CASE STUDY: PMI Group, Inc - Simplifying Compliance Auditing with Access Auditor

Background

The PMI Group, Inc. (NYSE:PMI), headquartered in Walnut Creek, CA, provides innovative credit, capital, and risk transfer solutions that expand homeownership and fund essential services for its customers and the communities they serve around the world. Through its wholly and partially owned subsidiaries, PMI offers residential mortgage insurance and credit enhancement products, financial guaranty insurance, and financial guaranty reinsurance. PMI has operations in Asia, Australia and New Zealand, Europe, and the United States.

With this project, PMI sought to systematically validate user privileges to systems and data. The Access Auditor solution from Security Compliance Corporation provided PMI an automated process to approve employee access rights to applications, view users' security profiles, and streamline internal and external audit functions.

The Challenge

Compliance legislation, such as Sarbanes-Oxley (SOX) and the Gramm-Leach Bliley Act (GLBA), mandates audits of employee access to business applications. PMI wanted an updated, easy-to-use system to validate internal controls and certify that the appropriate access rights had been granted to all employees and contractors.

Pam Pullem, AVP of Corporate Information Security, was charged with refining the process of reviewing and approving user access rights to systems. "Validation is increasingly important due to regulatory changes," says Pullem. "We wanted a product that would help verify all users have only the permissions necessary to perform their job functions and nothing more, and that would be easy for non-technical managers to use."

The distributed nature of access control systems, especially those for legacy applications, was a challenge. Systems often maintain a separate repository of user account information, so a typical company may have five or more unique systems of record storing user access data. PMI wanted to be able to better generate and merge multiple reports for each system of record in order to pull profiles for users of each application.

Security Compliance Corp

The Challenge

PMI needed to automate the auditing of user access rights for the entire enterprise.

The Solution

Access Auditor provided PMI with the automated discovery and validation workflow necessary to streamline their compliance auditing functions.

The Results

PMI had a smooth and successful deployment of Access Auditor and is expanding the number of applications being audited.

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Like most companies, PMI was already adhering to compliance controls involving the auditing of user entitlements and access to sensitive data. Their process, however, was highly labor-intensive, involving the manual creation and distribution of disparate reports for each critical application. Moreover, each report had a different format, further complicating the job for managers and application owners.

The goal for PMI was to find a product that would automate the entire process of discovering, reporting, and validating user access rights. PMI identified several requirements for this automation tool, including to:

- Better ensure user accounts and privileges for terminated or transferred employees were revoked.

- Provide a twofold perspective to look at users and applications (the ability to look at a user profile and see what rights and privileges they had, or to look at an application and see what users had rights to that application).

- Automate the discovery of access privileges and present them to reviewers through a web interface.

- Deploy and integrate seamlessly with existing systems and processes.

The Solution

Todd Berman, Director of Information Protection and Security for PMI, led the search for a solution that could automate the discovery and validation of user access rights. Berman turned to Security Compliance Corporation's (SCC) Access Auditor, a web-based application that discovers, consolidates, and reports on user access rights from a wide variety of data sources. PMI has the typical mix of commercial and custom applications. Using Access Auditor's flexible discovery tool, PMI imported data into Access Auditor from diverse systems ranging from Windows Active Directory to proprietary mainframe applications. Since read-only accounts are used to collect user access profiles, deployment was quick, simple, and required no changes to PMI's existing systems and processes.

After merging entitlement data across the various mission-critical applications, the true value of Access Auditor was immediately realized. Through a single, unified web interface, managers and business owners could view consolidated user profiles. Moreover, the periodic user recertification efforts that were previously performed manually were now automated. Access Auditor provided a web page showing user access rights and allowed reviewers to approve or deny each individual privilege. Those access rights marked as inappropriate were then sent to PMI's help desk for remediation through existing processes.

By simply scheduling repeated data imports, Access Auditor can provide a near real-time view into user privileges.

A great unexpected benefit to PMI was the value of having an authoritative copy of all user entitlement data. Berman notes, "Access Auditor is able to provide the single pane of glass view into user access rights." Ad-hoc reports can be created for both current and historic data. For example, when a user leaves the company, an administrator simply needs to query Access Auditor to validate that all of the user's privileges have been removed.

