at the time that it establishes a customer relationship and not less than annually during the continuation of the customer relationship. This has resulted in an avalanche of paper from banks, brokerage houses, accountants and others who provide financial services.

In addition to regulating how financial institutions may intentionally share information, GLB also regulates what steps a business must take to prevent the unintentional sharing of nonpublic personal information in its computer systems. Each of the different federal and state agencies having GLB jurisdiction have written separate information security safeguard regulations. While no two are identical, all have a similar flavor:

- Executive management involvement
- Risk- and vulnerability-driven, based on regular assessments
- Written information security policies
- Employee training

- Control of 3rd-parties

There has also been a spill-over effect from regulation under the GLB Act. The key regulator under the GLB Act is the Federal Trade Commission, and its experience has spurred it to explore areas not directly implicated under the GLB Act.[4] Additionally, many of the industries which are directly impacted by the GLB Act, such as the banking and insurance industries, are beginning to apply the standards imposed on them to their clients. For example, insurance companies are beginning to review privacy statements and policies of their insureds, and banks are beginning to consider these issues in their underwriting decisions. (Braun Esq & Stahl PhD, 2005)

Effect of Regulatory Compliance on Data Management

SOX section 404 mandates segregation of duties. This segregation must also include access to systems. For example, the DBA can no longer have access to the root password for the UNIX operating system. Although this may seem to be a simple fix, the reality is that when the 2:00 am system error occurs, both the System Administrator and the DBA will have to address the issue, rather than just the DBA. This requirement is especially burdensome to the small to medium sized company where the system administrator is also the database administrator.

Under SOX section 404 these must be separate job functions OR provide an adequate audit trail to document changes or alterations to the system. If physical segregation of duties is not in place, external and internal auditors will expect documentation of system access controls. Unfortunately this can be a rather daunting task and quite expensive for the company. The cost of auditing this documentation by an external auditing firm alone can be cost prohibitive for the small organization. The ISACA guidelines for accomplishing this documentation are: (ISACA Professional Resources, 2005)

Audit trails—Audit trails are an essential component of all well-designed systems. They help the IS and user departments as well as the IS auditor by providing a map to retrace the flow of a transaction. They enable the user and IS auditor to recreate the actual transaction flow from the point of origination to its existence on an updated file. In the absence of adequate segregation of duties, good audit trails may be an acceptable compensating control. The IS auditor should be able to determine who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.

Reconciliation—Reconciliation is ultimately the responsibility of the user. In some organizations, limited reconciliation of applications may be performed by the data control group with the use of control totals and balancing sheets. This type of independent verification increases the level of confidence that the application ran successfully and that the data are in proper balance.

Exception reporting—Exception reporting should be handled at the supervisory level and should require evidence, such as initials on a report, noting that the exception has been handled properly. Management should also ensure that exceptions are resolved in a timely manner.

Transaction logs—A transaction log may be manual or automated. An example of a manual log is a record of transactions (grouped or batched) before they are submitted for

processing. An automated transaction log or journal provides a record of all transactions
processed, and it is maintained by the computer system.

Supervisory reviews—Supervisory reviews may be performed through observation and inquiry or remotely.

Independent reviews—Independent reviews are carried out to compensate for mistakes or intentional failures in following prescribed procedures. These are particularly important
when duties in a small organization cannot be appropriately segregated. Such reviews will
help detect errors or irregularities.

Based on the 2007 CSI/FBI Computer Crime and Security Survey, Data protection is clearly at the top of the critical issues list for most organizations. Out of the 31 critical categories, Data protection ranked #1 among the 426 survey respondents, with policy and compliance ranking a close second. Clearly both of these topics are on the minds of most organizations today and each is considered in the methodology design for controlling, managing, and auditing the other.

Compliance has had a sobering effect on data and its management within the organization. Once thought of as the "mysterious answer box" by many executives, compliance and regulatory requirements have placed the certification of data accuracy and integrity at the doorstep of the executive offices and therefore, at the top of the budgetary fiscal expenditure list.

How much does it cost to secure and verify the integrity of your corporate data? Given that databases are deployed across the organization and typically serve as the backbone storage

engine for most applications, hundreds or thousands of databases may be "live" within the organization. Depending upon the state of these databases and the degree of data management best practices deployed, securing your data to appropriately meet governance requirements can easily consume your IT budget. However, the focus of achieving a level of acceptable corporate governance is moving away from PC controls to creating and implementing security policies and controls against the core information engine – the database. "While many companies' have focused primarily on fixing compliance automation technologies onto their PCs messaging systems and other fast-moving elements of IT infrastructure, creating smarter policies and controls for the database provides a baseline for all audit-related efforts Starting in the database and brining governance efforts to the top of compliance strategy is one way to foster better relationships between IT and internal and external auditors to better prepare for compliance reviews." (Ponemon, 2007)

The more accurate question --- what is the cost of a security breach against your corporate data or effect on the companies stock price, should earnings have to be restated?

