NIST SPECIAL PUBLICATION 1800-9B

Access Rights Management for the Financial Services Sector

Volume B:
Approach, Architecture, and Security Characteristics

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

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. 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.

National Institute of Standards and Technology Special Publication 1800-9B Natl. Inst. Stand. Technol. Spec. Publ. 1800-9B, 104 pages, August 2017 CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: financial_nccoe@nist.gov

Public comment period: August 31, 2017 through October 31, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Managing access to resources (data) is complicated because internal systems multiply and acquisitions add to the complexity of an organization's IT infrastructure. Identity and access management (IdAM) is the set of technology, policies, and processes that are used to manage access to resources. Access rights management (ARM) is the subset of those technologies, policies, and processes that manage the rights of individuals and systems to access resources (data). In other words, an ARM system enables a company to give the right person the right access to the right resources at the right time. The goal of this project is to demonstrate an ARM solution that is a standards-based technical approach to coordinating and automating updates to and improving the security of the repositories (directories) that maintain the user access information across an organization. The coordination improves cybersecurity by ensuring

that user access information is updated accurately (according to access policies), including disabling accounts or revoking access privileges as user resource access needs change. Cybersecurity is also improved through better monitoring for unauthorized changes (e.g., privilege escalation). The system executes user access changes across the enterprise according to corporate access policies quickly, simultaneously, and consistently. The ARM reference design and example implementation are described in this NIST Cybersecurity "Access Rights Management" practice guide. This project resulted from discussions among NCCoE staff and members of the financial services sector.

This *NIST Cybersecurity Practice Guide* also describes our collaborative efforts with technology providers and financial services stakeholders to address the security challenges of ARM. It provides a modular, open, end-to-end example implementation that can be tailored to financial services companies of varying sizes and sophistication. The use case scenario that provides the underlying impetus for the functionality presented in the guide is based on normal day-to-day business operations. Though the reference solution was demonstrated with a certain suite of products, the guide does not endorse these specific products. Instead, it presents the NIST Cybersecurity Framework (CSF) core functions and subcategories, as well as financial industry guidelines, that a company's security personnel can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a company's existing tools and infrastructure. Planning for deployment of the design gives an organization the opportunity to review and audit the access control information in their directories and get a more global, correlated, disambiguated view of the user access roles and attributes that are currently in effect.

KEYWORDS

Access; authentication; authorization; cybersecurity; directory; provisioning.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Institution
Jagdeep Srinivas	AlertEnterprise
Hemma Prafullchandra	HyTrust
Roger Wigenstam	NextLabs
Don Graham	Radiant Logic
Adam Cohen	Splunk
Clyde Poole	TDi Technologies
Dustin Hayes	Vanguard Integrity Professionals

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:

Product Vendor	Component Name	Function
AlertEnterprise	Enterprise Guardian	Access policy management, administration and account provisioning system
HyTrust	Cloud Control	Privileged user access controller, monitor, and logging system for VSphere
NextLabs	NextLabs	Attribute based access control interface for SharePoint
Radiant Logic	RadiantOne	Virtual directory system
Splunk	Enterprise	Log aggregation and analytics system
TDi Technologies	ConsoleWorks	Application and operating system privileged user access controller, monitor, and logging system
Vanguard Integrity Professionals	Vanguard	Mainframe RACF to LDAP interface system

Contents

List of Figures

List of Tables

1 Summary

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses the challenge to provide a more secure and efficient way to manage access to data and systems. The NCCoE developed a reference design and an example implementation for this problem using commercially available products. This approach delivers an Access Rights Management (ARM) system that coordinates changes throughout the enterprise, thereby reducing the risk of unauthorized access caused by malicious actors or human error. Throughout this practice guide, access is used as a generic term for privileges and permissions to view, modify, and delete data, applications, and systems.

This example implementation is documented as a NIST Cybersecurity Practice Guide, a how-to handbook that presents instructions to implement an ARM system using standards-based, cybersecurity technologies in the real world. Based on risk analysis and regulatory guidance, this design is intended to help companies gain efficiencies in ARM, while saving money and time during the research and proof-of-concept phases of a project. This guide presents an architecture for implementing an ARM that improves the control of user access information using automation. It also quickly identifies unapproved changes such as privilege escalations by including multiple methods of monitoring the user access information repositories (directories).

1.1 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 (HR) 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 collaboration partners that provided the requisite equipment and services, we developed representative use-case scenarios to describe user 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 a company.

1.2 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 a company 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 sector 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. 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.

In the sections that follow, we show how a financial services company can implement an ARM platform using commercially available products to provide a comprehensive management platform for all user access information within the company. As part of the planning process to deploy an ARM system, an organization will have the opportunity to audit the access control information in their directories and get a more global, correlated, disambiguated view of the user access roles and attributes that are currently in effect. User access information includes directory accounts, group membership, and attributes independent of the use of Active Directory or other directory products. We chose the term *user access information* because it is transparent to non-technical readers.

This practice guide:

- Maps security capabilities of the reference design to guidance and best practices from NIST, International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), and the FFIEC CAT
- Delivers:
  - a detailed reference design
  - an example implementation that is modular and can be implemented using different products to achieve the same results
  - instructions for implementers and security engineers, including examples of all the necessary components and installation, configuration, and integration information

- an example implementation that uses products that are readily available and interoperable with existing information technology infrastructure
- solutions that can meet the needs of financial services companies of all sizes

Although the example implementation is built from a suite of commercial products, this practice guide does not endorse these particular products. A company's IT personnel should identify the standards-based products that will best integrate with its existing tools and infrastructure. Companies can adopt this solution or one that adheres to these guidelines in whole, or they can use this guide as a starting point for tailoring and implementing parts of the solution.

The reference design and example implementation support efforts to comply with financial services sector regulations. However, implementation of the reference design or example implementation does not imply or guarantee regulatory compliance.

1.3 Risk Considerations

Members of the financial services sector identified risk factors at both the operational and strategic levels. Operationally, the absence of an ARM platform can increase the risk of compromise of the confidentiality, integrity, and availability of the corporate systems and data.

At the strategic level, an organization might consider the cost of mitigating these risks and the potential return on investment from implementing a product (or multiple products). It may also want to assess if an ARM system can help enhance the productivity of employees, speed delivery of services, or explore the potential to support oversight of resources, including IT, personnel, and data. We review the potential benefits of the reference design in Section 1.4.

We understand that introducing new technology into any environment may introduce new attack vectors. In addition, converging ARM functions concentrates control over the modifications to user access information. We address these key risk areas and provide a comprehensive list of mitigations in Section 6, Security Analysis.

1.4 Benefits

The reference design and example implementation has the following benefits:

- reduces the risk of malicious or untrained people gaining unauthorized access to systems and data
- allows rapid automated provisioning and de-provisioning of user access information, freeing up system administrators to address more critical tasks
- improves management of user access information changes
- rapidly identifies anomalous user account changes

- can be integrated into an organization's existing infrastructure in whole or in part

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to ARM. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-9A: *Executive Summary*
- NIST SP 1800-9B: *Approach, Architecture, and Security Characteristics*—what we built and why **(you are here)**
- NIST SP 1800-9C: *How-To Guide*—instructions for building the example solution

Depending on their role in an organization, readers might use this guide in different ways:

Business decision makers, including chief security and technology officers will be interested in the *Executive Summary (NIST SP 1800-9A)*, which describes the:

- challenges identified by financial services companies
- operational benefits of adopting the solution
- high-level solution description

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-9B,* which describes what we did and why. The following sections will be of particular interest:

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- Section 3.4.2, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

The *Executive Summary, NIST SP 1800-9A,* could be shared with the leadership team members to help them understand the importance of adopting standards-based ways to manage access to data and systems in a secure and efficient manner.

IT professionals who want to implement an approach like this will find the whole practice guide useful. The How-To portion of the guide, *NIST SP 1800-9C*, can be used to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does

not endorse these particular products. An organization can adopt this solution or one that adheres to these guidelines in whole, or it can use this guide as a starting point for tailoring and implementing parts of an ARM solution. An organization's security experts should identify the products that will best integrate with its existing tools and IT system infrastructure. We hope organizations will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A *NIST Cybersecurity Practice Guide* does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute comments using email financial_nccoe@nist.gov or online via the web content tool.

