NIST SPECIAL PUBLICATION 1800-9A

# Access Rights Management for the Financial Services Sector

**Volume A:**
**Executive Summary**

**James Banoczi**
National Cybersecurity Center of Excellence
Information Technology Laboratory

**Sallie Edwards**
**Nedu Irrechukwu**
**Josh Klosterman**
**Harry Perper**
**Susan Prince**
**Susan Symington**
**Devin Wynne**
The MITRE Corporation
McLean, VA

August 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use-cases/access-rights-management


# Executive Summary

- The NCCoE has developed an example implementation that demonstrates ways in which a financial services company can improve their information system security by limiting employee access to only the information they need to do their job, at the time they need it, and nothing more. Essentially, enabling a company to give the right person the right access to the right resources at the right time.
- Specifically, this project provides an example solution that describes how to execute changes and coordinate employee access to data and systems quickly, simultaneously, and consistently—and in accordance with corporate access policies.
- Today's threat landscape has created ever-increasing challenges for financial services companies as they work to protect important financial assets and customer data. Financial services companies are under a high and sustained level of attack, in some instances experiencing a direct loss. Costs associated with these cyber attacks are growing and have reached an average loss of one million dollars per incident.[*]
- Complicating efforts to protect important data is the highly complex infrastructure that established financial services companies must manage. Disparate, legacy systems that run on different operating platforms are difficult to manage and ensure appropriate levels of access management.
- To combat these challenges, various regulatory organizations, such as the FFIEC as well as other federal, state, and other industry organizations, have developed a range of compliance mandates for financial services companies. As an example, financial services companies should apply the principles of least privilege to grant employee access to systems and data. This guide acknowledges these compliance requirements.
- A properly implemented and administered Access Rights Management (ARM) system can help your organization meet compliance requirements, limit opportunity for and reduce the damage of an attack, and improve enforcement of enterprise information system access policies.

## CHALLENGE

Managing user access in a fast-moving industry such as the financial services sector requires frequent changes to user identity and role information and to user access profiles for systems and data. Employees using these various ARM systems may lack methods to coordinate access across the corporation effectively to ensure that ARM changes are executed consistently throughout the enterprise. This inconsistency is inefficient and can result in security risks. See Section 1.3 for the risk factors addressed by the solution.

Many financial services companies use ARM systems that are fragmented and controlled by numerous departments. For example, changes to user identity and role information should be managed by an ARM system within the Human Resources department; changes to user access profiles may be managed by IT system administrators; and changes to user access profiles for specific resources or data may be managed by still other systems under the control of various business unit managers.

In collaboration with experts from the financial services sector and technology collaborators that provided the requisite equipment and services, we developed representative use-case scenarios to describe user

[*] *Kapersky Lab Report 2017, New Technologies, New Cyberthreats: Analyzing the state of IT Security in financial sector* https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf

access security challenges based on normal day-to-day business operations. The use cases include user access changes (e.g., promotion or transfer between departments), new user onboarding, and employees leaving an institution.

## SOLUTION

The NCCoE developed an ARM system that executes and coordinates changes across the enterprise ARM systems to change the employee's access for all data and systems quickly, simultaneously, and consistently, according to corporate access policies. The example implementation provides timely management of access changes and reduces the potential for errors. It also enhances the security of the directories. Generally, an ARM system enables an institution to give the right person the right access to the right resources at the right time. The ARM reference design and example implementation are described in this NIST Cybersecurity "Access Rights Management" practice guide.

Financial services companies can use some or all of the guide to implement an ARM system. The guide references NIST guidance and industry standards, including the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC CAT). The NCCoE used commercial, standards-based products that are readily available and interoperable with commonly used IT infrastructure and investments. We built an environment that simulates a financial services company's infrastructure. The infrastructure includes the typical network segmentation and IT components (i.e., virtual infrastructure, directories, etc.). Simulated financial systems (banking and loan operations systems) further illustrate the solution.

The NCCoE reference design includes the following capabilities:

- A single system that is capable of interacting with multiple existing access management systems for a complete picture of access rights within the organization
- Secure communications between all components
- Automated logging, reporting, and alerting of identity and access management events across the enterprise
- Ad hoc reporting to answer management, performance, and security questions
- Support for multiple access levels for the ARM system (e.g., administrator, operator, viewer)
- Protection from the introduction of new attack vectors into existing systems
- A complement to, rather than replacement of, existing security infrastructure

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

## BENEFITS

The NCCoE's practice guide to address Access Rights Management for the financial services sector can help your organization:

- Reduce damage caused by a successful insider threat attack by limiting the amount of data to which any one person has access
- Limit opportunity for a successful attack by reducing the available attack surface
- Increase the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- Reduce complexity, which leads to:
    - Faster and more accurate access policy modifications
    - Fewer policy violations due to access inconsistencies
- Simplify compliance by producing automated reports and documentation

## SHARE YOUR FEEDBACK

View or download the guide at https://nccoe.nist.gov/projects/use_cases/access_rights_management. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing these guidelines.

To provide comments or to learn more by arranging a demonstration of this reference solution, contact the NCCoE at financial_nccoe@nist.gov.

## TECHNOLOGY PARTNERS/COLLABORATORS

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

AlertEnterprise! HYTRUST NEXTLABS RADIANT LOGIC splunk> tdi technologies VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

Certain commercial entities, equipment, products, or materials may be identified to adequately describe an experimental procedure or concept. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology.

**LEARN MORE**

Visit https://nccoe.nist.gov
nccoe@nist.gov
301-975-0200