ecora

WHITEPAPER

A Strategic Approach to Gramm-Leach-Bliley Act Compliance

Ensuring Compliance and Security on the IT Infrastructure

Alex Bakman
Chairman and Chief Technology Officer
Ecora Software

About the Gramm-Leach-Bliley Act

When the Gramm-Leach-Bliley Act (GLBA) was signed into law in 1999, the goal of the legislation was "to enhance competition in the financial services industry by providing a framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers…." The law made consumer insurance, banking, and investment information accessible through a single source. At the same time, the law mandated that any organization with access to non-public customer information—including financial institutions, insurance companies, credit card companies, debt collection agencies, and real estate settlement firms—meet stringent administrative, technical, and physical safeguards to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Staying Compliant; Staying Secure

Until now, for most organizations, compliance has been driven by events—like a security breach or network outage—which led to a review of the IT infrastructure and security controls, and external and internal pressure to make improvements. With the advent of significant new regulations like the Gramm-Leach-Bliley Act, however, ensuring compliance has become a business requirement, and concerns about new corporate and regulatory requirements have made compliance a top-of-mind issue for executives and the organizations they lead. In fact, a published report from a leading research firm stated that "compliance spending in 2006 will reach $27.3 billion. Spending will climb even higher in 2007, with companies devoting $28 billion to compliance initiatives."

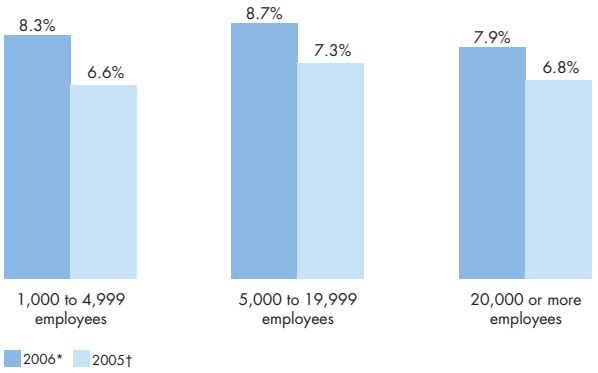
The challenge for many organizations lies in the common misconception that compliance and security are equal, and, by achieving compliance, an organization will ensure infrastructure security and vice versa. According to Khalid Kark, senior research analyst at Forrester Research Inc., security and compliance are two distinct issues; compliance does not always equal security, and the real challenge is to remain compliant while staying secure.

"There are two broad trends," Kark said during a recent Ecora webinar. "Because of well-publicized security breaches, many organizations have taken a broad view and consider security in terms of the possible risk to corporate information. At the same time, regulatory pressures and compliance requirements have dominated the agenda, so organizations are focusing on just one particular area and not looking at security holistically. **To get desired results, organizations must address both information risk and compliance through a comprehensive corporate governance framework.**"

In recent years, implementing this comprehensive governance framework has been made more difficult because the annual investment in security spending is dropping.Kark added that sometimes this funding has been redirected to compliance at the expense of security. "To be both compliant and secure, organizations need to shift their thinking from responding to tactical IT security issues like firewalls, intrusion detection systems, viruses and worms, system hardening, and encryption to addressing information risk and more strategic business concerns, such as protecting intellectual

What's happening to security spending?

"Approximately what percentage of your IT spend will go toward security?"



Base: 370 IT execs at North American Enterprises
Base: 528 IT execs at North American Enterprises
*Source: *Forrester's Business Technographics' November 2005 North American And European Enterprise IT Budgets And Spending Survey*
†Source: *Forrester's Business Technographics' November 2004 North American And European Benchmark Study*

property, ensuring regulatory compliance, preventing insider abuse, and safeguarding customer privacy," he said. "The result can be a comprehensive program that addresses both information risk and compliance concerns within an organization."