2.1 Typographical Conventions

The following table presents the typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

3 Approach

This project began with a detailed discussion between NCCoE and members of the financial services sector community about their security challenges around implementing least privilege and separation of duty policies. The principle of least privilege, defined as providing the least amount of access (to systems or data) necessary for the user to complete his or her job [1], and the principle of separation of duties, which restricts the amount of responsibilities held by any one individual, are important security tools. The focus of the project became the risk impacts that result from user access information updates not being implemented consistent with corporate access policies. The NCCoE drafted a use case (i.e., project description) that identified the solution security controls with feedback from the financial industry. After an open call in the Federal Register, technology partners volunteered products, services, and resources that provide the desired security controls. The following sections describe the areas of discussion that led to the development of the subject of this practice guide, including the areas of the NIST Cybersecurity Framework (CSF) and FFIEC CAT.

3.1 Audience

This practice guide is intended for individuals or entities interested in understanding the ARM reference design and example solution the NCCoE designed and implemented. The guide describes how financial services companies (or any other sector organization) can add automation to existing identity and access management (IdAM) systems. In addition, the guide describes how to add IdAM monitoring for anomalous identity and access management system changes, such as unauthorized privilege escalations.

3.2 Scope

We determined that the scope should be ARM, including a converged provisioning component. The scope was further refined to include successful execution of the following provisioning functions:

- enabling access for a new employee
- modifying access for an existing employee (including converting an ex-employee to contractor status)
- disabling access for a terminated employee
- identifying anomalous directory changes

The objective of the project is to perform any of these three access change actions from a single management system that can provision user access information changes to all directories (authoritative sources) within a financial services company. The actions can be initiated via an administrative interface by an approved administrator or via a bulk update from a human resource system. In addition, a Monitoring capability was implemented to enhance the security of the directories.

Although the example implementation can provide an approval workflow to ensure that proper management governance is followed, this optional feature was not implemented. Note also that the project does not address access policy decision and enforcement, and identity validation and credential management.

3.3 Assumptions

3.3.1 Security

All network and system changes have the potential to increase the attack surface within an enterprise. Therefore, it is important that the reference design itself be secured to minimize any risks that may otherwise be inherent in its adoption. In the ARM security analysis (Section 6), we identify the security functions and controls that the reference design supports (Section 6.4), and we also discuss the security of the reference design itself (Section 6.5). We assume that all potential adopters of the reference design will implement network security policies. The assessment focuses on how risk factors introduced by the reference design itself are mitigated. We also recommend ways to secure the reference design deployment. However, our evaluation cannot identify all weaknesses, especially those that a specific deployment or specific commercial products may introduce.

3.3.2 Modularity

As noted, this example implementation uses commercially available products. Organizations can swap any of the products we used for ones better suited for their environment. A combination of some or all the components described here, or a single component, can improve the security of identity and access management functions without requiring an organization to remove or replace its existing infrastructure. In addition, organizations may find that we describe new ways to use currently deployed components.

3.3.3 Human Resources Database/Identity Vetting

We assume that a company has a user change process, databases, and other components necessary to establish a valid identity.

3.3.4 Technical Implementation

This practice guide is written from a how-to perspective and aims to provide details on how to design, install, configure, and integrate components. We assume that financial services companies have the technical resources to implement all or parts of the example implementation or have access to companies that can perform the implementation on its behalf. The guide may also provide insights regarding the level of effort and types of resources required to accomplish an ARM implementation.

3.3.5 Limited Scalability Testing

We did not attempt to replicate the user base size that would be found in most companies. We do not identify scalability thresholds in our ARM example implementation because they depend on the type and size of the implementation and are particular to the individual enterprise. We believe the reference design can be applied to any size company because it can be implemented in a modular fashion and is based on standards.

3.3.6 Replication of Enterprise Networks

We were able to replicate the typical information technology or corporate network in a limited manner. The goal was to demonstrate that provisioning functions could be performed from an ARM system regardless of its location in the enterprise. In a real-world environment, the interconnections between enterprise subnetworks depend on the business needs and compliance requirements of the enterprise. We did not attempt to replicate these interconnections. Rather, we acknowledge that implementing our example implementation or its components creates new interfaces across subnetworks.

3.4 Risk Assessment

NIST SP 800-30 Rev. 1, *Risk Management Guide for Information Technology Systems*, defines risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The risk management framework (RMF) guidance, as a whole, proved invaluable in giving us a baseline to assess risks, from which we developed the project, the required security controls of the reference design, and this guide.

We performed two types of risk assessment:

- initial analysis of the risk factors discussed with the financial services companies, which led to the creation of the use case and the desired security posture
- analysis of how to secure the capabilities within the solution and minimize any vulnerabilities that they might introduce (see Section 6, ARM Security Analysis)

3.4.1 Assessing Risk Posture

Using the guidance in NIST's series of publications concerning risk, we worked with financial services companies and the Financial Sector Information Sharing and Analysis Center (FS-ISAC) to identify the most compelling risk factors that financial services companies encounter. We participated in conferences and met with members of the financial services sector to define the main security risks to business operations. These discussions resulted in the identification of a primary risk area—the lack of

automated ARM capabilities. We then identified the following threats that an ARM system can help mitigate:

- insiders gaining access through access creep and undocumented accounts
- regular users unintentionally accessing unauthorized data or systems
- external actors gaining access by using malware techniques

These discussions also gave us an understanding of the vulnerabilities that threat actors can exploit due the lack of automated ARM capabilities. We identified the following vulnerabilities:

- undocumented accounts
- accounts with unnecessarily elevated privileges
- dependence on humans to enforce user access policies

These risk factors can also be viewed from a business operations risk perspective:

- impact on service delivery—ensuring that people have access only to the systems they need to perform their job functions reduces the risk of inappropriate or unauthorized use of access that could then affect availability to others
- cost of implementation—implementing ARM once and using it across all systems may reduce both system development costs and operational costs
- compliance with existing industry standards—FFIEC requires deliberate and timely control of logical access to corporate resources
- maintenance of reputation and public image

We subsequently translated the risk factors identified to security functions and subcategories within the NIST CSF and the FFIEC CAT that the design needed to support. We also mapped the categories to NIST's SP 800-53 Rev.4 [2] controls and IEC/ISO controls for additional guidance in Table 3-1.

3.4.2 Security Control Map

As explained in Section 3.4.1, we identified the CSF security functions and subcategories that we wanted the reference design to support through a risk analysis process conducted in collaboration with our financial services sector stakeholders. This was a critical first step in designing the reference design and example implementation to mitigate the risk factors. Table 3-1 lists the addressed CSF functions and subcategories and maps them to relevant NIST standards, industry standards, controls, and best practices, including those published by FFIEC. The items in the FFIEC Examination Handbook column of Table 3-1 are mapped from and reflect the FFIEC Cybersecurity Assessment Tool, dated June 2015, Appendix A – Mapping Baseline Statements to FFIEC IT Examination Handbook. The references provide solution validation points in that they list specific security capabilities that a solution addressing the CSF subcategories would be expected to exhibit.

Organizations can use Table 3-1 to identify the CSF subcategories and NIST 800-53 controls or FFIEC guidance that they are interested in addressing. Note that not all the CSF subcategories or FFIEC guidance can be implemented using technology. The subcategories that describe processes and organizational policies are supported by the reference design, not implemented. Therefore, any organization adopting an ARM solution would need to develop and implement specific processes that address those processes and policies. For example, some of the subcategories within the CSF function "Identify" are processes and policies that should be developed prior to an ARM implementation.

