HITACHI
Inspire the Next

Gramm-Leach-Blilely

Hitachi ID Solutions Support GLB Compliance

The Hitachi ID Management Suite

The Hitachi ID Management Suite is an integrated solution for managing user onboarding, security management and deactivation processes. It uses automation, self-service, consolidated and delegated administration to reduce IT support cost, improve user productivity and strengthen security.

Sample financial institutions using the Hitachi ID Management Suite:

- American Financial Group
- Assurant
- Bank of Hawaii
- Citizens Bank
- City National Bank
- Credit Lyonnais
- First National Bank of Nebraska
- MetLife
- Northern Trust
- Royal & SunAlliance
- Southwest Bank of Texas
- Wells Fargo
- Zurich North America

The Challenge

Regulatory compliance with the Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act,” has created significant challenges for financial institutions. The Safeguards Rule in the GLB (16-CFR-314), enforced by the Federal Trade Commission, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information. Such privacy protection depends on effective internal controls, including:

- Who can access sensitive customer data?
- How are these users authenticated?
- What can they see and modify?
- Are users held accountable for their actions?

These requirements are met by classic AAA infrastructure: Authentication, Authorization and Audit. AAA infrastructure has been standard in enterprise applications for years. Unfortunately, a large and growing number of applications, combined with high staff mobility have made it much harder to manage user entitlements. As a result, users get access rights inappropriate to their jobs and users may be inadequately authenticated. Problems with user security include:

- Orphan accounts.
- Dormant accounts.
- Stale or excess privileges.
- Weak passwords.
- Vulnerable caller authentication at the help desk.

These weaknesses are not in the AAA technology -- they are in the business processes for managing user entitlements.

To view the full text of the Gramm-Leach-Bliley Act go to http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106

The Solution

Organizations must implement sound processes to manage identities and entitlements, so that only the right users get access to the right data, at the right time. This is accomplished by:

- Correlating different user IDs to people.
- Controlling how users acquire and when they lose security rights.
- Logging current and historic access rights, to support audits.
- Periodic audits of user privileges, carried out by managers and data owners.
- Controlling access to administrative accounts.
- Requiring strong passwords or two-factor authentication.
- Using reliable processes to authenticate callers to the help desk.

Hitachi-ID.com

The Hitachi ID Management Suite

The Hitachi ID Management Suite is an integrated solution for managing user lifecycles. It automates setup, maintenance and termination of user profiles, passwords and access rights. It supports stronger security, and therefore GLB compliance, with the following components:

Automated Discovery

Map user IDs to owners and identify orphan and dormant accounts.

Password Manager

Enforce a global password policy and ensure that when users forget their password they are still reliably authenticated.

Identity Manager

Automatically deactivate access for terminated employees. Report on current and past security rights.

Access Certifier

Prompt managers, application owners and group owners to periodically review security rights within their scope of authority. Deactivate inappropriate rights.

Privileged Access Manager

Periodically randomize administrator passwords and control access to those accounts by authenticating users, authorizing disclosure and logging events.

Rapid Deployment

Identity and access management systems can be challenging to implement. Common problems include poor user entitlements quality, costly role engineering and hard to manage workflow systems. To overcome these problems, the Hitachi ID Management Suite:

- Leverages auto-discovery and self-service to find and map login IDs.
- Is fully functional even without defined roles.
- Simplifies workflow management: one process to authorize all requests.

Technical Specifications

TARGET SYSTEM INTEGRATION

Directory:

Windows domains, Active Directory, eDirectory, Novell NDS, any LDAP

File/Print:

Windows 2000, 2003, 2008; Novell NetWare, Samba

Databases:

Oracle, Sybase, SQL Server, DB2/UDB, Informix

Unix:

Linux, Solaris, HPUX, AIX, Tru64, Irix, Unisys, SCO, DG; passwd, shadow, TCB, Kerberos, NIS, NIS+

Mainframes:

z/OS, VM/ESA, Unisys, Siemens

Minis:

iSeries OS400, OpenVMS, Tandem

Applications:

Oracle eBusiness Suite, PeopleSoft, SAP R/3, JD Edwards

Groupware:

Microsoft Exchange, Lotus Notes, Novell GroupWise

Networking:

Cisco ACS, RADIUS, TACACS+, etc.

Flexible Agents:

API, Web services, command-line, SSH, Telnet, TN3270, TN5250, SQL injection, LDAP attributes, Web services, web forms

SUPPORT INTEGRATION

Automatically create/update/close incidents:

- Axios Assyst
- BMC Remedy AR System
- BMC Service Desk Express
- CA Unicenter Service Desk
- Clarify eFrontOffice
- FrontRange HEAT
- HP Service Manager
- Tivoli Service Desk

Additional integrations through e-mail, ODBC, web services, web forms, SQL injection, LDAP attributes and command-line.

Hitachi ID Systems, Inc.
500, 1401 - 1 Street SE
Calgary AB Canada T2G 2J3
Tel: 1.403.233.0740   Fax: 1.403.233.0725
E-Mail: info@Hitachi-ID.com