FFEIC *IT Examination Handbook* as a Framework to Ensure Compliance and Security

The Federal Financial Institutions Examination Council (FFIEC) designs and supervises audits for the majority of federal agencies that oversee organizations that must comply with GLBA. To ensure that all auditors work within uniform principles, standards, and report forms, the FFIEC publishes the *IT Examination Handbook*. The *Handbook* was substantially revised and expanded in July 2006 and can now provide a clear framework for an organization's compliance/security program, including a five-step security process:

1. Information Security Risk. Identify and assess threats, vulnerabilities, attacks, probabilities and outcomes.
2. Information Security Strategy. Mitigate risk by integrating technology, policies, procedures, and training, approved by the board.
3. Security Controls Implementation. Define and implement specific roles and responsibilities, and ensure that sufficient knowledge, skills, and motivation exist to fulfill the duties; acquire and operate technology to support security controls.
4. Security Monitoring. Assure that risks are appropriately assessed and mitigated and that controls are effective and performing as intended.
5. Security Process Monitoring and Updating. Gather and analyze information regarding new threats and vulnerabilities, actual attacks on the organization or others combined with the effectiveness of the existing security controls.

Kark believes that if an organization addresses the issues, meets the objectives, and follows the security process outlined in the *Handbook*, they will meet GLBA requirements, while ensuring that all information remains safe, private, and secure. In fact, many of the security standards outlined in the *Handbook* are fulfilled when an organization accurately documents and reports on the information held within their IT infrastructure.

Four Pillars of GLBA Compliance

According to Kark, there are "four pillars" of GLBA compliance, and these "pillars" represent the essential elements of an effective compliance strategy.

1. Focus on the policies. To begin, Kark said, an organization must identify their business requirements (which encompass regulatory requirements), and define clear policies to meet them and understandable metrics to measure and document success. To ensure effective enforcement, information about policies should be communicated clearly with employees, contractors, and other third parties. Compliance with policies (or violations of policies) should be measured, tracked, and reported.

   - Can you track, report, and manage changes to processes?
   - Do you have a system for controlling configurations?
   - At any given point in time, do you know the roles and responsibilities of those who have access to non-public customer information?
   - Do you have resources in place to manage changes to regulations?

2. Manage change. According to Kark, managing change is critical to ensuring both compliance and security, and organizations should be equipped to manage change at four levels: processes, configurations, roles and responsibilities, and regulations.

   "Given the effort required to manage change at all levels, automation is the only way to ensure an efficient, controlled change process," Kark said. "Organizations shouldn't be reluctant to automate controls."

3. Concentrate on user training and awareness. Training employees, contractors, and other third parties is central to an effective compliance/security program. Roles and responsibilities should be clearly defined, and each user should understand what is expected of them. In addition, key messages about the compliance/security program should be reinforced throughout the organization—whether at employee meetings, in company newsletters, or using other means—to build awareness.

4. Monitor third parties. Kark explained that it is essential for organizations to ensure that contracted third parties have security controls in place to protect customer data; assuming that such controls exist can be a recipe for disaster, and auditors will expect evidence of due diligence. In addition, organizations should establish and monitor service levels that clearly state how data will be used and protected, and then be prepared to take action if third parties do not meet security requirements.

"Implementing these pillars is integral to a good compliance program," Kark says, "and will help an organization achieve sustainable information security while staying compliant with regulatory requirements."

How Ecora Can Help

Ecora's industry-leading software solution, Auditor Professional, collects detailed configuration, asset, and security information from throughout an organization's IT infrastructure—including operating systems, database management systems, servers, applications, and network devices. The information collected includes:

- Password Settings
- SSL Settings
- Local Users and Groups
- Terminal Server
- Logins
- Local Policies
- TCP-IP Settings
- Domain Users & Global Groups
- AD Group Policy Object
- SSH Configurations
- NTFS Shares & Permissions
- IP Routing
- Server Hardware
- WINS Server Settings
- DHCP Server Settings
- DNS Server Settings
- File and Print Information
- SNMP
- Scheduled Jobs
- Network Services
- Custom File Checksums
- Network Interface Cards
- IPX/SPX Settings
- Partitions and Replicas
- Groups, Organizational Roles, & Profiles

