

# Practical Guide to Understanding and Complying with the Gramm-Leach-Bliley Act

## Executive Overview

The success of any financial institution depends on customers' willingness to place their personal finances in that institution's care. For years, bank vaults, safety deposit boxes, security systems, and guards offered very visible signs of protection and security to a financial institution's customers. Today however, "protection" and "security" are harder to see. The world of banking and finance now operates electronically, hosting and sharing clients' financial and other non-public information on servers and workstations, and across data lines around the globe.

Ensuring the security of this privileged information was the impetus behind the Gramm-Leach-Bliley Act (GLBA), which was signed into law on November 12, 1999.

Section 501 of the GLBA, "Protection of Nonpublic Personal Information," requires financial institutions to establish appropriate standards related to the administrative, technical, and physical safeguards of customer records and information. The scope of these safeguards is defined in the GLBA Data Protection Rule, which states that financial institutions must:

- ensure the security and confidentiality of customer data,
- protect against any reasonably anticipated threats or hazards to the security or integrity of such data, and
- protect against unauthorized access to or use of such data that would result in substantial harm or inconvenience to any customer.

While the initial deadline for compliance has passed, many organizations have not yet developed an information security program that meets the requirements of GLBA. In fact, on a regular basis, headlines expose the loss of hundreds of thousands and even millions of records at institutions like CitiBank, Bank of America, City National Bank, and CardSystems.

One key to securing customer financial information effectively is completely understanding and controlling the IT infrastructure. Many of the security standards included in both the Interagency Guidelines published by the Federal Financial Institutions Examination Council (FFIEC) and the Safeguards Rule established by the Federal Trade Commission (FTC) are fulfilled when an organization accurately documents and reports on the information held within their IT infrastructure.

In this whitepaper, we'll summarize the background of GLBA, the precedents it sets for securing nonpublic consumer information, and the responsibilities it places on senior management and IT departments to ensure that customer data is safeguarded. We'll address the value of change and configuration reporting in meeting the compliance requirements of GLBA, and explain how it can address other critical IT concerns, including business continuity, risk management, and security.

## About the Gramm-Leach-Bliley Act

The primary motivation behind the passage of the Gramm-Leach-Bliley Act 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 reversed more than six decades of restrictions on financial institutions, and, when President Clinton signed Public Law 106-102 (113 Stat. 1338) on November 11, 1999, consumer insurance, banking, and investment information became accessible through one source.

With the passage of GBLA, legislators directed the respective governing agencies to establish appropriate 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.

## Protecting Nonpublic Personal Information under the GLBA

Financial institutions, including banks, savings and loans associations, credit unions, insurers, stock brokerages, financial advisors, and investment firms, are all required to comply with the privacy protections afforded to consumers by GLBA.

In addition to the three privacy standards cited above, institutions are required to provide consumers with notice of their policies for sharing information when a customer relationship is established and annually thereafter.

GLBA defines nonpublic personal information (NPI) as personally identifiable financial information provided by a consumer to a financial institution during any transaction or service, or that is otherwise obtained by the financial institution. Nonpublic personal information includes:

- Customer name, address, social security number, account number
- Information a customer provides on an application
- Information obtained on a legal document that pertains to a summons, bankruptcy, divorce, etc.
- Information from a "cookie" obtained in using a website
- Information on a credit report obtained by a financial institution

In the first few years following the enactment of GLBA, most compliance efforts were focused on addressing "external" risks to NPI misuse. In recent years, however, greater emphasis has been placed on securing NPI internally. This requires that financial institutions have comprehensive information security programs in place to prevent the theft, destruction, or alteration of their customers' information.

## Enforcing GLBA

### The Federal Financial Institutions Examination Council

Many federal agencies oversee financial institutions, and the FFIEC designs and supervises audits for the majority of them. The FFIEC is an interagency working group made up of representatives from the five major financial governing bodies: the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

The member agencies of the FFIEC created the Interagency Guidelines Establishing Safeguards for Safeguarding Customer Information in 2001 to give more direction in meeting the policy goals in the GLBA. In March 2005, the FFIEC supplemented the Interagency Guidelines with guidance on incident response following unauthorized access to customer information.

The Interagency Guidelines provided only limited guidance, however. In fact, the various versions of the Interagency Guidelines take up less than two pages in the Federal Register, so even the statutes, regulations, and Interagency Guidelines together do not provide regulators and institutions with much detail.