430 **Table 3-1 ARM Reference Design CSF Core Components Map**

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
ID.AM-3: Organizational communication and data flows are mapped.	AC-4, CA-3, CA-9, PL-8	A.13.2.1	D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	IS.B.1.3: Identify changes to the technology infrastructure or new products and services that might increase the institution's risk from information security issues. Consider … network topology, including changes to configuration or components. IS.B.9: A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic.
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established.	CP-2, PS-7, PM-11	A.6.1.1	D1.R.St.B.1: Information security roles and responsibilities have been identified.	IS.B.7: Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Financial institutions should define these responsibilities in their security policy.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
ID.BE-4: Dependencies and critical functions for delivery of critical services are established.	SA-14, CP-8, PE-9, PE-11, PM-8, SA-14	A.11.2.2, A.11.2.3, A.12.1.3	D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	IS.WP.I.4.1: Review and evaluate security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution: software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
PR.AC-1: Identities and credentials are managed for authorized devices and users.	AC-2, IA Family	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	D3.PC.Im.B.7: Access to make changes to systems configurations (including virtual machines and hypervisor) is controlled and monitored. D3.PC.AM.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware. D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	IS.B.56: Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include maintaining appropriately robust configuration management and change control processes.

PR.AC-3: Remote access is managed.	AC-17, AC-19, AC-20	A.6.2.2, A.13.1.1, A.13.2.1	D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. D3.PC.Im.Int.2: Security controls are used for remote access to all administrative consoles, including restricted virtual systems.	IS.B.45: Financial institutions should secure remote access to and from their systems … securing remote access devices and using strong authentication and encryption to secure communications. IS.WP.II.B.17: Determine whether remote access devices and network access points for remote equipment are appropriately controlled. For example, authentication is of appropriate strength (e.g., two-factor for sensitive components), and remote access devices are appropriately secured and controlled by the institution. IS.B.56: Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include maintaining appropriately robust configuration management and change control processes. IS.WP.II.H: Determine whether management explicitly follows a recognized security standard development process or adheres to widely recognized industry standards.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. D3.PC.Am.B.2: Employee access to systems and confidential data provides for separation of duties. D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	IS.B.19: Access rights should be based on the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. IS.WP.I.4.1: Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation. IS.B.18: Financial institutions should have an effective process to administer access rights, including assigning users and devices only the access required to perform their required functions and updating access rights based on personnel or system changes.

PR.DS-1: Data-at-rest is protected.	SC-28	A.8.2.3	D1.G.IT.B.13: Confidential data is identified on the institution's network. D3.PC.Am.A.1: Encryption of select data-at-rest is determined by the institution's data classification and risk assessment.	IS.B.9: A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic. IS.WP.I.3.1: Consider whether the institution has identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer non-public information as well as the risks to the institution. IS.B.12: Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation. IS.B.51: Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information.

PR.DS-2: Data-in-transit is protected.	AC-4, SC-8, SC-12, SC-13, SC-17, SC-23, SC-8	A.8.2, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet). D3.PC.Am.E.5: Controls are in place to prevent unauthorized access to cryptographic keys. D3.PC.Am.Int.7: Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones. D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used. D3.PC.Im.Int.1: The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.	IS.B.51: Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. IS.WP.II.B.15: Determine whether appropriate controls exist over the confidentiality and integrity of data transmitted over the network (e.g., encryption, parity checks, message authentication). IS.B.21: Encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates). IS.B.33: Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as domain name service (DNS). Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
				IS.WP.I.4.1: Evaluate the appropriateness of technical controls mediating access between security domains.
PR.DS-5: Protections against data leaks are implemented.	AC-4, AC-5, AC-6, SC-8, SC-13, SI-4	A.6.1.2, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.13.1.3, A.13.2.1, A.13.2.3	D3.PC.Am.Int.1: The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.	IS.B.19: Access rights should be based on the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. IS.WP.I.4.1: Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	AU Family IR-5, IR-6	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.	IS.B.79: Institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility. IS.WP.II.B.13: Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period and that reporting to those logs is adequately protected. IS.B.83: Because the identification of incidents requires monitoring and management, response centers frequently use (security information management (SIM) tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. (p. 29).	AC-3, CM-7	A.9.1.2	D3.PC.Am.B.4: User access reviews are performed periodically for all systems and applications based on the risk to the application or system. D3.PC.Am.B.3: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). D4.RM.Om.Int.1: Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.	IS.B.18: Reviewing periodically users' access rights at an appropriate frequency based on the risk to the application or system. IS.WP.I.7.6: Evaluate the process used to monitor and enforce policy compliance (e.g., granting and revocation of user rights). IS.B.19: Authorization for privileged access should be tightly controlled. IS-WP.II.A.1: Determine whether access to system administrator level is adequately controlled and monitored. OT.B.26: Appropriate access controls and monitoring should be in place between service provider's systems and the institution.

PR.PT-4: Communications and control networks are protected.	AC-4, AC-17, AC-18, CP-8, SC-7	A.13.1.1, A.13.2.1	D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used. D3.PC.Im.Int.1: The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.	IS.B.33: Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as domain name service (DNS). Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening. IS.WP.I.4.1: Evaluate the appropriateness of technical controls mediating access between security domains. Evaluate the adequacy of security policies and standards relative to physical controls over access to hardware, software, storage media, paper records, and facilities. IS.B.46: Management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. OPS.B.23: Transmission controls should address both physical and logical risks. In large, complex institutions,

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
				management should consider segregating wide area networks (WAN) and local area networks (LAN) segments with firewalls that restrict access as well as the content of inbound and outbound traffic. IS.WP.I.4: Review security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution … Network Access - Remote Access Controls (including wireless, virtual private network, modems, and Internet-based). OPS.WP.8.1: Determine whether management has implemented appropriate daily operational controls and processes including … alignment of telecommunication architecture and process with the strategic plan.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	AC-4, CM-2, SI-4	A.13.1.1, A.13.2.1	D3.DC.Ev.B.1: A normal network activity baseline is established.	IS.B.77: The behavior-based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices. IS-WP-II-M: Determine whether appropriate detection capabilities exist related to network-related anomalies.
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	CA-7, IR-5, SI-4	A.12.4.1	D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	IS.B.83: Because the identification of incidents requires monitoring and management, response centers frequently use SIM tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents. IS.WP.II.G.7: Determine whether appropriate logs are maintained and available to support incident detection and response efforts. IS.B.43: Management has the capability to filter logs for potential security events and provide adequate reporting and alerting capabilities.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
DE.AE-5: Incident alert thresholds are established.	IR-4, IR-5	A.12.4.1	D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions. D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response. D3.DC.An.Int.3: Tools actively monitor security logs for anomalous behavior and alert within established parameters.	IS.B.83: Because the identification of incidents requires monitoring and management, response centers frequently use SIM tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents. IS.WP.II.G.7: Determine whether appropriate logs are maintained and available to support incident detection and response efforts. IS.B.43: Management has the capability to filter logs for potential security events and provide adequate reporting and alerting capabilities.

CSF Subcategory	NIST 800-53 rev4[a]	IEC/ISO 27001[b]	FFIEC CAT v1[c]	FFIEC IT Exam Handbook Information Security[d]
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	A.12.4.1	D3.DC.An.A.3: A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.	IS.B.73: Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by monitoring network and host activity to identify policy violations and anomalous behavior. IS.WP.II.M.1: Review security procedures for report monitoring to identify unauthorized or unusual activities. IS.B.77: The behavior-based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices.

a. Mapping taken from "Framework for Improving Critical Infrastructure Cybersecurity," NIST, February 12, 2014

b. Mapping taken from "Framework for Improving Critical Infrastructure Cybersecurity," NIST, February 12, 2014

c. Mapping taken from FFIEC Cybersecurity Assessment Tool Appendix B, FFIEC, June 2015

d. Mapping taken from FFIEC Cybersecurity Assessment Tool Appendix A, FFIEC, June 2015

3.5 Security Functions and Subcategories Related to FFIEC

The example implementation is responsive to the desire to support compliance with the FFIEC CAT guidance as well as the NIST standards and best practices as detailed in Table 3-1.

The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) provides specific guidance that applies to financial institutions and was used as a reference by the development team. The proposed solution is designed to be CAT-informed. This document attempts to capture some of the key areas where CAT guidance is relevant to elements of the solution and its implementation, for reference purposes. Please consult an auditor or examiner for any questions on FFIEC compliance.