Once collected, this data is available through a centralized configuration database for reporting, auditing, baselining, and change tracking. With Ecora software solutions, organizations can generate customized reports or any of the more than 2,000 audit-ready report templates included in Auditor Professional that show configuration changes and deviations from standards; identify problems, such as a security breach or rogue system; highlight the impact of a new service; validate access controls; document existing systems to provide a baseline for disaster recovery; and more. Plus, Ecora's Executive Dashboard allows an at-a-glance view of compliance status, with a green-red pie chart that provides a summary across selected systems for each policy or standard for rapid assessment of IT controls, alignment with policies, and problem identification and remediation.

Realize these Benefits with Ecora Software

- Assess your current security controls prior to an audit
- Generate "audit-ready" reports for auditors
- Detect and mitigate security vulnerabilities
- Reduce trouble tickets by 50% over time
- Standardize configuration settings across all systems
- Reduce the time spent resolving trouble tickets by 50%
- Migrate to new platforms confidently
- Increase IT Staff Efficiency through Closed-Loop Validation
- Increase Revenue-Generating Service Offerings

The FFIEC IT *Examination Handbook* was updated and expanded in July 2006, and clearly outlines procedures an organization should follow when undertaking risk assessment and risk management. Examination procedures are divided into two tiers: Tier I assesses an institution's process for identifying and managing risks, and Tier II provides additional verification where risk warrants it. Ecora software provides significant support in meeting nearly all of the procedures and objectives outlined in the *Handbook*, particularly those at Tier II. In fact, the reports called out below represent only a sample of the reports available.

Tier I Procedures

Objective 1: Determine the appropriate scope for the examination.

Objective 2: Determine the complexity of the institution's information security environment.

Objective 3: Determine the adequacy of the risk assessment process.

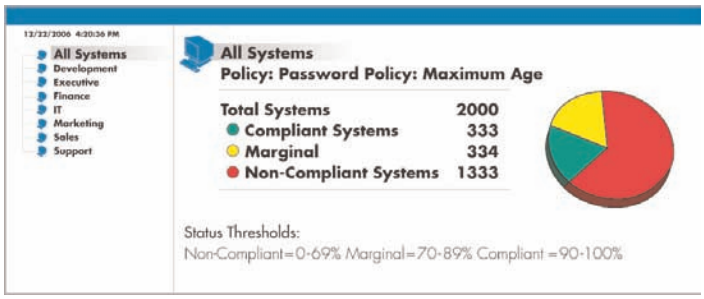
Objective 4: Evaluate the adequacy of security policies and standards relative to the risk to the institution.

Objective 5: Evaluate the security-related controls embedded in vendor management.

Objective 6: Determine the adequacy of security monitoring

Objective 7: Evaluate the effectiveness of enterprise-wide security administration.

Objective 8: Discuss corrective action and communicate findings.