To provide further information about security safeguard standards, the FFIEC publishes an *IT Examination Handbook*, which also serves to ensure that examiners work within uniform principles, standards, and report forms. The Handbook was substantially revised and expanded in July 2006.

Under the requirements outlined in the *IT Examination Handbook*, institutions must:

- Document IT inventory and network device configurations, including device name, IP address, access method, vendor and model, and physical location.
- Track and report every configuration change to network equipment, including the who, what, why, and where information, and have a managed enforcement process for implementing changes.
- Track and report on user activities, especially that which could be inappropriate, incompetent, or malicious.
- Enforce access control to all network devices and network servers, and produce audit reports that document and verify this.
- Monitor the compliance of outsource vendors and TSPs.
- Demonstrate that procedures and conclusions in the audit reports have been implemented.
- Provide clear documentation that appropriate reporting is in place within the institution.

### The Federal Trade Commission

While the FFIEC covers the five major financial institutions affected by GLBA, the Federal Trade Commission (FTC) serves as the enforcement agency for all financial institutions not specifically covered by one of the other agencies.

In order to provide more guidance in establishing and sustaining administrative, technical, and physical safeguards for customer information, the Federal Trade Commission enacted 16 CFR Part 314, Standards for Safeguarding Customer Information, on May 23, 2002.

Under this rule, financial institutions subject to the jurisdiction of the FTC are required to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards.

### Draft Interagency Guidance and NCUA Guidance

The final set of regulations related to GLBA that impact financial institutions are the draft Interagency Guidance and NCUA Guidance. Current drafts of both regulations would require institutions to develop a written incident response and customer notification program that contains the following elements:

- Assessment of the incident, including which systems have been accessed or misused.
- Notification of regulatory and law enforcement authorities under Suspicious Activity Report (SAR) regulations and agency bulletins.
- Procedures to contain and control the incident.
- Corrective measures such as flagging and securing affected accounts and notifying and assisting customers in protecting their accounts.

### The Penalties for Non-compliance with GLBA

GLBA calls for severe civil and criminal penalties for noncompliance, including fines and imprisonment. If a financial institution violates GLBA:

- The institution will be subject to a civil penalty of not more than \$100,000 for each violation,
- Officers and directors of the institution will be subject to, and personally liable for, a civil penalty of not more than \$10,000 for each violation, and
- The institution and its officers and directors will also be subject to fines in accordance with Title 18 of the United States Code or imprisonment for not more than five years, or both.

If a violation occurs while another federal law is being violated, or as a part of a pattern of illegal activity involving more than \$100,000 within a twelve-month period, the violator will be subject to a fine of up to twice the amount provided in Title 18 and imprisoned for more than ten years, or both.

Financial Institutions who violate GLBA will also be subject to a number of sanctions, such as the penalties specified in section 8 of the Federal Deposit Insurance Act, including termination of FDIC insurance; removal of the financial institution's management, including directors, officers, etc., and potentially barring them from working in the banking industry; and fines of up to \$1,000,000 for an individual or the lesser of \$1,000,000 or 1% of the total assets of the financial institution.

In addition to these substantial penalties, failure to comply with GLBA can have an adverse effect on an institution's reputation in the community and a serious impact on profitability.

It is clear that officers and managers, including a financial institution's president, vice president, CEO, CFO, and/or CIO, bear responsibility for establishing and sustaining the measures required by GLBA regulations. This includes proposing an appropriate information security program to an institution's board of directors. Once approved, the officers can delegate the ongoing task of carrying out the program to departmental directors or managers. Not only will managers need to fulfill the obligations of the approved information security program, but they will also have to provide regular status reports to both the officers and the board as part of a regular compliance review process.

## Finding a Solution

Ensuring the security of privileged information, while achieving GLBA compliance, requires a formal evaluation of administrative procedures, networks, and applications. Many of the security standards included in both the Interagency Guidelines published by the FFIEC and the Safeguards Rule established by the FTC can be fulfilled by accurately documenting the configuration information on systems throughout the infrastructure.

## Change and Configuration Reporting

Few companies, including financial institutions, completely understand and control their infrastructures. Many can't tell how many servers are active, for example—let alone define each server's configuration. Understanding existing systems significantly improves planning and management of the IT infrastructure. It is essential that financial institutions can automate discovery and documentation of critical IT assets such as servers, databases, applications, and related configuration details. It is also important that institutions can validate that approved changes are made, and pinpoint any unauthorized changes and configurations that deviate from established policies and standards. This starts with detailed reporting.