Dan Roberts, Chief Information Officer for The PMI Group, Inc. summarizes why PMI chose the Access Auditor solution. "It is a flexible, targeted solution that looks only at the access issue. It does not require us to implement more than we need. Companies with a smaller number of users, like PMI, may find that it does not make sense to implement a full provisioning solution, but we still have important compliance objectives related to access. We were able to install and configure Access Auditor without having to change our existing infrastructure. Security Compliance Corporation provided excellent support."

The Results

PMI deployed Access Auditor and achieved very positive results. Every one of PMI's users successfully used Access Auditor's web interface to validate their security profiles. A full record of all privilege data and validation results was stored for historical reporting.

Access Auditor was configured to audit user access rights for several key financial applications. PMI continues to expand the role of Access Auditor by increasing the number of applications being audited and leveraging historical data to track environmental changes and provide alerts.

"It is a flexible, targeted solution that looks only at the access issue... We were able to install and configure Access Auditor without having to change our existing infrastructure. Security Compliance Corporation provided excellent support."

Dan Roberts, Executive Vice President and Chief Information Officer

Access Auditor Key Features

FEATURE	DETAILS	BENEFITS
Entitlement Reviews and Access Certification	• Managers and business owners certify access rights with a simple web-based solution • Flexible rules-based workflow defines custom approvers at various phases of a certification	• Provides company-wide attestation of employee access rights and privileges required for IT best practices and compliance-related audits (SOX, HIPAA, GLBA, ISO 27001, PCI, and others)
Fuzzy ID and the Identity Mapper	• Link users from disparate applications even when no consistent login ID exists • Proprietary name-matching algorithms automatically identify the same user in multiple systems even with no common attribute	• Solves one of IT's largest challenges, how to view access rights when no common attributes exist • Eliminates the need to modify applications to insert a unique identifier • Establishes a single repository of all access data across the entire enterprise
Role-Based Certifications and Role Definition Tool	• Define roles and role memberships • Perform certifications by roles and exceptions to improve accuracy and relevance • Perform what-if scenarios to define cross-application enterprise roles	• Improves relevance of certifications by reviewing a handful of roles instead of hundreds of privileges • Defines and manages roles by comparing role memberships and exceptions
Consolidated View of User Access Rights	• Custom reports show real-time and historical data • Orphaned user accounts from transfers and terminations are detected and reported • Historical record of access rights compliance	• Reveals users with inappropriate combinations of access rights • Discovers orphaned or lost user IDs • Provides documentary evidence of meeting access-related compliance controls
Real-Time Access and SOD Alerting	• System monitors for changes to user access data • Simple interface for configuring custom alerts and actions • Comprehensive cross-application separation of duties reports and alerts	• Generates alerts if access data has changed since the last audit scan • Detects unauthorized changes to systems • Warns business owners if users violate separation of duties rules
Automated Discovery	• User access rights and group memberships are automatically discovered and processed • Support provided for wide variety of commonly used applications without product customization	• Consolidates user data from diverse systems and groups by user and application • Enables Access Auditor to provide a near real-time view of user entitlements

Security Compliance Corporation

120 Village Square, Suite 76
Orinda, CA 94563
(866) 657-4550
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Security Compliance Corporation's (SCC) Access Auditor® automates the periodic review and certification of user access rights and entitlements. SCC's workflow engine provides the ultimate flexibility in defining and managing the periodic attestation of user access rights. The enhanced Identity Mapper™ utilizes a proprietary algorithm to link user accounts from disparate systems back to the correct person, even when common identifiers or login IDs do not exist. Access Auditor's consolidated view of user access rights enables customers to identify orphaned accounts left behind from terminated users, thus reducing the risk of fraud and audit findings. By automating labor-intensive tasks related to user access rights and separation of duties, SCC's customers improve security while minimizing the costs of compliance. Founded in February 2005, Security Compliance Corporation is based in Orinda, CA.