Tier II Objectives and Procedures

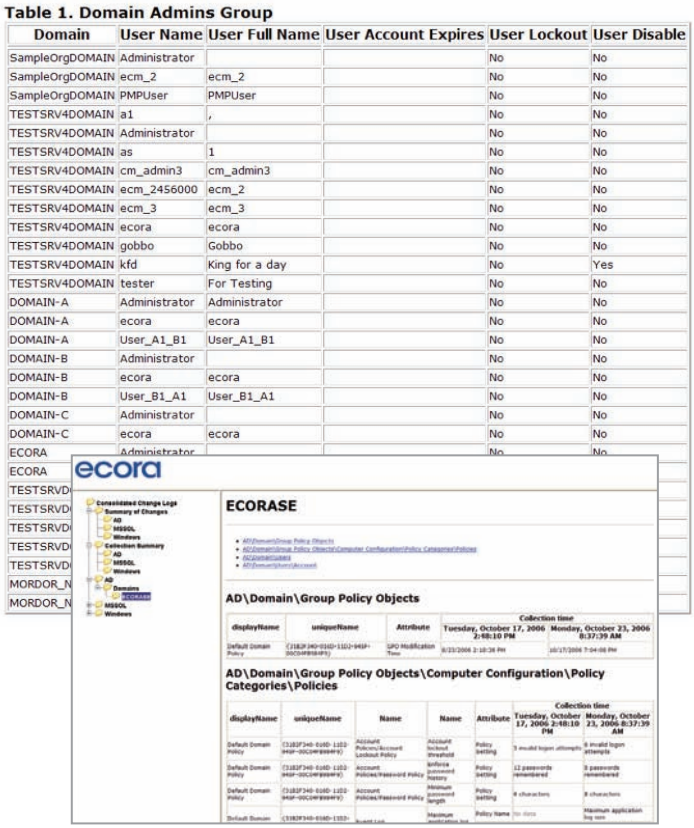
A. Authentication and Access Controls

These procedures ensure effective access rights administration and authentication.

The **Ecora Domain Admins Group Reports** helps organizations meet the requirements of **Access Controls Objective 4: Determine that administrator or root privilege access is appropriately monitored, where appropriate**.

The **Ecora Change Reports** helps organizations meet the requirements of **Access Controls Objective 5: Evaluate the effectiveness and timeliness with which changes in access control privileges are implemented and the effectiveness of supporting policies and procedures**.

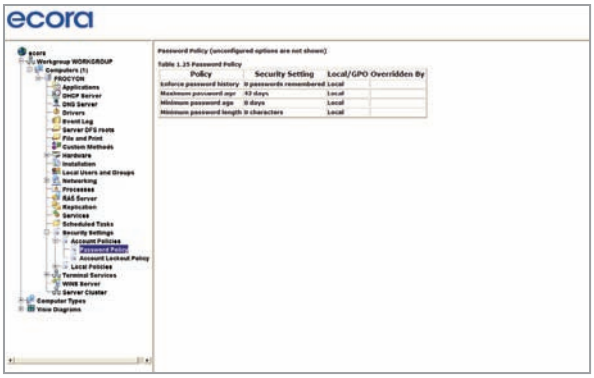
The **Ecora Log-in with No Password Reports** helps organizations meet the requirements of **Authentication Objective 1: Determine whether the financial institution has removed or reset default profiles and passwords from new systems and equipment**.



B. Network Security

These procedures ensure the effectiveness of security controls on the network architecture.

The **Ecora Documentation Reports** helps organizations meet the requirements of **Objective 1: Evaluate the adequacy and accuracy of the network architecture**.



C. Host Security

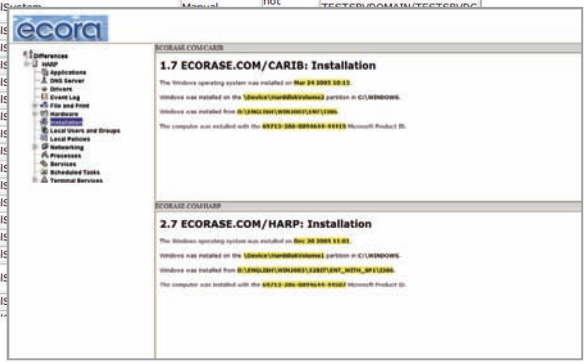
These procedures determine the security of hosts, ensuring that only those with the need to know have access credentials.

The **Ecora Services Report** by Service Name helps organizations meet the requirements of **Objective 1: Determine whether hosts are hardened through the removal of unnecessary software and services, consistent with the needs identified in the risk assessment, and that configuration advantage of available object, device, and file access controls**.

The **Ecora Baseline Comparison Reports** helps organizations meet the requirements of **Objective 4: Determine whether new hosts are prepared according to documented procedures for secure configuration or replication, and that vulnerability testing takes place prior to deployment**.