> "Over the past few years, as the frequency and gravity of security breaches have increased, there have been several attempts to estimate the cost of a security breach. These estimates, however, have churned out vastly different figures. For example, a study of U.S. Department of Justice cases, published in August 2006, determined that the average loss per incident was $1.5 million. These calculations conflicted with a 2005 CSI/FBI survey that estimated the cost to be $167,000. Meanwhile, a 2006 Ponemon Institute survey figured the average cost to be $4.8 million per breach.3 And if that dizzying array of estimates isn't bewildering enough, a recent Forrester survey found that 25% of respondents do not know, or do not know how to determine, the cost of data security breaches….However, the undeniable fact is that the vast majority of

organizations will incur additional costs, sometimes significant enough to put them our of business." (Kark, 2007)

Issues with corporate financial reporting can have an equally serious effect, resulting in significant value loss per share or at its worst, executives serving hard time and the company out of business.

.Both of these situations lead companies to focus their capital budgets on securing their data. The cost of not doing so is too great to assume.

Database Compliance and Governance Requirements

The functionality of your particular database software determines if recommended best practices to meet regulatory compliance can be consolidated, automated or remain manual. For example, information life cycle management (ILM) is a function that can be automated within one instance of an Oracle database; however to achieve this within other database engines the data must be kept in separate physical databases. Whatever the method, the following are areas that require a concentrated effort in order to insure database compliance with regulatory acts such a SOX, HIPPA and GLB.

1. Authorization: Companies must insure that sensitive data is protected from unauthorized access both internally and externally.
2. Change Management: Proper change management must ensure that changes to the system (hardware and software) are controlled and documented.
3. Disaster Recovery Plan: A documented and auditable verification of successful plan execution for disaster recovery, within a reasonable time, for financial systems of record. This includes systems containing financial data that may not be "mission critical" to the organization.
4. Secure backup and transmission of data to authorized sites only. Must be performed

and routinely verified to ensure the data is secure.

5. Clear separation of duties between administrators with access to systems containing sensitive data.

All of these best practices center on the ability of the database administrator to effectively audit and document audit results. "More than merely tracking and monitoring user activity, database auditing encompasses all aspects of database information controls and safeguards including: access policies, configuration standards, sensitive data usage, and vulnerability management practices. Auditing is an important component of a defense-in-depth approach to database security. After all, privacy, integrity, confidentiality of data and accountability for changes to that data are core, driving forces behind the need for audit." (Ponemon, 2007).

Compliance requirements have increased the scrutiny of measurable database controls Questions range from the general to the specific. 1)What are we doing to protect and audit access to the customer database? 2)Does our compliance effort include assessing controls on the e-commerce backend? There are five major components of database auditing:

1. Non-Privileged User Access and Activity Auditing Defines who is authorized to access the system and what they can do. Documents who accessed which systems, when, and how.

2. Privileged User Access and Activity Auditing Identifies what activities were performed in the database by administrators and other privileged users. Documents who accessed which systems, when, and how.

3. Suspicious Activity and Attack Signature Auditing Flags any suspicious, unauthorized or abnormal access to sensitive data or critical systems.

4. Vulnerability Assessment and Threat Auditing Detects vulnerabilities in the database, then monitors for users attempting to exploit them. Identifies threats and

related countermeasures.

5. Database Schema and Configuration Change Auditing Establishes a baseline policy for configuration, schema, users, privileges and structure, then tracks deviations from this baseline. (Ponemon, 2007)

Many database software providers are including enhancements to automate database compliance. Currently Oracle leads in this area of functionality; however, IBM and Microsoft have also taken steps to provide increased auditing and security functionality within their database engines. Without automation to some degree, compliance auditing becomes an unmanageable and virtually impossible task to undertake and maintain successfully.

Care should be taken to insure that auditing policies maintain a degree of flexibility to allow for additions to the IT infrastructure. Auditing features provided by the database vendor typically include this flexibility. Manual procedures that are undertaken by the organization should also take IT infrastructure expansion into consideration during the analysis phase without compromising the underlying security goals.

Prior to implementing an auditing methodology, organizations must first determine the systems that require this type of extensive auditing. Although, at first glance, this should seem apparent, it is not as easy as it looks. Over the years, many databases were implemented in response to application implementations at a departmental level. This is especially true in companies where IT was organized using a distributed methodology rather than a centralized organization. In many cases these were departmental applications (i.e.: datamarts) rather than enterprise wide. Therefore, redundant data may be present within the organization and there may be sensitive data housed in these systems. It may not be apparent that these systems even exist during an overview audit of existing systems. These systems are also prime targets for

unauthorized access, as they generally do not adhere to the more stringent security requirements of enterprise-wide systems.

