SANS ANALYST PROGRAM

Sponsored by Lumigent

The SANS Database Audit and Compliance Survey

A SANS Whitepaper – February 2008

Written by Barbara Filkins

Regulation: The Organizational Driver

The Data: It's Personal

Compliance: Perception vs. Practice

Database Controls: Management vs. Compliance

Product Dreams: Compliance and Audit

Summary

Responses to the SANS 2007 Database Audit and Compliance survey demonstrate a clear need for methods and tools to monitor compliance with regulations and protect sensitive information in databases. The survey also reveals that organization's perceptions of their compliance status differ from how compliant they really are.

The majority of respondents (87 percent) consider data privacy and its protection as important or very important to their organizations, and 82 percent say the need to protect sensitive data has risen in organizational awareness over the past three years. Overall, 70 percent of survey respondents say they meet basic regulatory or internal standards for compliance well or very well. Yet only 39 percent feel that they have a true handle on data mapping, while 25 percent say they have no data classification model or active data classification initiative underway.

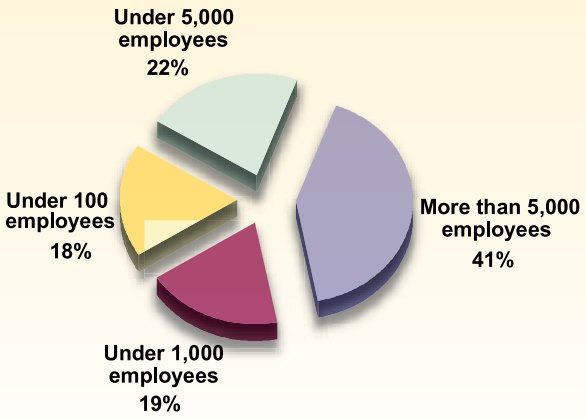
The drivers for this raised awareness are also clear from the survey. Most organizations are subject to more than one regulation affecting the controls placed on sensitive data. In fact, 60 percent of respondents consider data auditing and regulatory compliance mandatory for their company to conduct business.

The survey attracted respondents from a variety of industry sectors, primarily financial (24 percent), information technology (18 percent), and government (16 percent).

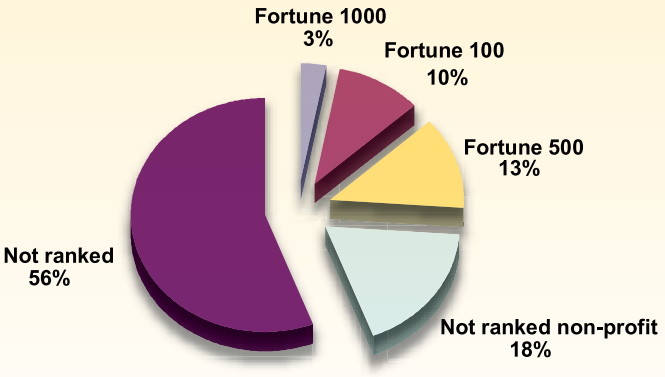
Forty-one percent of respondents came from organizations with over 5,000 employees, although only 26 percent consider their firm as belonging to the Fortune rankings.

With respect to their roles, the majority of respondents (52 percent) consider themselves to be hands-on IT staff, including database administrators (DBAs) and developers. Twenty-nine (29) percent are involved in IT and/or security-related management at all levels, and the remaining 19 percent include specialists, such as auditors, personnel involved with the organization's data as end-users, business unit managers, or outside consultants.

Survey Respondent Size Distribution



Respondent Revenue Ranking



Regulation: The Organizational Driver

Regulations are the primary driver for establishing data compliance and audit requirements. Survey respondents overwhelmingly (74 percent) feel their organizations utilize data that is or might be considered regulated.

Regulations are grouped into several basic rule sets based on the primary focus of the specific regulation. Privacy is a theme that permeates most of the health and financial services regulations. The following table presents the percentage of total respondents affected by each regulation. As you can see from the high percentages on multiple regulations, individual organizations are dealing with two or more regulatory rule sets.