Table 1. Services Summary

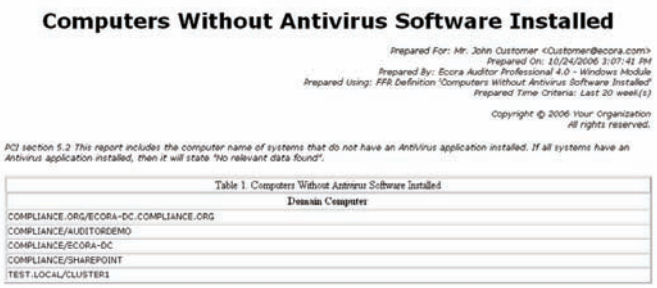
Service Name	Startup Account	Start Method	Status	Computer
Alerter	LocalSystem	Automatic	running	TESTSRVDOMAIN/TESTSRVDC
Application Management	LocalSystem	Manual	not running	TESTSRVDOMAIN/TESTSRVDC
ASP.NET State Service	TESTSRVDOMAIN\IWAM_PARENT13177	Manual	not running	TESTSRVDOMAIN/TESTSRVDC
Automatic Updates	LocalSystem	Automatic	running	TESTSRVDOMAIN/TESTSRVDC
Background Intelligent Transfer Service	LocalSystem	Manual	not running	TESTSRVDOMAIN/TESTSRVDC
Certificate Services	LocalSystem	Automatic	running	TESTSRVDOMAIN/TESTSRVDC
ClipBook	LocalSystem	Manual	not	TESTSRVDOMAIN/TESTSRVDC
COM+ Event System	LocalS			
Computer Browser	LocalS			
DHCP Client	LocalS			
DHCP Server	LocalS			
Distributed File System	LocalS			
Distributed Link Tracking Client	LocalS			
Distributed Link Tracking Server	LocalS			
Distributed Transaction Coordinator	LocalS			
DNS Client	LocalS			
DNS Server	LocalS			
Ecora Log Service for Auditor 4.0	LocalS			
Ecora Monitor for Configuration Auditor 4.0	LocalS			
Ecora Scheduler Service for Auditor 4.0	LocalS			
Event Log	LocalS			
Fax Service	LocalS			
File Replication Service	LocalS			



D. User Equipment Security (e.g., Workstation, Laptop, Handheld)

These procedures determine that proper processes are in place to ensure the security of all user equipment.

The **Ecora Computers without Antivirus Reports** helps organizations meet the requirements of **Objective 7: Determine whether systems are protected against malicious software such as Trojan horses, viruses, and worms**.



Computers Without Antivirus Software Installed

Prepared For: Mr. John Customer <Customer@ecora.com>
Prepared On: 10/24/2006 3:07:41 PM
Prepared By: Ecora Auditor Professional 4.0 - Windows Module
Prepared Using: FFR Definition 'Computers Without Antivirus Software Installed'
Prepared Time Criteria: Last 20 week(s)

PCI section 5.2 This report includes the computer name of systems that do not have an Antivirus application installed. If all systems have an Antivirus application installed, then it will state "No relevant data found".

Table 1. Computers Without Antivirus Software Installed

Domain Computer
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG
COMPLIANCE/AUDITORDEMO
COMPLIANCE/ECORA-DC
COMPLIANCE/SHAREPOINT
TEST.LOCAL/CLUSTER1

E. Physical Security

These procedures evaluate the adequacy of an organization's physical security, including processes to control facility access and procedures for the destruction of physical media.

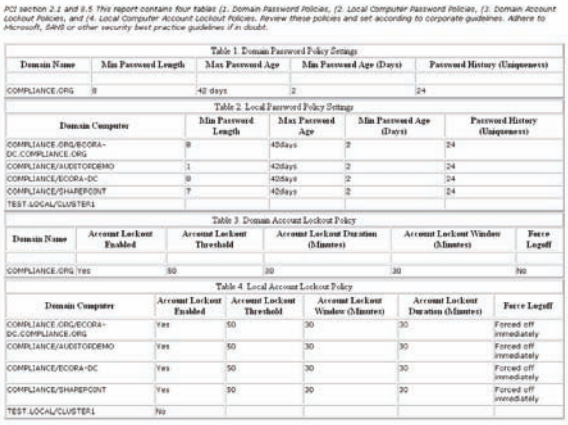
F. Personnel Security

These procedures ensure the credibility of those who have access to critical systems and data, including clear roles and responsibilities, background checks, and confidentiality agreements.