The example implementation is informed by FFIEC CAT guidance and may contribute to CAT-aligned implementations by providing mechanisms supporting management, logging, and auditing of all ARM activity efficiently and cost effectively. With this solution in place, information regarding which users have access to which resources is maintained by the existing directories and modified via the central administration and provisioning system. Without the solution, the user access information is provisioned separately to each directory.

Table 3.2 describes how the ARM solution supports compliance with FFIEC CAT guidance.

Table 3-2 FFIEC CAT Guidance

FFIEC CAT Guidance	ARM Solution Characteristics
D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	Data flows into and out of the ARM system are documented and enforced because of the asset value to the organization.
D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	The ARM system is classified as a critical asset that needs to be protected.
D3.PC.AM.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware.	The ARM system manages the updates to the identity and authentication systems (directories) using automation to ensure access policy compliance.
D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	The ARM workflow receives information from the HR system on terminations and job changes. It can immediately de-provision access for these employees. The

FFIEC CAT Guidance	ARM Solution Characteristics
	workflow can also include an approval process.
D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. **D3.PC.Im.Int.2: Security controls are used for remote access to all administrative consoles, including restricted virtual systems.** **D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.** **D3.PC.Am.B.2: Employee access to systems and confidential data provides for separation of duties.** **D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.** **D3.PC.Am.Int.1: The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.**	A privileged account management (PAM) system is not required as part of an ARM solution. PAM was included to enhance the security of the implementation and addresses this guidance.
D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet). **D3.PC.Am.E.5: Controls are in place to prevent unauthorized access to cryptographic keys.** **D3.PC.Am.Int.7: Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.** **D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.** **D3.PC.Im.Int.1: The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.**	The solution uses Lightweight Directory Access Protocol Secure (LDAPS) to protect data-in-transit between the ARM provisioning system and the directories. The solution is implemented to address this guidance.
D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.	The ARM solution includes a security management and monitoring system to address this guidance.

FFIEC CAT Guidance	ARM Solution Characteristics
D3.PC.Am.B.4: User access reviews are performed periodically for all systems and applications based on the risk to the application or system. **D3.PC.Am.B.3: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).** **D4.RM.Om.Int.1: Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.** **D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).** **D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions.** **D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response.** **D3.DC.An.Int.3: Tools actively monitor security logs for anomalous behavior and alert within established parameters.** **D3.DC.An.A.3: A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.**	

452

3.6 Technologies

Table 3.3 lists all the technologies used in this project and provides a mapping between the generic application term, the specific product used, and the security control(s) that the product provides. (Recall that Table 3-1 explained the CSF subcategory codes.) This table describes only the product capabilities used in our example solution. Many of the products have additional security capabilities that were not used in our example implementation. The table's Product column contains links to vendor product information that describes the full capabilities.

Table 3-3 Products and Technologies

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
Provision, modify or revoke access throughout all user information repositories (directories)	User access policy management	PR.AC-1: Identities and credentials are managed for authorized devices and users.	Virtual Directory	Radiant Logic	RadiantOne VDS Note: Radiant Logic changed their product name from RadiantOne Virtual Directory Server (VDS) to RadiantOne Federated Identity Service (FID)		Consolidated source for digital identities and authorized access to resources
	User access policy management	PR.AC-1: Identities and credentials are managed for authorized	Policy management	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
	User access authoritative information repository	devices and users. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	User access information management	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard
	Centralized provisioning of access information		Provisioning	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard
	User access information repository		Directory	AlertEnterprise	Guardian	4.0 SP04 HF3	Maintains the authoritative source for user access information
				Microsoft	Active Directory		User access information repository
				OpenLDAP	OpenLDAP		User access information repository
			Mainframe RACF interface	Vanguard Integrity Professionals	Vanguard		User access information repository and RACF (mainframe access control interface)

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
	Privileged user access control	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. PR.AC-3: Remote access is managed.	Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of operating systems (OSs) and applications. Limits functions available to privileged users to reduce the potential of out of policy activities.
			Privileged User Access Management	HyTrust	CloudControl		Creates an audit trail of access by privileged users of the virtual environment management system
Protect data	Protect stored data	PR.DS-1: Data-at-rest is protected.	Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of OSs and applications. Limits functions available to privileged users to reduce the potential of out of policy activities.
	Protect data while in transit	PR.DS-2: Data-in-transit is protected.		Multiple products	-		Data-in-transit is protected using encrypted transmissions such as LDAPS. Protection is also provided via network segmentation.

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
	Limit functions available to privileged users	PR.DS-5: Protections against data leaks are implemented.	Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of OSs and applications. Limits functions available to privileged users to reduce the potential of out-of-policy activities.
	Limit access to control network	PR.PT-4: Communications and control networks are protected.		Multiple products	-		Communications are protected through network segmentation.
Track privilege user activity	Monitor privileged user activity	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Records logs from all systems to monitor for anomalous personnel activity.
			Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of OSs and applications. Limits functions available to privileged users to reduce the potential of out of policy activities.

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
Log aggregation, correlation and analysis	Aggregate log data and analyze for anomalous activity	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Records logs from all systems to monitor for anomalous personnel activity.
	Generate alerts based on anomalous activity	DE.AE-5: Incident alert thresholds are established.	Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Log analysis and correlation rules are established to alert incidents.
	Log management	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	Log data timing and security	TDi Technologies	Console Works	4.9-0u0	Controls access to industrial control system (ICS) devices by people (ICS engineers and technicians).
	Log aggregation and analysis		Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Records logs for analysis and correlation.

459

4 Architecture

ARM involves the organization and control (by organizational policy) of approved access information (directory user account details) used to authenticate and authorize users for access to organizational resources. This guide presents an architecture for implementing an ARM automation and security solution, which improves the control of access information and the cybersecurity monitoring of the information repositories (directories).

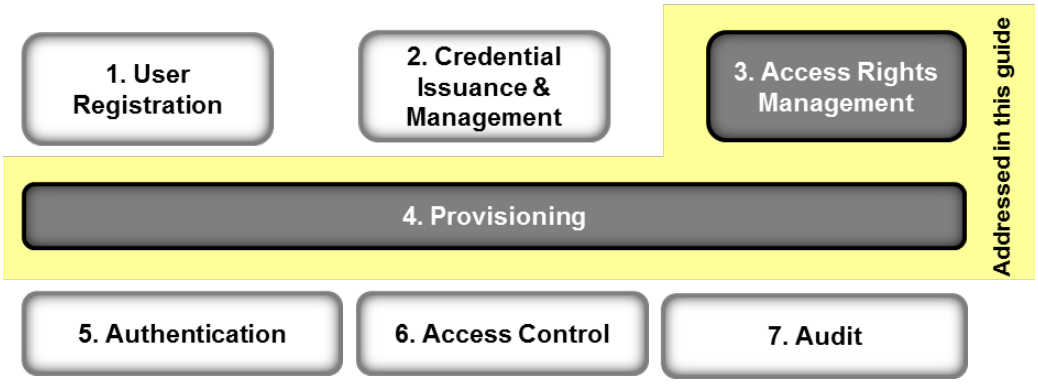
This section describes the high-level architecture and reference design for the ARM system.

4.1 Architecture Description

4.1.1 High-Level Architecture

Figure 4-1 depicts a high-level architecture for identity and access management systems, followed by a description of each of the capabilities. The ARM-solution described in this practice guide is composed of the capabilities illustrated in the yellow portion of Figure 4-1 and is designed to address the security functions and subcategories described in Table 3-1.

Figure 4-1 ARM High-Level Architecture



1. **User registration** determines that there is a reason to give a person access to resources, verifies the person's identity, and creates one or more digital identities for the person.
2. **Credential issuance and management** [3] provides life-cycle management of credentials such as employee badges or digital certificates.
3. **Access rights management** (ARM)determines the resources a digital identity is allowed to use. Arm includes Policy Management and Policy Administration capabilities. (addressed by this guide). In this document, the terms digital identity, account, and user access information are synonymous.