Prior to automation, organizations rarely (if ever) documented IT infrastructures because system documentation could only be done manually. By the time a system was entirely documented, the process had to begin all over again to stay current.

Automated IT infrastructure documentation and reporting allows an organization to:

- Create "audit-ready" documents on demand
- Detect and mitigate security vulnerabilities
- Simplify server consolidation
- Understand dependencies between elements of the network
- Optimize network and system configuration
- Standardize configuration settings across all systems
- Accelerate problem resolution and troubleshooting
- Migrate to new platforms
- Manage and preserve system knowledge despite IT staff changes
- Limit downtime and speed up disaster recovery
- Educate new staff and consultants on the organization's IT infrastructure

Change and configuration reporting plays a central role in IT best practices by providing accurate and up-to-date information that enables an institution to plan, conduct, and validate changes.

In simplest terms, you need a process for collecting, archiving, and reporting on detailed system configuration data. By automating and standardizing the process, the accuracy and reliability of this data improves dramatically. There is also a dramatic reduction in the resources required to collect the data—providing an almost instant return on investment.

Ideally a change and configuration reporting solution collects and manages infrastructure configuration data from throughout the enterprise to ensure the security and integrity of supported systems, data, and applications. This data then serves as the basis for generating reports that provide a record of how the system is configured, a check for inconsistencies and potential security vulnerabilities, and useful information for troubleshooting. Since it is essential that all servers and devices are configured to meet corporate GLBA compliance plans and policies, IT documentation of configurations must be a fundamental component of any GLBA-compliant plan to ensure consistent, documented compliance.

Effective change and configuration reporting makes data accessible through documentation and reports pulled from the Configuration Management Database (CMDB). This provides a critical foundation for managing the entire IT infrastructure, with value in security, standards and policy implementation, and day-to-day management.

## Business Continuity and Disaster Recovery Planning

Both the FFIEC Interagency Guidelines and the FTC Safeguard Rules require contingency plans to be in place to enable a financial institution to recover in the event of an emergency or disaster. The regulations require a data backup plan, a disaster recovery plan, and an emergency mode operation plan.

On a practical level, downtime caused by emergencies or disasters are costly, and the cost of downtime can be felt through missed revenue opportunities, reduced or non-existent productivity, weakened financial performance and, depending on the source of the downtime, damage to an institution's reputation. To ensure that a financial institution keeps current documentation for all IT configuration settings, the IT infrastructure should be designed so that it can "roll back" to a previous state by accessing historical configuration data, and then validating that the recovery was performed correctly.

Backup tapes stored offline or off site are one key component to any disaster recovery plan, and can enable an institution to retrieve data in the event of a problem or corruption. In the case of complete system loss, the value of the backup tapes depends on how rapidly they can be reloaded and accessed. This requires a server with configuration settings that match those that were in place when the information was last backed up. (IT system configurations aren't usually included in typical data backups.)

Most programs only provide server configuration data in partial or raw-data format and may require a high-level IT professional to decipher and then reconfigure the servers. In addition, backup tapes do not contain hardware specifications for each system, EEPROM settings, specific boot instructions, SCSI ID manipulation, BIOS versions, virtual memory swap space sizes, disk partition slices, space allocation considerations, recovery/re-installation prerequisite

considerations, network services provided, network dependencies required for normal functioning, kernel parameters, initial system installation cluster, and configurations that affect storage devices.

Detailed knowledge of server, database, and router configurations is essential to re-establishing a working framework in which to restore corporate data and services. This information must be more than just a snapshot in time. Given the amount of planned and unplanned change taking place within an IT environment, it is essential that configuration settings are identified and documented on a consistent, ongoing basis.

### Risk Analysis and Risk Management

GLBA security standards, as defined by the FFIEC and FTC, require both risk analysis and risk management. Risk management is the process of identifying, measuring, monitoring, and managing risk. An effective risk management process involves several key factors:

- Establishing senior management and board awareness of identified risks to ensure effective risk management practices;
- Systematically assessing needs while establishing risk-based requirements;
- Implementing effective controls to address identified risks;
- Performing ongoing monitoring to identify and evaluate changes in risk from the initial assessment; and
- Documenting procedures, roles/responsibilities, and reporting mechanisms.