G. Application Security

These procedures ensure the security of software and the protection of sensitive information.

The **Ecora Password and Account Lockout Reports** helps organizations meet the requirements of **Objective 5: Determine whether re-establishment of any session after interruption requires normal user identification, authentication, and authorization**.



PCI section 2.1 and 8.5 This report contains four tables (1. Domain Password Policies, (2. Local Computer Password Policies, (3. Domain Account Lockout Policies, and (4. Local Computer Account Lockout Policies. Review these policies and set according to corporate guidelines. Adhere to Microsoft, SANS or other security best practice guidelines if in doubt.

Table 1. Domain Password Policy Settings

Domain Name	Min Password Length	Max Password Age	Min Password Age (Days)	Password History (Uniqueness)
COMPLIANCE.ORG	8	42 days	2	24

Table 2. Local Password Policy Settings

Domain Computer	Min Password Length	Max Password Age	Min Password Age (Days)	Password History (Uniqueness)
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	8	42days	2	24
COMPLIANCE/AUDITORDEMO	1	42days	2	24
COMPLIANCE/ECORA-DC	8	42days	2	24
COMPLIANCE/SHAREPOINT	7	42days	2	24
TEST-LOCAL/CLUSTER1				

Table 3. Domain Account Lockout Policy

Domain Name	Account Lockout Enabled	Account Lockout Threshold	Account Lockout Duration (Minutes)	Account Lockout Window (Minutes)	Force Logoff
COMPLIANCE.ORG	Yes	50	30	30	No

Table 4. Local Account Lockout Policy

Domain Computer	Account Lockout Enabled	Account Lockout Threshold	Account Lockout Window (Minutes)	Account Lockout Duration (Minutes)	Force Logoff
COMPLIANCE.ORG/ECORA-DC.COMPLIANCE.ORG	Yes	50	30	30	Forced off immediately
COMPLIANCE/AUDITORDEMO	Yes	50	30	30	Forced off immediately
COMPLIANCE/ECORA-DC	Yes	50	30	30	Forced off immediately
COMPLIANCE/SHAREPOINT	Yes	50	30	30	Forced off immediately
TEST-LOCAL/CLUSTER1	No				

H.Software Development and Acquisition

These procedures ensure adequate security controls for software, including compliance with industry standards, the inclusion of audit trails and activity logs, authentication and encryption, etc.

I. Business Continuity—Security

These procedures ensure "recoverability," including the physical security of data backups and program libraries, and adequate contingency planning.

The **Ecora Permissions Reports** helps organizations meet the requirements of **Objective 3: Determine whether appropriate access controls and physical controls have been considered and planned for the replicated production system and networks when processing is transferred to a substitute facility**.

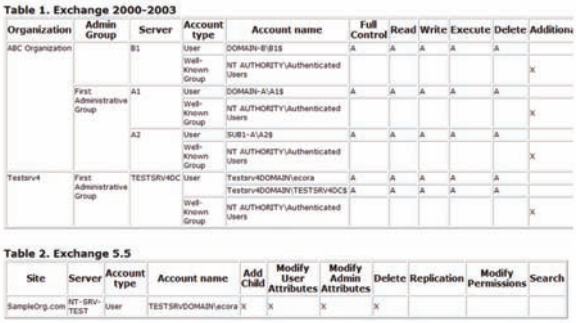


Table 1. Exchange 2000-2003

Organization	Admin Group	Server	Account type	Account name	Full Control	Read	Write	Execute	Delete	Addition
ABC Organization		B1	User	DOMAIN-B\B1$	A	A	A	A	A	
			Well-Known Group	NT AUTHORITY\Authenticated Users						x
	First Administrative Group	A1	User	DOMAIN-A\A1$	A	A	A	A	A	
			Well-Known Group	NT AUTHORITY\Authenticated Users						x
		A2	User	SUB1-A\A2$	A	A	A	A	A	
			Well-Known Group	NT AUTHORITY\Authenticated Users						x
Testsrv4	First Administrative Group	TESTSRV4DC	User	Testsrv4DOMAIN\ecora	A	A	A	A	A	
				Testsrv4DOMAIN\TESTSRV4DC$	A	A	A	A	A	
			Well-Known Group	NT AUTHORITY\Authenticated Users						x