4. **Provisioning** populates repositories (directories) digital identity, credential, and access rights information for use in authentication, access control, and audit. (addressed by this guide).
5. **Authentication** establishes confidence in a person's digital identity.
6. **Access control** [4] allows or denies a digital identity access to a resource.
7. **Audit** maintains a record of resource access attempts by a digital identity as well as changes to digital identities.

The following capabilities included in the high-level architecture are not addressed in this practice guide: User Registration, Credential Issuance and Management, Authentication, Access Control and Audit. These capabilities are not addressed because they are either manual administrative processes invoked when an employee is hired or changes jobs or are automated (run-time) activities that occur every time a person attempts to access a corporate resource (e.g., computer system).

Access rights management and provisioning are addressed in the project. Provisioning connects the administrative activities to the run-time activities by populating and modifying the directories with the user access information. Access rights management (policy management and administration) includes automated functions such as assigning user access rights based organizational policies and determining the proper user access information to be stored in the directories.

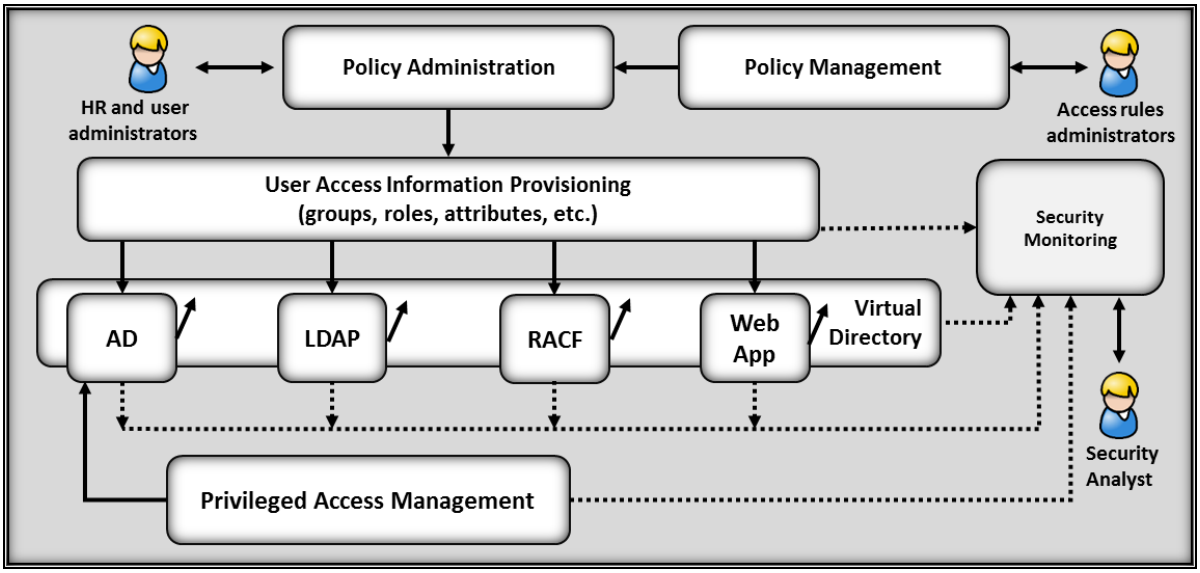
Directories, such as Microsoft Active Directory (AD), Resource Access Control Facility (RACF), and OpenLDAP, are often used in the implementation of run-time functions. Companies typically maintain multiple directories based on application needs and business acquisitions/combinations. These directories are often managed by multiple administrators. Managing access information across directories is complicated because of the coordination effort required among directory administrators. This leads to unwanted situations such as:

- administrators finding it difficult to ensure that employees have access to the resources they need to perform their jobs, and only those resources
- newly hired employees not having access to all the resources they need
- employees who change jobs retaining access to resources they no longer need (access or privilege creep)
- terminated employees retaining access long after they leave

4.1.2 Reference Design

The reference design described here addresses the unwanted situations by implementing ARM and Provisioning capabilities for an enterprise. Figure 4-2 illustrates the reference design of the solution.

514 **Figure 4-2 ARM Reference Design**



515

516 Note: 1) Solid lines represent policy and user access information transfer/communications, 2) the dotted
517 lines indicate system event and log transfer/communications.

518 The *Policy Management* capability provides the interface and automation that enable the company to
519 document and store access policy rules for use by the *Policy Administration* capability. The *Policy*
520 *Management* system includes an interface for business and application owners to record the attributes,
521 groups, or roles that are required to allow access to data and applications.

522 For example, an individual who serves in the role of bank manager and works in the mid-west division of
523 her company may be given certain access rights that are denied to a bank manager in a different region
524 or division. Implementation of separation of duties and of least privilege access policies enables
525 organizations to reduce the risk of unauthorized access. However, over time, the number and
526 combination of attributes, group memberships, and roles can be quite large. Companies should make
527 efforts to consolidate the attributes, group memberships, and roles used to reduce the number of
528 combinations and complexity **wherever possible**.

529 The *Policy Administration* capability provides the interface and automation, including approval
530 workflows, to create, modify, and disable user accounts within the directories. It also provides the
531 automation to read files from an HR system that contain user information (new, changed, or terminated
532 employee information). After the *Policy Administration* system reads the user information, it references
533 the user access policies from the *Policy Management* system and initiates any workflows required for
534 access approvals. The workflow may require multiple approvals. In some cases, workflows check for
535 training or other corporate credentials as part of the approval process. The system will then initiate the
536 approved changes (performed by the provisioning capability) needed in all the directories of the

company, virtually simultaneously and within corporate policy. Automation greatly reduces the chances of incorrect account creation or changes.

The *User Access Information Provisioning* capability performs the directory access and change functions to apply the approved changes processed by the *Policy Administration* system. The provisioning capability generates logs for each change action. The *Security Monitor* uses these logs as an input to the anomalous activity monitoring analytics.

The *Virtual Directory* capability performs a directory caching function that is used to monitor the state of the directories. The *Virtual Directory* is configured to mirror the contents of the directories. Directory changes are identified in real time and logged by the *Virtual Directory*. The *Security Monitor* uses this information as an input to the anomalous activity monitoring analytics.

The *Privileged Account Management* (PAM) capability provides the management and control of privileged users of the ARM capabilities and underlying infrastructure. The capability includes logging of user actions (including keystrokes and mouse clicks) and logins, credential management, and user action controls. The *Security Monitor* uses this information as an input to the anomalous activity monitoring analytics. User action controls can include limiting the types of commands users can run.

The *Security Monitor* capability collects and analyzes logs from the provisioning capability, directories, PAM, and the virtual directory. Analytics monitor the incoming logs for indications of anomalous activity. In the example implementation, anomalous activity has been defined as any change to a user account within any directory that the provisioning system did not initiate. Analytics have been created to generate an alert for unexpected changes and logins. Unexpected changes may be an indicator of preparations for or actual malicious activity. The Security Monitoring capability also monitors the PAM capability for all system logins. The monitoring analytics will correlate these logins with directory changes.

The ARM workflow is a pre-defined sequence of steps to process each user access change request. The steps may include approval requests that require an individual or individuals to acknowledge and approve a user access information change before the workflow completes and the change is provisioned. The ARM capability, through provisioning, manages changes to the information in the directories. The combined capabilities can reduce the time to update access information. They also ensure that changes are provisioned consistently across multiple directories and improve the audit trail. The Monitoring Capability is designed to identify directory changes generated by the provisioning system and approved administrators. If an unauthorized change to the user access information in a directory occurs (i.e., a change is made directly rather than being made via the provisioning system), the monitoring system generates an alert for the security analysts. Once an ARM solution is implemented,

administrators do not need to make changes to the directories except for limited situations using the PAM capability.

