FORTRA

CASE STUDY (Core Security)

Banking Customer

Access and Compliance Case Study

Background

This Core Security customer is the largest banking institution headquartered in its state. Its strong focus on community and providing a positive local banking experience puts a premium on customer service quality, customer privacy and security. As the bank expanded its services and locations, this aggressive growth strategy put a strain on its original access provisioning and compliance process and infrastructure.

The Challenge

Like many diversified financial institutions, the bank relies on numerous financial systems to support the business. Manually provisioning employee access to new systems, or revoking access based on changing employment status, limited productivity and created risks to the security and privacy of customer data. The process of manual provisioning also became disconnected from business processes, making documentation for audit and compliance cycles laborious and difficult to manage.

In order to address these challenges, the bank sought a solution that could meet its specific access provisioning and compliance goals, including: automating provisioning processes, eliminating the quarterly profile review and attestation process, maximizing existing administration staff and technology including integration with existing workflows, and meeting regulatory requirements and federal mandates such as Sarbanes-Oxley and the Gramm-Leach-Bliley Act.

As the team reviewed various vendor solutions, the bank prioritized their options based on vendors' ability to accommodate its existing technology applications, systems and solutions in order to avoid the need for massive new builds or lengthy implementation times.

OVERVIEW

With Core Security, the banking customer:

+ Achieved "go-live" status within five months of project launch

+ Streamlined operational and business processes associated with on-boarding and off- boarding staff

+ Leveraged role-based provisioning to grant employee access by job code

+ Demonstrated policy and regulatory compliance, including recognition by external auditors of adherence to process

> "We can point to substantial achievements against our business and IT goals. By taking advantage of the benefits associated with automating audit issues and IT administration, we are on solid footing with a flexible Access, Provisioning and Compliance solution that will grow with our business and continue to support productivity, security and quality of service goals."
> —VP and Support Systems Manager

Mission Possible: Using Automation to Realize New Compliance and Operational Efficiencies

To further illustrate the bank's provisioning and access compliance burden, the large number of financial systems to support operations and business transactions includes, but is not limited to, applications and systems such as HRIS, Active Directory, the loan servicing system, wire system, core banking system, loan origination system and the help desk ticketing system.

For every new hire, promotion or other shift in job responsibility, approximately 10 new "help desk tickets" were generated to grant access to systems. These tickets were often "blind," requiring system administrators to track down more information from business managers on what system access needed to be granted, what system profile changes needed to be made, what job code to enter or what cost center changes.

The Approach

To address these challenges, the bank selected Core Security's Identity Governance Administration solution to automate rolebased provisioning and access compliance verification to ease documentation requirements for laborious audit and compliance cycles.

Additionally, a new workflow was developed for human resources to terminate users outside the standard scheduled workflow. This allows thorough systems access termination at any time for an employee whose status has changed, immediately alleviating security exposure and privacy risk.

Aside from knowing what access employees require, it's equally important for administrators to know what access needs to be taken away. By automating workflows and incorporating intelligent "what if" scenarios, this became much easier to manage – enabling a "lights out" scenario that achieves provisioning and compliance goals without the need for manual intervention.

The Results

Soon after going live, the bank immediately recognized benefits, especially in terms of productivity gained by automating policy enforcement and role management tasks along with streamlined operational and business processes associated with on-boarding and off-boarding staff.

Wire system access control is especially important as wire approval limits are monitored and documented by the right people with the right credentials. With the ability to automatically ensure compliance with business policies, the need for quarterly profile reviews has been virtually eliminated.

The bank also recognized several opportunities to improve business processes outside of traditional provisioning. For example, they created new operational efficiencies associated with timeconsuming security procedures. This was accomplished by creating new workflows to enable remote access for employees while maintaining alignment with business requirements and complying with information security policy.

Overcoming Challenges and Unexpected Benefits

The bank faced challenges within their organization associated with internal staff communications – from gaining initial buy-in from human resources and other business units, to addressing their questions about implementation timelines and expected benefits. In order to achieve universal support for the new systems and processes, they worked closely with individual departments. They worked with human resources to map out and document the required hiring, updating and termination process. They worked with the business units to identify the system requirements for an individual to complete their job. The bank also recognized the importance of working closely with the Access Provisioning and Compliance vendor to properly set expectations, adjusting them along the way as needed. By properly setting expectations and recalibrating as necessary, the bank achieved an intimate understanding of time tables, ensured that proper support mechanisms were in place, provided allowances for last minute process flow changes and ensured the proper steps were taken to assign accountability and ensure data integrity with as little down time as possible. Comprehensive communication and marketing throughout the organization was key to this customer's successful deployment.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.