AltiusIT

Database Regulatory and Compliance Issues

Introduction

Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) Act were all enacted to help protect information. These acts require internal controls to protect information integrity, confidentiality, availability, and accountability. While accountants and auditors are familiar with internal controls, many IT departments lack the the knowledge and controls needed to safeguard information. Even sophisticated databases, managed by Database Administrators (DBAs), lack secure controls and and connectivity to information. Risk assessments help your organization identify, manage, and reduce its risks.

When evaluating internal controls, management and IT Database Administrators must consider a number of factors including:

- Storage – hardware, software, or external service used to store documents
- Creation – if required, allow individuals to collaborate to create documents
- Capture – Metadata information including user storing document, date & time
- Filing – how documents are organized, how ensure filed appropriately, etc.
- Retrieval – indexing, how documents are located, response times, etc.
- Workflow – if required, ensure documents are available to workgroups, document flow
- Distribution – ensure documents are available to appropriate personnel
- Security – protect against loss, tampering, or destruction, hide sensitive information
- Encryption – protect against unauthorized access, distribution
- Archival – ensure readability of information in the future, protect against disasters
- Retention – documents to be retained, retention period, how destroyed, etc.
- Authentication – documents are original and meet their standards for authentication

Compliance Regulations

Traditionally, DBAs have access to your organization's data but often times have limited access to tools that provide controls and limit internal and external threats. With the necessary technology, people, and processes, your organization can reduce threats and provide the necessary reporting for regulatory compliance. Sample compliance regulations are included in the table below.

Regulation	Risk Area
Sarbanes-Oxley Section 302	Unauthorized changes to data
Sarbanes-Oxley Section 404	Modification to data, unauthorized access
Sarbanes-Oxley Section 409	Denial of service, unauthorized access
Gramm-Leach-Bliley Act	Unauthorized access, modification, disclosure
HIPAA 164.306	Unauthorized access to data
HIPAA 164.312	Unauthorized access to data
Basel II – Internal Risk Management	Unauthorized access to data
Code of Federal Regulation Sec 11	Unauthorized access to data

Audit Logs

Most vendors include security controls and auditing capabilities as a part of their database package. Unfortunately, the controls must be implemented by your organization's DBA. Without sufficient knowledge and understanding of internal controls, the DBA frequently makes a "best guess" of the type of information to be tracked and reported. Basic auditing might include successful and unsuccessful logon attempts. Many audit trails provide great volumes of data, but not much information. In addition, simply turning on auditing is not sufficient as the raw data must be reformatted into information that can identify "regulatory" type of events.

Many database vendors provide auditing tools. Unfortunately, these tools, when not properly used, can require volumes of CPU time, disk space, memory resources, and archiving. Audit logs clearly require sufficient available resources to maintain database performance.

Trend Analysis

Database vendors typically provide tools that will search a database audit file for specific access violations. While this is beneficial information, it is not sufficient to protect against internal threats which come from employees authorized to access the database. Consider a technical support employee authorized to access customer records. On a routine day, he might access 50 records. Accessing 100,000 records in a day might be an indication of data theft. This scenario can only be detected by trend analysis.

DBA Access to Information

Many DBAs have complete access to all of your organization's data. While complete access helps manage and minimize downtime, it also puts your organization at risk as the DBA has access to all information and log files. Your management must determine the minimum amount of access needed to allow the DBAs to perform job duties. For example, must the DBA have access to confidential or sensitive data such as payroll, protected health information (PHI), or other types of confidential information?

Internal Controls

Most regulations are concerned with effective internal controls with appropriate reporting and procedures, detecting unauthorized use of systems, controlling and verifying access to information, an independent risk assessment and audit.

Risk assessments help your organization:

- Identify risk areas
- Analyze risks
- Risk Response
- Risk Control

Security audits review technology, people, and processes to identify risk areas and ensure policies and procedures are in place to mitigate risk. Audits ensure that your organization has taken the appropriate steps to protect information. These “reasonable efforts” include, but are not limited to:

- Auditing - turned on, log files secured, and reviewed in a timely manner
- Authentication - user access to systems approved by management, passwords expire
- Change Management - formal testing, approval procedures
- Risk Management - Single Point of Failure (SPOF) analysis, business continuity
- Patch Management - software is tested and patched in a timely and appropriate manner
- Documentation - terminated employees have database access removed

A 50+ point network security audit can help your organization comply with regulations and protect your information assets.

Database Audit Trails

Sample database audit trails and reporting include, but are not limited to:

- Scripts run daily to confirm all accounts that exist on the system are approved
- Quarterly review all access to applications and databases
- All key system passwords are periodically changed
- Access to databases and systems is limited to DBAs
- Auditing of access to key data at a database level
- Protected database schema (database design)
- Change management processes, testing, and approvals when moving programs into production

Database Firewalls

When selecting a new database management system, determine if the vendor offers auditing, reporting, and data management tools. In addition, the software should provide application level security and interface to your organization's corporate-wide procedures for granting access to systems. For example, authentication should allow a secure protocol, such as Secure Sockets Layer (SSL). In addition, data may need to be encrypted to ensure additional protection.

Application security gateways and database firewalls understand the application and track user access. Deep packet inspection examines each packet going over the network to the database server to determine the type of access being attempted. Application security gateways can provide other benefits such anomaly-based Intrusion Detection System, a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.

Some protection systems also have modules that provide compliance information specifically targeted to SOX and HIPPA. Unfortunately if you use certain types of encryption on the traffic going directly to the database then a firewall that uses deep packet inspection will be prevented from reviewing the packets.

Software Tools

Software vendors offer a variety of tools to manage internal and external threats and address regulatory compliance issues. Sample tools include:

- Oracle Database Vault and Secure Backup (encrypts backup data)
- IPLocks - assesses the vulnerability of databases, monitors data users, forensic auditing of logs
- Imperva's SecureSphere monitors and protects sensitive information
- Guardium's SQL Guard network based appliance intercepts network traffic going to and from the database

Summary

Electronic document management and communications solutions allow organizations to control costs and improve their operational efficiencies. To manage these risks, organizations will implement solutions that address the liabilities associated with electronic records and communications. Network security audits help organizations identify, manage, and reduce their risks.

Publication Information

Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.