REGULATION	PERCENT
Health/Pharmaceutical	
21 CFR Part 11 (FDA)	8.6
Health Insurance Portability and Accountability Act (HIPAA)	36.8
Privacy	
Federal privacy laws (e.g., Federal Privacy Act, FERPA)	37.5
California SB 1386	11.9
Other state privacy laws	25.7
Financial	
Basel II	6.7
Gramm-Leach-Bliley Act (GLBA)	21.2
Sarbanes-Oxley (SOX)	44.2
Payment Card Industry Data Security Standard (PCI DSS)	25.3
Energy	
Federal Energy Regulatory Commission (FERC)	4.1
North American Electric Reliability Corporation (NERC)	1.9
Other	
Federal	7.8
State	0.7
International	3.7
Miscellaneous	3.0
Unknown	**12.6**

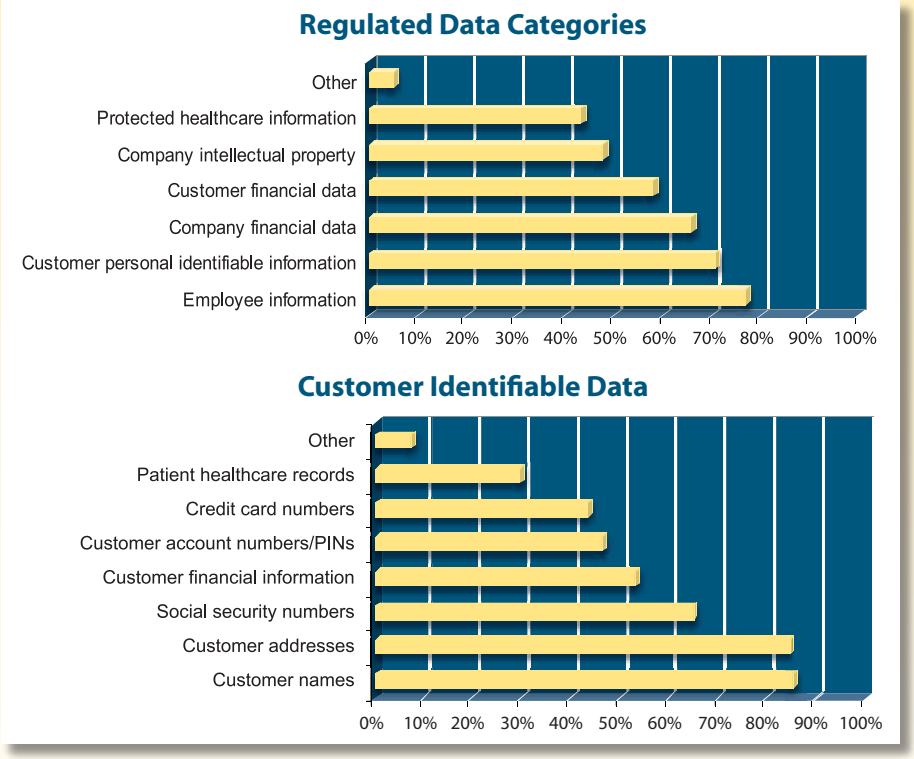
The Data: It's Personal

No wonder there is a market trend toward identifying effective methods and procuring appropriate tools for data audit and compliance. Eighty-seven (87) percent of all respondents rate the criticality of data privacy and its protection as important to their organization. Eighty-two (82) percent consider that this emphasis on data privacy has increased over the past three years. Additionally, 64 percent report that recent, publicly-announced data breaches have impacted their organization's focus on data privacy and its protection.

Single organizations deal with an overwhelming amount of regulated data. The emphasis is on information related to individual privacy as opposed to financial data or intellectual property, a fact consistent with the emphasis placed on personal privacy by both privacy and financial regulations.

For those organizations that collect, process, and store specific customer-identifiable data, items that fall (or might fall) under data privacy policies include customer names and addresses, social security numbers, customer financial information, account numbers and PINs, credit card numbers, and patient healthcare records. The graph below shows the emphasis that respondents place on each item.

Interestingly, customer names and addresses, essential data in any demographic database, are ranked the highest in terms of the need for protection, whereas information still associated with a person — but somewhat abstracted (i.e., SSN and credit card numbers) — is not considered as critical.



Compliance: Perception vs. Practice

Most organizations are comfortable with their current ability to meet compliance and auditing requirements. Seventy (70) percent of survey respondents believe they meet the basic regulatory or internal standards for compliance well or very well. This perception is not clearly supported by their actual practices. Seventy-eight (78) percent address databases and database systems in their compliance and data protection requirements. However, only 39 percent feel that they have a true handle on data mapping. A fairly high percentage (25 percent) indicates their organizations have no data classification model or active classification initiative underway.

If an internal practice is a means to manage and control compliance with external demands, the percentage of organizations with an internal practice should be fairly high (50 percent or greater) in the more regulated industries. Surprisingly, healthcare, which has high regulatory demands, demonstrates the lowest percentage of organizations having an internal compliance program for data privacy and its protection.