A thorough initial risk assessment is critical to ensuring successful risk management, including disaster recovery/business continuity planning. If the information gathered is limited or outdated, the resulting management plan may be inadequate.

Financial institutions should perform a "gap analysis." In this context, a gap analysis is a methodical comparison of what types of plans the institution needs to maintain, resume, or recover normal business operations in the event of a disruption, over and above what the existing disaster recovery or business continuity plan provides. The difference between the two highlights additional risk exposure that management and the board need to address in updating present plans.

The risk assessment considers:

- The impact of various business disruption scenarios on both the institution and its customers;
- The probability of occurrence based on a rating system of high, medium, and low;
- The loss impact on information services, technology, personnel, facilities, and service providers from both internal and external sources;
- The safety of critical processing documents and vital records; and
- A broad range of possible business disruptions, including natural, technical, and human threats.

Using an automated change and configuration management and reporting solution, an institution can establish thresholds for critical configuration settings and run reports to identify deviations to those standards on an ongoing basis. Not only will the institution have the

information necessary to provide an initial risk assessment, they will be able to effectively manage risk through a regular schedule of reports that will monitor ongoing compliance to the standards initially established, while also identifying gaps in compliance for remediation.

## GLBA IT Security Standards Compliance and Ecora Auditor Professional

The IT infrastructure of a typical financial institution contains hundreds of thousands of configuration settings, including servers, operating systems, databases, mail servers, directory services, and network devices. Each component has settings that can be exploited if not properly configured. To meet GLBA security requirements, an organization must develop a plan and methodology to ensure that critical settings are correctly configured and that they stay that way.

In terms of security, the IT infrastructure is an institution's last line of defense. Antivirus, antispam, firewalls, intrusion protection devices, etc. all work to filter incoming attacks. While these tools improve constantly, they are not 100 percent effective.

The infrastructure—servers, operating systems, directory services, routers, and databases—is managed through its configuration settings. By leveraging configuration data an institution can harden systems and significantly reduce the risk of incidents, both internal and external.

Changes to configuration settings happen all the time, both through a planned change process and otherwise. Awareness of changes to the infrastructure enhances control of a key security component and enables institutions to remediate unwanted or unplanned changes that potentially expose the entire organization to attacks. Ecora Auditor Professional provides automated, detailed reporting about the configuration settings and changes in the IT infrastructure.

**As discussed earlier, IT documentation can help financial institutions meet GLBA compliance mandates. The samples that follow show examples of some of the reports Ecora Auditor Professional generates to address FFIEC requirements.**

### Summary

Until recently, creating comprehensive documentation, and ensuring it remained current, was a tedious, time-consuming, and expensive task—that was not legally mandated.

The Gramm-Leach-Bliley Act makes the real-time availability of secure and confidential nonpublic personal information an obligation of every financial institution. The key foundation for successful compliance is the ability to be in control of the IT systems where the information resides.

By providing ongoing, automated documentation of the configuration settings from throughout the IT environment, financial institutions will not only meet the GLBA security compliance requirements, but will also have the information needed to recover rapidly from a disaster or emergency, effectively assess and monitor risk, reduce security vulnerabilities, and quickly troubleshoot problems caused by planned and unplanned change in the environment.

## Sample GLBA Reports from Ecora Auditor Professional

### Users with Passwords Older than 30 Days

Security best practices recommend that users change their passwords at regular intervals. Each company's policy on password changes can vary, but a common interval for password updates is 30 days. This security report identifies user accounts that have passwords older than 30 days.

#### Password Age by Domain

Domain Name	User Name	User Password Age
Dom	Administrator	291
	ASPNET	48
	Evirginia	40
	Guest	315
	IUSR_ANGEL	54
	IWAM_ANGEL	54
	Jnesper	131
	Revans	291
ChildDom	Administrator	108
	Adow	113
	bparker	108
	Cmayne	113
	Evirginia	108
	Rsharon	113
	Selizabeth	51
	Treynolds	57
NTDom	Administrator	593
	Bgridley	608
	Cmayne	657
	Dmcbride	542
	Fpasters	557

### Operating System and Service Pack Report by Computer Role

This report provides a quick way to make sure all computers are at the proper operating system and service pack level. As soon as a software vulnerability is identified, the likelihood of a mass distributed program that exploits the vulnerability increases, and outdated operating system and service pack levels make the risk of such security compromises even greater.

