



Identisphere™

Solutions for Financial Institutions and GLBA Compliance



Identity Aware Gateways for Effective Compliance

The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions that offer financial products or services to individuals. Sections of the GLBA of 1999 addresses “Protection of Nonpublic Personal Information” and requires federal banking agencies and non-bank mortgage lenders, financial or investment advisers, tax preparers, loan brokers, and debt collectors to establish consistent and comparable standards to protect customer information.

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth standards pursuant to section 39 of the Federal Deposit Insurance Act (section 39, codified at 12 U.S.C. 1831p-1), and sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Effective compliance requires that there are comprehensive facilities for logging and reporting all relevant security events, as well as capabilities to analyze and present this information in a meaningful format for network managers so that it can be quickly acted upon. Identisphere ID-ID-Enforce is an identity aware network enforcement solution that authorizes and audits access to critical network resources. ID-Enforce provides network-level enforcement that allows users to access only the resources they have the privileges to use, and creates an audit trail of when they were used. Every network authorization attempt, whether authorized or denied – is recorded in detailed, identity-based logs making it easier to fulfill annual GLBA security program status reports.

Applied Identity offers solutions to assist in compliance with the GLBA in the following areas:

Section II: Standards and Safeguarding Customer Information

A. Information Security Program. Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

B. Objectives. A bank’s information security program shall be designed to:

Applicable Sections		Applied Identity Solutions Provide:
B.1	Ensure the security and confidentiality of customer information.	ID-Enforce is an identity aware network-level access enforcement solution that only allows predefined user identities to access protected resources on the network. Providing granular access control, successful or unsuccessful access attempts are logged with the user account and common name information as stored in the directory.
B.2	Protect against any anticipated threats or hazards to the security or integrity of such information.	ID-Enforce will only allow users with the correct privileges to access specific services and data. Any unauthorized user would not be able to see the network resource as it would be completely cloaked from them at the network layer.
B.3	Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.	ID-Audit provides an audit capability to aid in the creation of policies of know user identities. Once enforced, any unauthorized access attempts would be logged and access automatically blocked.

Applied Identity Solutions

Identsphere

Identsphere is a line of identity and access management solutions that enable organizations to consolidate the creation, management and auditing of user identity and access policies from a single, or across multiple identity stores.

Identsphere Manager

Management interface for the creation, management and implementation of access policies utilizing user identities. Also provides a central management, audit and reporting interface for Applied Identity's ID-Audit, ID-Unify and ID-Enforce appliances.

ID-Audit

Provides a central repository of audit data on user behavior and resource usage. Enables the creation of real-time views and historical reports that can be used to create new or refine existing policy.

ID-Unify

Manages user identities between multiple and disparate identity stores, creating a virtual mapping and normalization of user information.

ID-Enforce

ID-Enforce is a line of network enforcement appliances that enable enterprises to embed identity and access management into the network, reducing operating costs and complexity associated with IP based security solutions.

ID-Mark

In environments that require an increased level of accountability and non-repudiation of events, an optional ID-Mark™ agent can be installed on the client workstation to further enhance security.

© 2007 Applied Identity, Inc. All rights reserved. Applied Identity, Applied Identity Logo, Identsphere, Identsphere Manager, ID-Audit, ID-Unify, ID-Policy, ID-Mark and ID-Enforce are trademarks of Applied Identity, Inc. All other trademarks included in this document are the property of their respective owners.

Section III: Development and Implementation of Information Security Program

B. Assess Risk. Each bank shall:

Applicable Sections		Applied Identity Solutions Provide:
B.1	Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.	ID-Audit's detailed logging capability assists in the tracking of user and resource usage, which in turn helps to define policy enforcement to limit potential unauthorized access to sensitive information. ID-Enforce also has the ability to cloak critical resources from unauthorized user access at Layers 3 and 4, minimizing the resource's exposure and limiting the number of potential attack vectors.
B.2	Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.	Applied Identity helps organizations to align their security program with the requirements and expectations of examiners and auditors. The reporting, policy creation, and implementation of Identsphere helps organizations centralize and deliver pertinent information requested by IT examiners.
B.3	Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.	Identsphere uses an auditing mechanism to monitor policy definition, implementation, use, and workflow.

C. Manage and Control Risk. Each bank shall:

Applicable Sections		Applied Identity Solutions Provide:
C.1.a	Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.	Identsphere provides an easy to define identity-based policy for user access to network resources. ID-Enforce integrates policy management with existing LDAP identity management systems such as Microsoft Active Directory, Oracle ID, Sun Java Directory, Novell eDirectory and other LDAP v3 compliant systems. Role based access can be defined using existing users and groups in a directory service without requiring a separate policy management infrastructure. ID-Mark definitively associates a user with their IP by tagging each packet sent from the client workstation via the gateway to protected resources, creating an irrefutable chain of evidence.
C.1	Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information.	Network level access policies may be defined by an administrator and authorized by a manager prior to implementation and enforcement, thereby meeting the provisions of duty segregation and dual control.
C.1.	Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	ID-Enforce allows access to resources based on user identity and the principle of least privileged. Any valid or invalid access attempts are logged by user name. Any unauthorized access attempts or reconnaissance techniques that target the protected resources are logged and recorded for via the secure ID-Audit appliance.
C.1.g	Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.	ID-Audit provides an audit trail based on user identity and the associated IP address to provide evidence of misuse for law enforcement and compliance reporting.



456 Montgomery, Suite 400
San Francisco CA 94104
Phone: 888.286.7336
Fax: 415.593.2100
www.appliedidentity.com



Arrange a **FREE Network Activity Assessment** that will tell you who is accessing what resources and when on your network
Call 888.286.7336 or email: sales@appliedidentity.com