Table 2. Exchange 5.5

Site	Server	Account type	Account name	Add Child	Modify User Attributes	Modify Admin Attributes	Delete	Replication	Modify Permissions	Search
SampleOrg.com	NT-SRV-TEST	User	TESTSRv\DOMAIN\ecora	X	X	X	X			

J. Service Provider Oversight—Security

These procedures ensure that contracts clearly identify security requirements and provide for adequate testing and controls, as well as appropriate reporting and institution oversight.

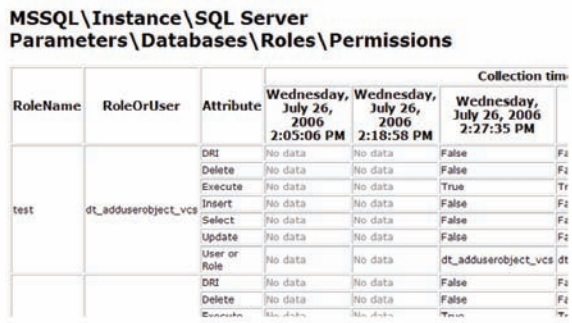
K. Encryption

These procedures ensure adequate encryption processes, including the criteria used to select encryption algorithms, the adequacy of cryptographic keys, and provisions for the recovery of data.

L. Data Security

These procedures ensure that controls are in place to protect data throughout its lifecycle.

The **Ecora SQL Database Roles and Permissions Reports** helps organizations meet the requirements of **Objective 3: Determine whether individual and group access to data is based on business needs**.



MSSQL\Instance\SQL Server Parameters\Databases\Roles\Permissions

RoleName	RoleOrUser	Attribute	Collection tim... Wednesday, July 26, 2006 2:05:06 PM	Wednesday, July 26, 2006 2:18:58 PM	Wednesday, July 26, 2006 2:27:35 PM	
test	dt_adduserobject_vcs	DRI	No data	No data	False	Fa
		Delete	No data	No data	False	Fa
		Execute	No data	No data	True	Tr
		Insert	No data	No data	False	Fa
		Select	No data	No data	False	Fa
		Update	No data	No data	False	Fa
		User or Role	No data	No data	dt_adduserobject_vcs	dt
		DRI	No data	No data	False	Fa
		Delete	No data	No data	False	Fa

M. Security Monitoring

These procedures ensure consistent monitoring and notification of security policies.

Using industry best practices—including regulatory compliance and IT best practices reporting with Ecora Auditor Professional—can help ensure a successful GLBA audit. In fact, by ensuring enterprise-wide control of change, organizations can realize better audit performance with less preparation, saving valuable resources and freeing up IT staff to work on projects that generate revenue. In addition, this approach can have far-reaching implications for other parts of the environment, ensuring continuous compliance and significant improvements in problem management and change management processes.

Find Out More

To learn more about how Ecora can help you achieve and maintain IT compliance, call 877.923.2672 or +1 603.436.1616, email sales@ecora.com, or visit us on the web at www.ecora.com.

About Ecora

Ecora Software is the market-proven leader in transforming enterprise-wide data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's Auditor Professional provides the only patented architecture proven to automate the collection and reporting of configuration information from the entire infrastructure, without agents. Ecora Software takes the cost and complexity out of compliance audits and adopting IT best practices for thousands of customers worldwide, including many of the Fortune 100. For more information, please visit the Company's Web site at www.ecora.com, or phone 603.334.1616.

ecora

2 International Drive, Suite 150 | Portsmouth, NH 03801 | p:877.92.ECORA 603.436.1616 | f:603.436.4344