#### Operating System and Service Pack Summary

Computer	OS Name	Service Pack	Computer Role
CADC001	Windows 2000	Service Pack 3	Domain Controller
CADC002	Windows 2000	Service Pack 3	Domain Controller
CADC003	Windows 2000	Gold	Member Server
CADC004	Windows 2003	Gold	Member Server
CADC005	Windows 2000	Service Pack 4	Member Server
CAFP002	Windows 2003	Gold	Member Server
CAXC001	Windows 2003	Gold	Member Server
CAXC002	Windows 2003	Gold	Member Server
FLFP001	Windows 2000	Service Pack 4	Member Server
FLFP002	Windows 2000	Service Pack 4	Member Server
FLFP003	Windows 2000	Service Pack 4	Member Server
FLFP004	Windows 2003	Gold	Member Server
FLFP005	Windows 2003	Gold	Member Server
FLFP006	Windows 2003	Gold	Member Server
FLFP007	Windows NT	Service Pack 6a	Primary Domain Controller
NVWKS0893	Windows 2000	Service Pack 4	Workstation

### Installed Applications by Computer

Auditing systems to identify inappropriate software can be critical to ensuring system security. Conversely, knowing which systems do not have a particular application installed (e.g., antivirus software) is also important to ensuring a secure IT infrastructure. This report identifies the installed applications on a per-system basis.

#### Installed Applications Summary

Domain Computer	Installed App Name
CADC002	ActivePerl 5.8.0 Build 806
	Adobe Acrobat 4.0
	D-Link AirPlus Access Point Manager
	Microsoft .NET Framework 1.1
	Microsoft Office 2000 SR-1 Premium
	Microsoft SQL Server 2000
	Norton AntiVirus Corporate Edition
	NVIDIA RIVA TNT/TNT2
	WebFldrs
	Windows 2000 Hotfix - KB823182
	Windows 2000 Hotfix - KB823559
	Windows 2000 Hotfix - KB823980
	Windows 2000 Hotfix - KB824105
	Windows 2000 Hotfix - KB824146
	WinVNC 3.3.3
	WinZip
FLXC009	Internet Explorer Q832894
	LiveUpdate
	Microsoft .NET Framework 1.1
	Microsoft Office 2000 SR-1 Premium
	Norton AntiVirus Corporate Edition

### Share and NTFS Permissions by User

It is essential that auditors know who has access to which systems and information. This report details Share and NTFS access rights on a user/group basis, making it easy to demonstrate that only appropriate people have been granted Full Control of sensitive information.

#### Share and NTFS Permissions by User/Group

Domain Server	Share Name	Account	Share Permission	NTFS Permission
CADC001	Address	Dom/Domain Users	Allow – Read (RX)	Allow – Change (RXWD)
CADC002	NETLOGON		Allow – Read (RX)	Allow – Full
CADC003	Resources\$		Allow – Read (RX)	Allow – Read (RX)
CADC004	SMSLOGON		Allow – Full	Deny – special (Create Files, Write Data)Deny – special (Create Folders, Append Data)Deny – special (Write Extended Attributes)Deny – special (Delete Subfolders and Files)Deny – special (Write Attributes)Deny – special (Delete)
CADC005	SYSVOL		Allow – Read (RX)	Allow – Full
CADC005	TempAccting		Allow – Full	Allow – Change (RXWD)
CADC005	TempHRInfo		Allow – Full	Allow – Change (RXWD)

### Services Report by Service Name

It is important to know the services running on all systems, since each service can be an open door for unauthorized access to an institution's systems. WWW, FTP, SNMP, and many other services can be a targeted access point on the network. This report identifies the services installed on an organization's systems on a per-service basis and shows how they are configured (e.g., startup account, start method, and status).

