CASE STUDY: First National Bank Succeeds with Access Auditor®

The Challenge

FNB needed to automate their labor-intensive and manual entitlement review process. With approximately 4500 employees and no common login ID format, access reviews became a significant resource burden.

The Solution

Following a full RFP, Access Auditor and its 100% success rate stood out as the simplest and fastest solution for FNB.

The Results

Access Auditor delivered success by providing FNB significant time savings, improvements in finding and removing orphaned user accounts, and positive feedback from internal and external auditors.

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(925) 255-5686
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Background

F.N.B. Corporation (NYSE: FNB), headquartered in Pittsburgh, Pennsylvania, is a diversified financial services company operating in seven states and the District of Columbia. The Company has total assets of more than $34 billion with approximately 4500 employees and 370 banking offices throughout Pennsylvania, Ohio, Maryland, West Virginia, North Carolina, and South Carolina.

As a highly regulated bank, First National Bank (FNB) has a significant interest in maintaining controls around terminated users and performing periodic reviews of user access rights. With increased requirements, these processes became a significant burden on the Company's information security team. Scot Pflug, CISO, and Barb Austin, Manager of I.T. Risk and Compliance, conducted a search for an automated solution. After reviewing, selecting, and implementing Access Auditor from Security Compliance Corp (SCC), FNB streamlined their review process, increased the scope and frequency of reviews, and implemented a robust automated approach to detecting and removing access from terminated users.

The Challenge

As part of FNB's ongoing compliance efforts, the information security team had been performing regular user access reviews on key SOX and other in-scope applications. The process, however, was very labor-intensive, requiring a combination of cumbersome spreadsheets and email. After increases in both frequency and number of systems, access reviews became a significant resource burden.

One of the biggest challenges was that many applications do not share a common login ID format. In order to validate active employment, FNB staff had to review each user account individually to link them back to HR records. This made basic user validation a difficult task. Compounding the identity matching challenge was a recent acquisition where a significant volume of employees used a preferred name (e.g., middle name rather than first name) that did not match the legal name from the HR system.

In addition, with approximately 4500 employees, the volume of user accounts across multiple in-scope applications was daunting. The entire process was extremely labor-intensive and a huge drain on staff resources to link each employee back to their HR record and attempt to sort by manager.

Ideally, the access reviews would be performed by the employee's direct manager. Due to the work effort involved, however, the application owner performed the entire application review rather than the user's manager approving the access.

In short, the experienced challenges included:

- **Labor-intensive**: With over 4500 employees and disparate applications, the manual process was difficult and time-consuming.
- **Collation and management of data**: Reviews were performed using spreadsheets and email, making data management and records retention a cumbersome chore.
- **Identity Mapping**: With disparate user accounts not sharing a common login ID, linking users back to their HR records for employment validation was a long and arduous task.

The Solution

After an increase in the number and size of entitlement reviews, FNB sought to automate and streamline the access governance process. The primary goal of the project was to find a fast and easy-to-use solution to automate the entitlement review process. The new automation would enable FNB to increase the quantity and frequency of audits and enable a more detailed review of user access rights.

Many vendors deliver Identity Management solutions that are expensive, cumbersome, and require lengthy deployment times. Pflug and Austin were instead looking for a much simpler solution that would provide a few key features:

- **Ease of Use:** The chosen solution must be easy to use with a fast deployment time. FNB needed a product that did not require any custom coding or scripting to implement, and that would improve the end users' performance of their entitlement reviews.
- **Identity Mapping / Fuzzy ID:** Since many applications do not share login IDs, the ability to use a fuzzy logic to link users between various applications was critical to the project success. Even though many employees used a preferred name, the Fuzzy ID quickly identified and linked the accounts.
- **Consistent Audit Documentation:** Reporting is a crucial and often-overlooked component of the user management process. FNB required robust and consistent reporting to meet compliance controls from a variety of SOX and financial auditors.

"Having purchased Access Auditor in a previous company, I turned to SCC for a fast, simple, and effective solution to automate user entitlement reviews. Once again, Access Auditor delivered success."

Scot Pflug
Chief Information Security Officer, First National Bank

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(925) 255-5686
www.securitycompliancecorp.com
info@securitycompliancecorp.com

FNB initiated a full Request for Proposal (RFP) process to compare multiple vendor solutions for functionality and value. Having used SCC's Access Auditor in the past, Pflug invited the company to submit a proposal. Access Auditor (with Access Manager and Role Manager for a phase 2 provisioning deployment) excelled above the competition, presenting the simplest solution for automating user access reviews and requiring no custom coding or development. Coupled with Fuzzy ID functionality to map users between unrelated applications, Access Auditor was able to maintain a 100 percent success rate and proved to be the right solution for FNB, offering several notable features including:

- Centralized repository for access data
- Easy web-based access for reviewing managers
- Easy report generation
- Significant time savings

The Results

Access Auditor provided a great success for FNB. According to Austin, "Training and assistance from SCC was tremendous; the vendor was extremely responsive and absolutely knowledgeable about the solution's technical and operational capabilities. User access data is being consolidated from various internal databases and critical financial applications. Active directory SSO has been well received by the reviewers and eliminates the need to setup users or reset passwords for Access Auditor access."
With the Access Auditor automation, user access reviews are being performed by managers across the company and FNB is now able to move to a quarterly review of the most critical systems.

Another impressive improvement relates to the user termination process. The Identity Mapper and Fuzzy ID allow the Bank to quickly and easily link users from most applications back with their HR data. Building this consistent view of user access provides a one-click report of orphaned users – in-active employees. Austin explains that this allows FNB to "ensure the effectiveness of the access revocation process and controls around timely removal of user accounts." Moreover, some applications are managed by various lines of business. Access Auditor can now easily identify and remediate those applications that may have user de-provisioning challenges

In short, Access Auditor delivered success by providing FNB significant time savings, improvements in finding and removing orphaned user accounts, and positive feedback from internal and external auditors as it relates to the process and reporting.

> *"Access Auditor and the Fuzzy ID allowed us to remove orphaned users in various applications and ensure the effectiveness of the termination process."*
>
> **Barbara Austin**
> **Manager of**
> **I. T. Risk &**
> **Compliance,**
> **First National**
> **Bank**

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(925) 255-5686
www.securitycompliancecorp.com
info@securitycompliancecorp.com

Access Certification COMPLIANCE PIPEDA Identity Governance HIPAA ISO27001 SOX Solutions GLBA

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	• Links users from disparate applications when no consistent login ID exists • Proprietary name-matching algorithms automatically identify the same user in multiple systems 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	• Defines roles and role memberships • Performs certifications by roles and exceptions to improve accuracy and relevance • Performs 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

SCC
SECURITY COMPLIANCE CORP

Security Compliance Corporation
120 Village Square, Suite 76
Orinda, CA 94563
(925) 255-5686
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.