THE EXAMPLE IMPLEMENTATION WAS DESIGNED TO ADDRESS FOUR BASIC TRANSACTIONS:

1. Creating all required user access information for a new employee in the appropriate directories
2. Updating directories for an existing employee who is changing jobs or requires a temporary access change (or change to contractor status)
3. Disabling all user accounts within ALL the appropriate directories for a terminated employee
4. Improving monitoring of directories for anomalous activity

The reference design does not assume that each person will have a single digital identity. A current employee is likely to have several distinct digital identities because of independent management of the directories. Requiring a single digital identity would create a significant challenge to the adoption and implementation of the reference design. The reference design supports continued use of multiple digital identifiers for employees. A virtual directory has been included in the solution to enhance the security of the directories by monitoring them for changes in real time. The virtual directory can also be used to assist in migrating users to a single digital identity.

Whereas the system to manage access changes is converged, the authority to make access changes remains distributed among appropriate company management. Some access changes will require explicit approval before being authorized. For these situations, the workflow notifies one or more access approvers for each such resource and waits for responses. When the workflow receives approvals, it provisions the authorized access changes in the directories. All information about approved, pending, and provisioned access changes are maintained in the workflow system. Pending access authorizations may be either authorizations that have been approved but not yet provisioned or time-bounded authorizations to be provisioned/de-provisioned at a future time. Explicit approval is used to ensure that managers and system owners retain control over access to critical systems.

When the HR system notifies the workflow that an employee has been terminated, the workflow removes or disables all the employee's accounts from the directories. Integration with HR allows for rapid activation, changes and de-activation of accounts across the organization. These capabilities reduce overhead and administrative downtime. Organizations may benefit significantly from reductions in the time to change access.

5 Example Implementation

This section describes the components of the example implementation of the reference design described in Section 4. A repeatable, demonstrable example of the reference design, it uses the products of participating vendors (collaboration team). The example implementation is not a reference implementation because, we believe, the products used are not the only products (or combination of products) that can provide the capabilities in the reference design.

5.1 Example Implementation Description

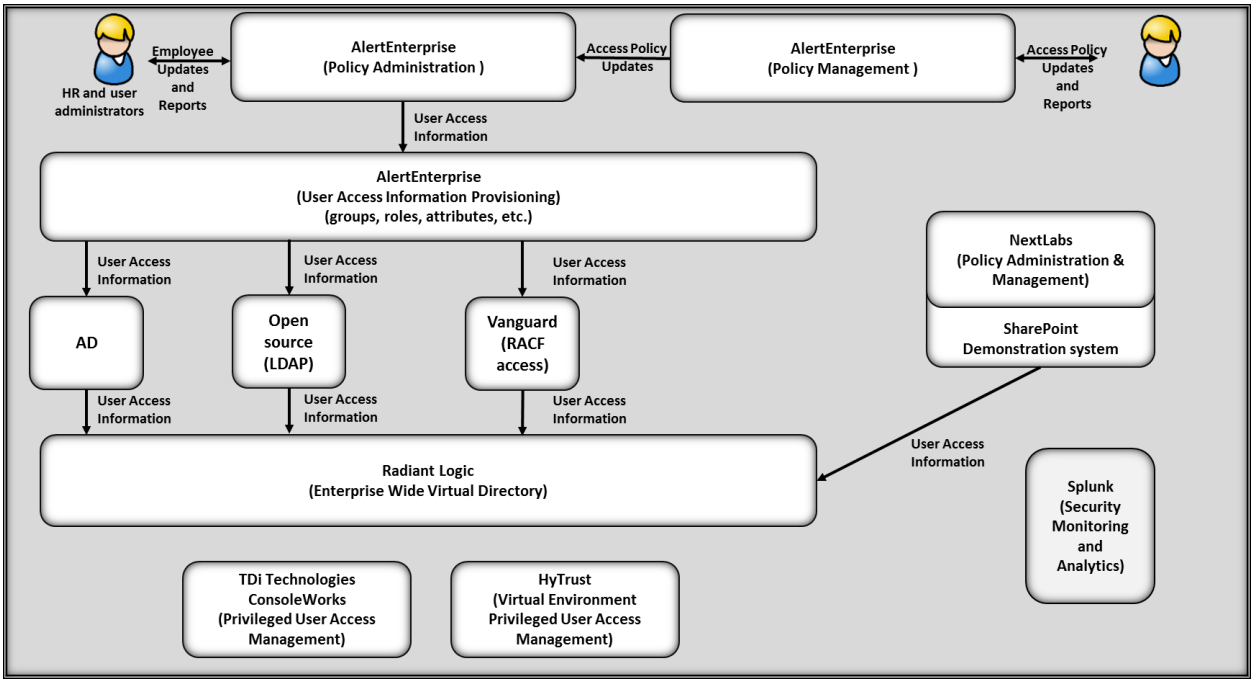
The example implementation is constructed on the NCCoE lab's infrastructure, which consists of a VMware vSphere virtualization operating environment. We used network-attached storage and virtual switches to interconnect the solution components as well as Internet access. The lab network is not connected to the NIST enterprise network. Table 5-1 lists (alphabetically) the software and hardware components we used in the example implementation, as well the specific function each component contributes.

Table 5-1 Example Implementation Component List

Product Vendor	Component Name	Function
AlertEnterprise	Enterprise Guardian	Automation, interface and translation between ARM IdAM servers and the HR system
HyTrust	Cloud Control	Privileged user access controller, monitor, and logging system for VSphere
NextLabs	NextLabs	Attribute-based access control interface for SharePoint
Radiant Logic	RadiantOne	Virtual directory system
Splunk	Enterprise	Log aggregation and analytics system
TDi Technologies	ConsoleWorks	Privileged user access controller, monitor, and logging system
Vanguard Integrity Professionals	Vanguard	Mainframe RACF to LDAP interface system

Figure 5-1 illustrates the example implementation.

608 **Figure 5-1 Example Implementation**



609

610 *Note:* The lines indicate the direction of information flow among components of the architecture.

611 AlertEnterprise (AE) Enterprise Guardian implements the workflow (*Policy Administration*) and the *Policy*
612 *Management* capabilities. It receives input from an HR system, which we simulated using a manually
613 produced comma-separated value (.csv) file. A .csv file was used to simulate a human resources (HR)
614 system because the NCCoE lab does not have an HR system. A mutually authenticated, integrity-
615 protected connection between an HR system and the Policy Administration capability is the preferred
616 solution. AE Enterprise Guardian also provisions information to the directory instances. No relationship
617 among these directories is assumed. The Policy Management capability provides an interface for
618 management to record access/privilege policies.

619 Privileged account management is an important to ensure separation of duties and manage
620 administrative accesses. ConsoleWorks uses the Active Directory account information to control
621 privileged user access to OS and application administrative accounts. In addition, we installed HyTrust
622 Cloud Control, to manage privileged user access to the virtual environment management accounts.
623 Cloud Control was installed with manually assigned user access permissions to depict an alternative
624 approach for the implementation of privileged account management.

625 Radiant Logic RadiantOne Virtual Directory System (VDS) is integrated with the directories in the
626 solution: Active Directory, OpenLDAP, and Vanguard. RadiantOne provides a Virtual Directory capability
627 that is used to integrate the group and attribute information from each directory for each user into a

single view. In the example implementation, the caching capability of this product provides a directory Monitoring capability that identifies user access/account changes in real time and reports those changes to the Security Monitoring capability.

NextLabs is integrated with an instance of SharePoint. NextLabs provides an attribute based access control system used in conjunction with the VDS to demonstrate the ARM example implementation functionality.

Splunk Enterprise is integrated with the directories, VDS, and Enterprise Guardian provisioning systems. It is used for log aggregation and storage as well for log analytics and correlation to identify anomalous conditions for security event alerting purposes.