#### Services Summary

Service Name	Startup Account	Start Method	Status	Computer
Indexing Service	LocalSystem	Automatic	running	CAB5GDB31
Indexing Service	LocalSystem	Automatic	running	CADC001
SNMP Service	LocalSystem	Automatic	running	CAB5GDB31
SNMP Service	LocalSystem	Automatic	running	CADC001
SNMP Service	LocalSystem	Automatic	running	CADC002
SNMP Service	LocalSystem	Automatic	running	FLXC009
SNMP Trap Service	LocalSystem	Automatic	Running	CAB5GDB31
SNMP Trap Service	LocalSystem	Manual	not running	CADC001
SNMP Trap Service	LocalSystem	Manual	not running	CADC002
SNMP Trap Service	LocalSystem	Manual	not running	FLXC009
Telnet	LocalSystem	Automatic	running	CAB5GDB31
Telnet	LocalSystem	Disabled	not running	CADC001
Telnet	LocalSystem	Disabled	not running	CADC002



**Cape Cod Cooperative Bank** is an independent, mutual, community bank with \$400 million in total assets. Although the bank's focus has not changed since it was founded, the types of products and services it offers has evolved over time. Cape Cod Cooperative Bank is now a one-stop provider of financial services to both residential and business customers, and is fully committed to offering cutting-edge products in a highly personalized way.

Cape Cod Cooperative Bank has eight locations across Massachusetts' Cape Cod. The bank's IT infrastructure includes 25 servers and more than 125 workstations.

To keep pace with the larger banks, the Cape Cod Cooperative Bank relies on its IT infrastructure to offer services like online banking, but balances advanced technology with the personal assistance it's known for. Like so many small regional banks, managing the IT infrastructure can be a challenge with monthly compliance audits scheduled and the constant barrage of security threats.

When Jason Bordun joined Cape Cod Cooperative as its IT manager, the bank's small IT staff was struggling to keep up with the maintenance of the IT infrastructure. As the infrastructure became more and more complex, manual management was no longer feasible. Auditors were also becoming more demanding and diligent when auditing IT systems and controls.

"We needed a way to automate the many manual tasks that we just did not have time to get to and were critical to our operations and security," said Bordun. "GraVoc Associates, our trusted IT consultant, told us about Ecora's change and configuration management reporting solutions and how they could help us save a significant amount of time and maximize our resources."

## Getting Control

The first audit in which Bordun took part lasted about half of a day; he just needed to provide screen shots to verify Active Directory integrity. Over the last year, the auditors began asking to see specific details, such as log files and how they are produced.

"We needed to provide auditors with reports that would prove our internal controls," added Bordun. "When we were evaluating Ecora's Auditor Professional, I asked if the software could automate the production of the audit reports that we painstakingly created manually. After Ecora produced the reports in a matter of minutes, we were sold."

Ecora Auditor Professional has automated the collection of configuration data so that the IT staff can continue to produce the reports that auditors need—ahead of time and on demand. The software is providing the bank with the ability to manage changes and better troubleshoot problems. Cape Cod Cooperative is now also keeping updated disaster recovery documentation using Ecora's out-of-the-box reports.

"With Ecora, we have greater control of our IT infrastructure—benefits we can directly pass on to our customers," discussed Bordun. "We now always know exactly what's in our environment, who our users are, and what access they have. This is everything our auditors are asking for and more."

*"When we were evaluating Ecora's Auditor Professional, I asked if the software could automate the production of the audit reports that we painstakingly created manually. After Ecora produced the reports in a matter of minutes, we were sold."*

—Jason Bordun  
IT Manager  
Cape Cod Cooperative Bank

## Challenges

- Maintain up-to-date server documentation for compliance audits, change management, and troubleshooting
- Keep servers and workstations current with all security patches
- Help small IT staff manage distributed IT systems more efficiently

## The Ecora Solution

Ecora Auditor Professional automates configuration data collection to a centralized configuration management database to generate hundreds of out-of-the-box reports

## Cape Cod Cooperative Bank Benefits with Ecora

- Automated configuration data collection validates Active Directory integrity, verifies security settings and controls, creates disaster recovery documentation, and manages changes
- On-demand reporting provides sustainable method to meet compliance audits (FDIC, GLBA)
- Vastly improved troubleshooting with in-depth change reports
- Significant time and resource savings applying critical security patches

## About Ecora

Ecora Software offers the industry's only solution for automating regulatory compliance and best practices for IT Systems Management. Over 30,000 global users in nearly 4,000 of the world's largest enterprise companies, system integrators and government agencies rely on Ecora's Auditor solution to accurately and completely report on the true impact of change to an IT environment and business services. For more information about Ecora, visit [www.ecora.com](http://www.ecora.com).

For more information on Ecora or its offerings, please contact sales at [877.923.2672](tel:877.923.2672) or email [sales@ecora.com](mailto:sales@ecora.com).