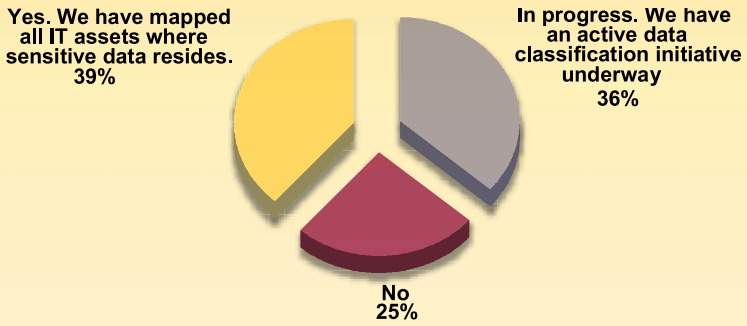
The respondents' false sense of compliance may stem from the organizations having a framework to ensure compliance and support auditing functions. Sixty-eight (68) percent have at least one internally-developed ISO-based or ITIL-based framework.

INDUSTRY SECTOR	% WITH INTERNAL COMPLIANCE PROGRAM
Media	100
Telecommunications	71
Financial Services	60
Government	58
Energy & Utilities	50
Retail	50
Entertainment	50
Information Technology	47
Other	46
Pharmaceutical	40
Education	33
Manufacturing	33
Healthcare	27

Another reason for the distorted sense of compliance may be a disparity between those held accountable for the protection of the data and those actually responsible. Accountability for protection of privacy data, including any data stored in databases or database systems, falls mainly (43 percent) to IT management or executive staff, whereas the daily protection of the privacy data in these same databases and systems, in practice, falls mainly (43 percent) to the database administration staff.

Twenty-two (22) percent of respondents do not know how much time their staffs spent engaged in auditing and compliance activities for data privacy. ***Recall that 29 percent of those actually completing the survey are involved in IT and/or security-related management, the same group accountable for the protection of privacy data.*** This raises a concern that management is not fully aware of the resource demands involved in the protection of the information for which they are accountable.

Data Mapping / Classification



Database Controls: Management vs. Compliance

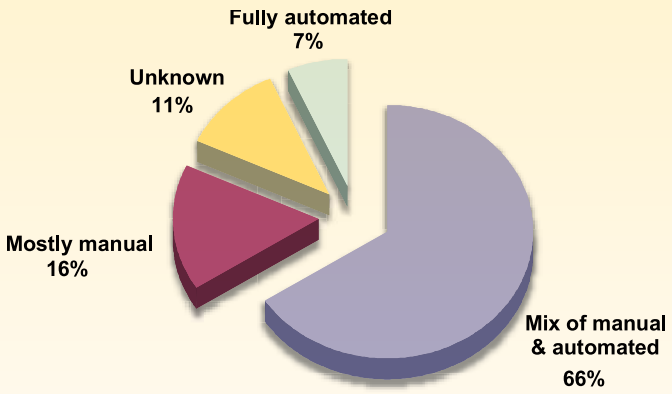
Sixty-two (62) percent of respondents indicate that they have some type of system in place for auditing and compliance that meets some or all of their needs, with 39 percent of these working to improve the systems they have. Of the 29 percent that do not have a system, less than half (11 percent) plan to deploy a system for audit and compliance.

Sixty-six (66) percent of respondents currently use a mix of manual and automated database controls. The distribution is shown on the left.

Most organizations use more than one database version or product and multiple operating systems. Microsoft products are dominant: 75 percent use Microsoft SQLServer, and 83 percent use Microsoft Windows.

Results show a significant dependency on native auditing for database compliance. Forty-six (46) percent depend on native database capabilities to collect database activity for compliance and auditing, with 21 percent combining the native capability with internally-developed custom applications. This is interesting given that many native auditing tools, such SQLServer Profiler Trace, are best described as methods for event capture. These native capabilities can be leveraged to build a more complete auditing solution through internally-developed or commercial applications. By themselves, however, they are nothing close to a next-generation database auditing solution with features such as statistical profiling of user access behavior, automatic detection of anomalous activity, and real-time alerting in response.

Database Controls Automation



Product Dreams: Compliance and Audit

The product characteristics for database auditing or compliance solutions that most organizations desire correlate with respondents' current levels of automation in the following ways:

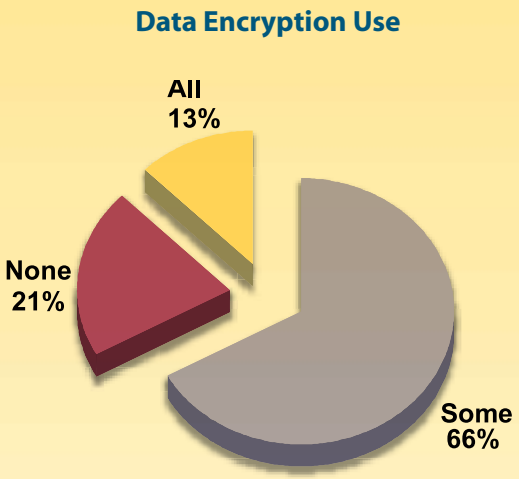
- Organizations that are fully automated feel that all items presented in the survey as possible product features are at least somewhat important. All others are more selective, with a percentage of each group indicating some features as not important or not applicable.
- Organizations that are fully automated are less concerned with impacts due to performance. For these organizations, protection of published database vulnerabilities, blocking of database access or specific commands, ability to archive database activity audit records, and handling of encrypted data for auditing and compliance purposes are rated equally.
- Organizations with manual or unknown processes are less concerned with the ability to archive database activity records. They're concerned with performance, detection of published database vulnerabilities, and the handling of encrypted data were rated the highest importance.

MOST IMPORTANT PRODUCT FEATURES:	ORGANIZATIONS WITH DATABASE CONTROLS THAT ARE: FULLY AUTOMATED	A MIX OF MANUAL AND AUTOMATED	MOSTLY MANUAL	UNKNOWN
Detect published database vulnerabilities	50%	45%	43%	42%
Block database access or specific commands	50%	33%	33%	47%
Archive database activity audit records	50%	30%	23%	26%
Handle encrypted data for auditing and compliance	50%	39%	37%	42%
Track all database activity	43%	17%	23%	21%
Provide deep visibility into each database transaction	43%	18%	20%	16%
Easy to install and maintain	21%	28%	27%	26%
Impact on database performance	43%	45%	43%	47%
Separation of duties	43%	31%	27%	42%

The extent to which an organization encrypts its data also influences the emphasis it places on product features. Seventy-five (75) percent of organizations that encrypt all their data place importance on a product's ability to handle encrypted data, followed closely by the ability to detect published database vulnerabilities (71 percent). For these organizations that have already committed to encryption, performance is not cited as a key factor.

Organizations that encrypt some or none of their data, on the other hand, place the highest importance on performance, indicating they may limit their encryption of critical data due to performance impacts. These organizations are not as concerned about the ability of a product to handle encrypted data.

Ranking database events used for auditing in descending order of importance to survey respondents shows standard monitoring functions (user login tracking, failed command tracking, and changes to data values in the database) are considered least critical. More detailed and difficult tasks, such as privileged user activity and exceptions to acceptable use policy, are ranked the highest.



DATABASE EVENT AUDITING IN DESCENDING ORDER OF IMPORTANCE

- Privileged user accounts and entitlements
- Exceptions to acceptable use policies
- Privilege grants or revocations
- Account termination
- Structural changes to the database
- Privileged user activity
- Auditing who viewed private data
- Changes to data values in the database
- Failed login and command tracking
- Reconciling database changes to an approved change ticket
- User login tracking

The importance placed on the more difficult tasks reflects the distinction between database management activity tracking, which answers simple event-oriented questions (e.g., what are the number of user logins?) through the use of native tools and database auditing. It also reveals that the more complex questions related to regulatory compliance — assessment, analysis, and correlation of events across all database activity — are foremost on the minds of respondents because native database tools can't help in responding to them.

Summary

Regulatory compliance is the main reason for establishing data privacy and protection standards. Most organizations are influenced by having to comply with the demands of more than one regulatory requirement to protect personal data, each slightly different in their demands. Their overall compliance strategy is uncertain; and they're looking for ways to manage compliance across multiple systems. Based on these and other trends identified in this survey, SANS offers the following strategies:

- **Equate perception with reality.** Just having a framework should not lull organizations into the feeling that all is well. Management, who is accountable for electronic data, must understand how regulated data is being handled by end users and IT staff. Establish and track quantifiable metrics to gauge the maturity and effectiveness of the actual auditing and compliance practices.
- **Know thy data.** Know what needs to be protected, where it is located, and who — by role and responsibility — is accountable and/or responsible for its protection.
- **Account for your human resources.** Know the tasks needed for auditing and compliance in addition to routine database management. Plan for the staff time that will be required and allocate resources accordingly.
- **Select products wisely based upon understanding and organizational needs.** Understand what next-generation database auditing involves, as opposed to the current state of database monitoring. Consider the limitations of native database capabilities when it comes to auditing and compliance. Consider both the functionality needed to meet the need and the demands a product will place on the infrastructure. Develop product requirements and select a product wisely.

About the Author

Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls "policy, process, platforms, pipes, AND people." Most recently she has been involved with HIPAA security issues in the health and human services industry. She has clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system lifecycle as well as its relation to many of the issues faced by modern society that are dependent on automation — privacy, identity theft, exposure to fraud, and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold), GCIH (Silver, working towards Gold), and GHSC certifications.

SANS would like to thank the sponsor of this survey:

LUMIGENT