5.2 Operation of the Example Implementation

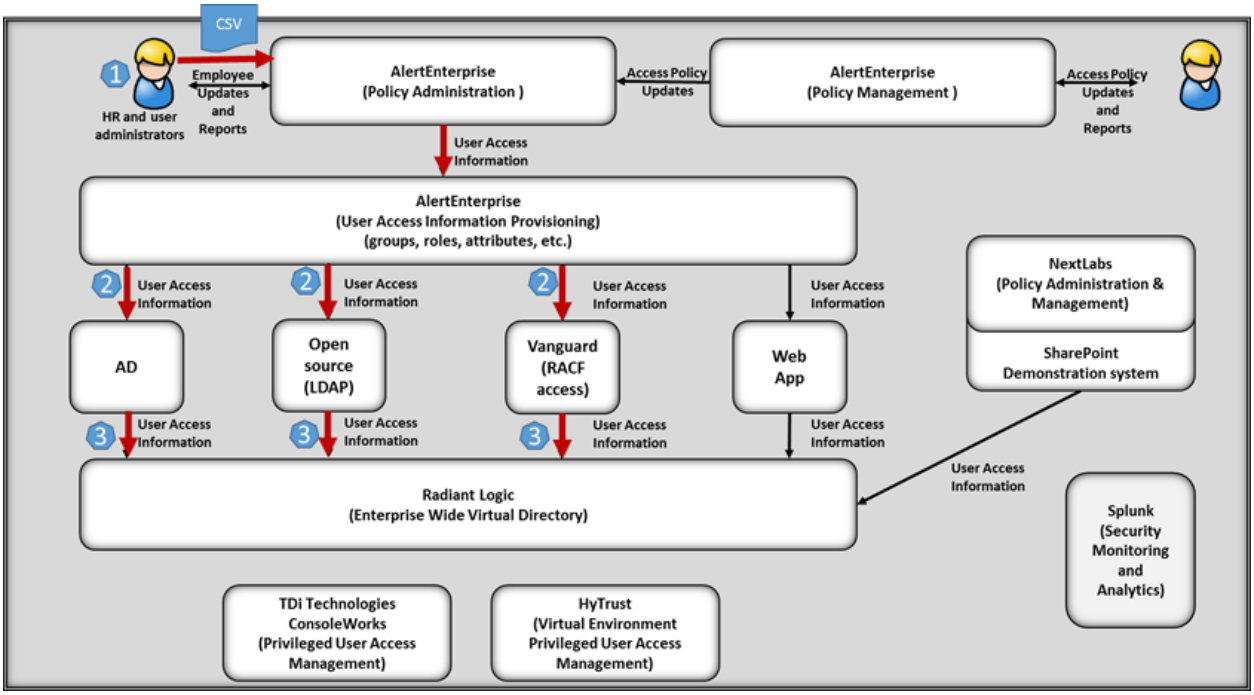
This section explains how the example implementation addresses the risk functions identified in Section 3.4.1. Those factors include inability to centrally manage user accounts and inability to provision, modify, or revoke access throughout the enterprise in a timely manner.

Before operating the solution, the access policies are recorded in the Policy Management capability. The AE Enterprise Guardian (policy management system) capability assists in automated policy compliance by providing an interface to record enterprise access policies. The policy management system feeds the policy administration system with the policy rules required to assign user access information to employees when new employees join the enterprise or change jobs.

The operation of the solution has three primary steps:

1. An update comes from the HR system (see Figure 5-2). The update consists of a .csv file that contains data on new employees and job changes for existing employees (including terminated employees). The AE Enterprise Guardian (policy administration system) reads the data from the HR .csv file. It then initiates the workflow that identifies the user access information to be provisioned to the appropriate directories based on the policies stored in the Policy Management capability. The example implementation does not include management approval in the workflow.
2. The workflow passes the user access information to the provisioning system, which populates the appropriate directories with the user/account access information (e.g., group membership, attributes) for new users and makes changes to the information for existing users as needed, based on the HR user update. If an employee is terminated, all his or her accounts are disabled in this step. Data-in-transit is protected using encryption.
3. once the directories are updated, the updates propagate to the virtual directory. The VDS compares the new version of the directory contents to its cached version at pre-defined intervals. If changes are identified, they are recorded by updating the cache and reported via the logging function. Data-in-transit is protected using encryption.

663 **Figure 5-2 Example Implementation Data Flow**

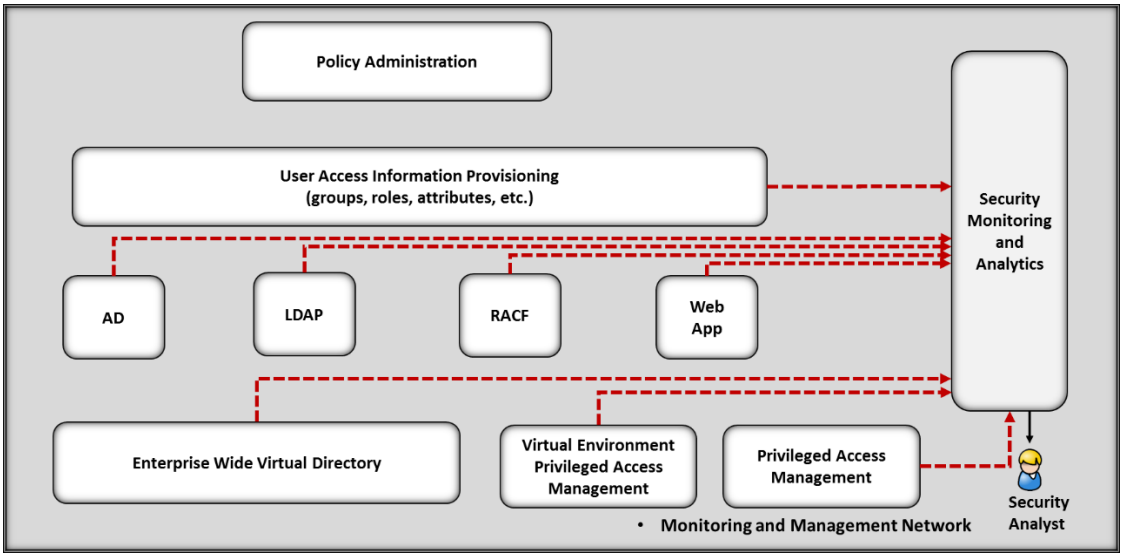


664

665 *Note:* The red lines show the data flows; their arrows indicate the flow direction.

666 The solution includes a monitoring and analytics component to detect anomalous conditions and activity
667 (see Figure 5-3). The analytics correlate logs from the provisioning system with logs from the directories
668 and the virtual directory. The logs from each system report changes to user/account information.
669 Therefore, all changes to an account within a directory must match the changes reported from the
670 provisioning system and virtual directory. If changes occur without matching logs, the security
671 Monitoring Capability generates an alert for an analyst to investigate. The full assessment of the security
672 aspects of the solution are described in Section 6.

673 **Figure 5-3 Monitoring Data Flow**



674

675 *Note:* The red dashed lines depict data flows with arrows indicating the flow direction. The data in
676 transit is protected by encryption.

677 Privileged accounts are accessed via the PAM system. These accounts/users have permission to make
678 changes and maintain the systems within their authority. All use of the PAM system is monitored and
679 logged by the Security Monitoring Capability. Anomalous activity for a privileged account, including
680 multiple failed PAM system login attempts, can be configured to alert.

681 The NextLabs system is used in conjunction with SharePoint to demonstrate the ARM example
682 implementation operations. NextLabs integrates with SharePoint to manage access to SharePoint
683 pages/sites. In the example implementation, SharePoint represents web applications. The site access is
684 based on an attribute-based access control model implemented in the NextLabs system. NextLabs
685 provides the policy decision point capability for the demonstration. NextLabs uses the VDS for user
686 access information.