Although, documenting and securing these systems may take a large amount of effort on the part of the organization, it is a mandatory exercise. A data breach of these systems would be much more costly.

. Once these systems have been identified, further analysis should ensue to determine if they require a separate database or can they somehow be integrated into the more secure enterprise-wide database systems. The more database systems that can be consolidated into one database store, the easier managing, auditing, and maintaining compliance becomes.

Database Administrators are also finding themselves under the "hot lights" when corporate audits are underway. The following is a list of questions a DBA should be prepared to answer/demonstrate during an internal or external compliance audit. (Lemme, 2006)

- Have data integrity ownership and responsibilities been communicated to appropriate data/business owners and their acceptance of responsibilities?
- Are key database systems inventoried, owners identified and documented?:
    - Number of databases and instances
    - Type and version of the database software installed
    - Type and version of the underlying operating system
    - Database users and privileges compared with user system security
    - Related applications accessing or transacting with the database
    - Utilities and tools that can access, manage or change the database or data
    - Organization charts identifying system owners and maintainers
- Do you have change management so you can attest to any changes or alterations?

- Where are the risks to financial data stored in databases documented? How often are they reviewed and updated?
- Is the data that is extracted, archived or backed up properly secured and tracked?
- How is division of roles and responsibilities (segregation of duties) set up so that it prevents a database administrator (DBA) from unauthorized data viewing, alterations or deletions?
- What are the database management process controls? Where are they documented for review? What monitoring and reporting do you have in place? Can you demonstrate this (pick randomly) one to me now?
- When was the last time the database management control methods were tested, gaps identified and controls improved?
- Do you understand and accept the responsibility regarding internal controls for the databases you manage?

Conclusion

Although compliance mandates have proven to be a challenging and costly endeavor for today's organizations, the result has provided many key improvements in data integrity and security across the enterprise. Companies are realizing that their data is their livelihood and are taking the necessary precautions to protect, validate and secure that data. Whether or not they are forced into this realization by various regulations is really beside the point, the resulting benefits are the same.

References

Application Security, Inc, (January 29, 2007), *Database Auditing Leading Practices.* [Whitepaper]

*Braun Esq, R., & Stahl PhD, S. (2005). *An Emerging Information Security Minimum Standard of Due Care*. Los Angeles, CA: Citadel Information Group, Inc.

Brewer, D. C. (2006, June 6). . Retrieved June 18, 2007, from www.datamanagement.com: http://searchdatamanagement.techtarget.com/originalContent/0,289142,sid91_gci11923 8.

*Connor, B., Noonan, T., Holleyman, I., & Robert, W. (2005). *Information security governance: Toward a framework for action* (Business Software Alliance)

Foster, J. C. (2006, January 18). *Database Compliance Demystified*. Retrieved June 18, 2007, from SearchSecurity.com: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1229016,00.html.

*Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *CSI/FBI computer crime survey* (Tech. Rep. No. 11, p. 27). Computer Security Institute.

Hines, M. (November 9, 2006). Website: www.eweek.com Retrieved June 18, 2007, from http://www.eweek.com/article2/0,1895,2055066,00.asp.

Hurley, J. (2004). *The Struggle to Manage Security Compliance for Multiple Regulations*, Symantec [Whitepaper]

*ISACA Professional Resources, 2005, CISA Review Manual, Chapter 2 - Management, Planning and Organization of IS, pp 88-91.

*Kaarst-Brown, M. L., & Kelly, S. (2005). IT governance and sarbanes oxley: The latest sales pitch or real challenges for the IT function. *Proceedings of the 38th Hawaii International Conference on System Sciences.*

*Kark, K. (2007, April 10). *Calculating the Cost of a Security Breach* (Forrester Research Inc., Ed.). . Cambridge, MA.

Lane, A. (Chief Technology Officer). (2005). *A Database Security Management White Paper: Securing the Information Business Relies On*. .

Lemme, S. (2006, July 7). *Regulatory Compliance and the DBA: What you need to know*. Retrieved June 18, 2007, from SearchDataManagement.com: http://searchdatamanagement.techtarget.com/originalContent/0,289142,sid91_gci1198079,00.html.

Lourie, S. (2005, October 20). Five Compliance Questions to Ask your CEO. *CIO Magazine.*

Mullins, C. (2006, March 3). . Retrieved June 18, 2007, from www.dbazine.com/blogs/glog-cm/craigmullins/blogentry.2006-03-20.1641871205.

North, K. (2005). *Weak Compliance Puts Database Users at Risk* (North Summit Media, Ed.).

Oracle Corporation. (June 2005). Oracle's Compliance Architecture: A Roadmap to Sustainable Compliance and Governance Best Practices. [Whitepaper]

*Ponemon, L. D. (2007, June 4). *2007 Survey on Database Security* (Application Security, Inc., p. 13). .