687 5.2.1 Example Implementation Network Components Overview

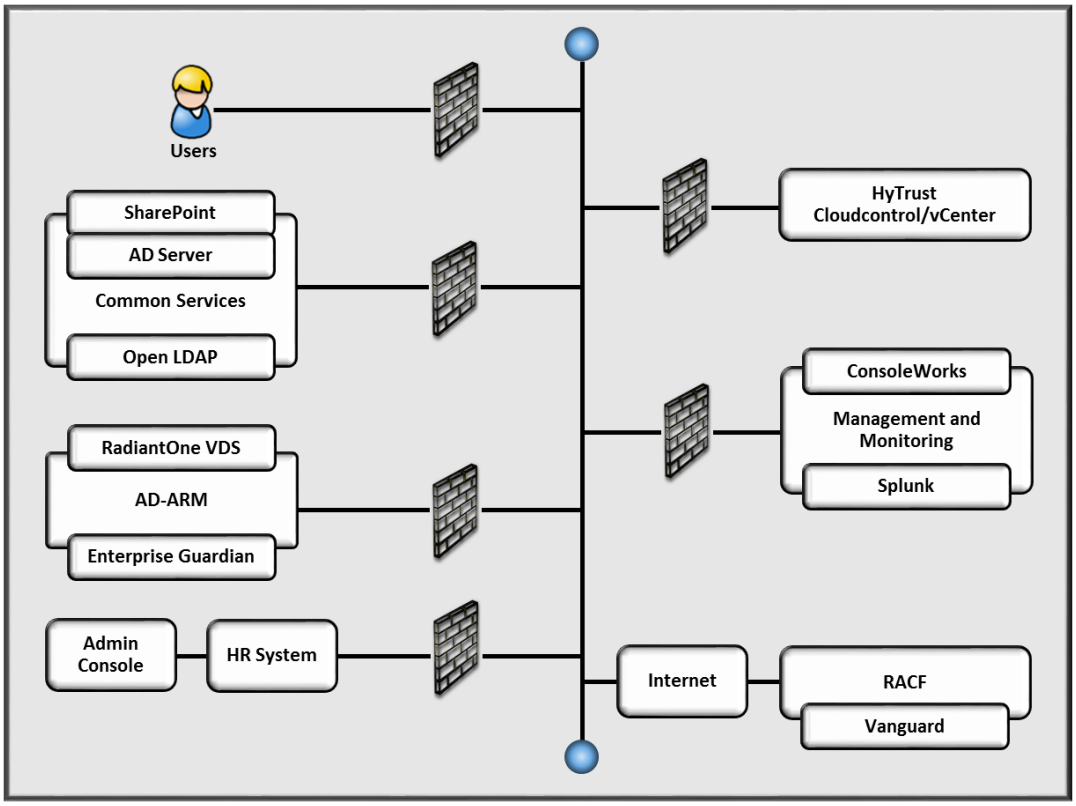
688 The example implementation architecture consists of multiple networks that partially mirror the
689 infrastructure of a typical financial services company. A management network was implemented to
690 facilitate the management and monitoring of the systems. The example implementation consists of the
691 following subnetworks:

692 - common services
693 - access rights management (ID-ARM)
694 - end-user systems

- virtual environment management
- users
- management and monitoring
- HR
- backbone

These subnetworks were implemented separately in line with best practices for enterprise infrastructure. Firewalls block all traffic except required internetwork communications.

Figure 5-4 ARM Example Implementation Network



The subnetworks shown in Figure 5-4 are described in the following paragraphs.

Internet—The lab environment can access the public Internet to facilitate access to a mainframe (RACF) Vanguard Authenticator demonstration system (provided by Vanguard Integrity Professionals) by the ARM example implementation.

Switching and Routing—Switching in the architecture is executed using a series of physical and virtual switches. Virtual Local Area Networks (VLANs) are implemented to segment the networks shown in

Figure 5-4. VLAN switching functions are handled by physical switches and the virtual environment. Routing was accomplished using routers that also hosted the firewalls.

Backbone—The backbone network provides a protected network space that the other networks can use to route traffic across.

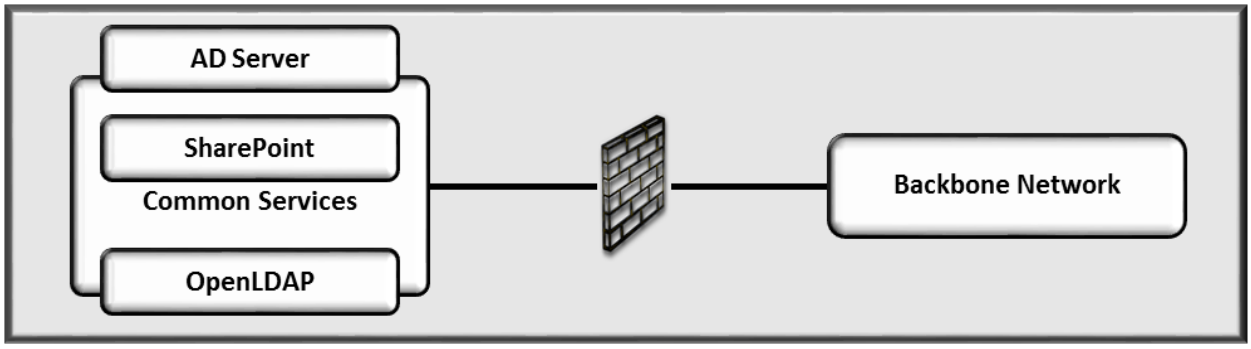
5.2.2 Common Services Network

The example implementation includes the following common services components:

- Active Directory
- OpenLDAP directory
- SharePoint servers

A typical enterprise includes other shared services, such as email servers. We did not include these in the architecture because they are not needed to demonstrate the effectiveness of the ARM example implementation. Table 5-1 and Figure 5-5 identify the specific vendor products we used in this network.

Figure 5-5 Common Services Network



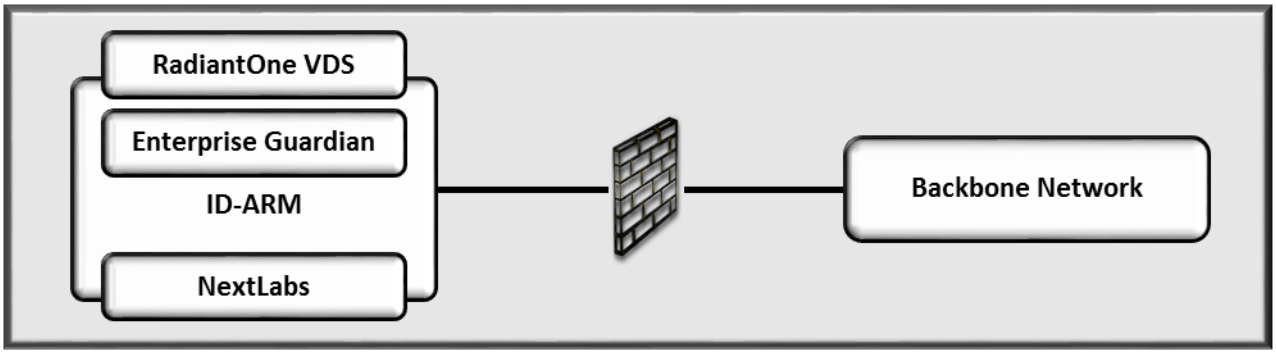
5.2.3 Access Rights Management Network

The following products were installed on the ARM network

- AlertEnterprise Enterprise Guardian ARM system
- Radiant Logic RadiantOne Virtual Directory
- NextLabs Entitlement Management

We separated the ARM systems to highlight the unique ARM components proposed to address the use case. We do not recommend separating ARM functions on their own network. Organizations need to determine the most appropriate implementation of an ARM product within their own infrastructure. Table 5-1 and Figure 5-6 identify the products used in this example implementation.

733 **Figure 5-6 ID-ARM Network**



734

735 AE Enterprise Guardian provides the workflow management capability. The ARM example
736 implementation takes over control of the directories in the company. An important aspect of the
737 implementation is that the control is implemented by assigning an administrative account credential for
738 each managed directory to the ARM system. When the administrative credential is issued, the company
739 must limit access to the managed directories to administrative users with a PAM system. The security of
740 the solution partially depends on limited access to the managed directories, as discussed in Section 6.

741 In this example implementation, the central ARM system uses LDAPS to access and update directories.
742 This encrypted data-in-transit version of LDAP prevents network sniffers from recording the provisioned
743 changes. In addition, Radiant Logic's virtual directory product synchronizes with the directories using the
744 same LDAPS protocol.

745 The Radiant Logic RadiantOne product provides a Virtual Directory capability. In the solution, this
746 product provides two functions: virtual directory for NextLab's use and directory caching for security
747 monitoring. This synchronization is set up to identify and record, at pre-defined intervals, changes within
748 each directory. Radiant Logic reports all changes via logs to the Security Monitoring System.

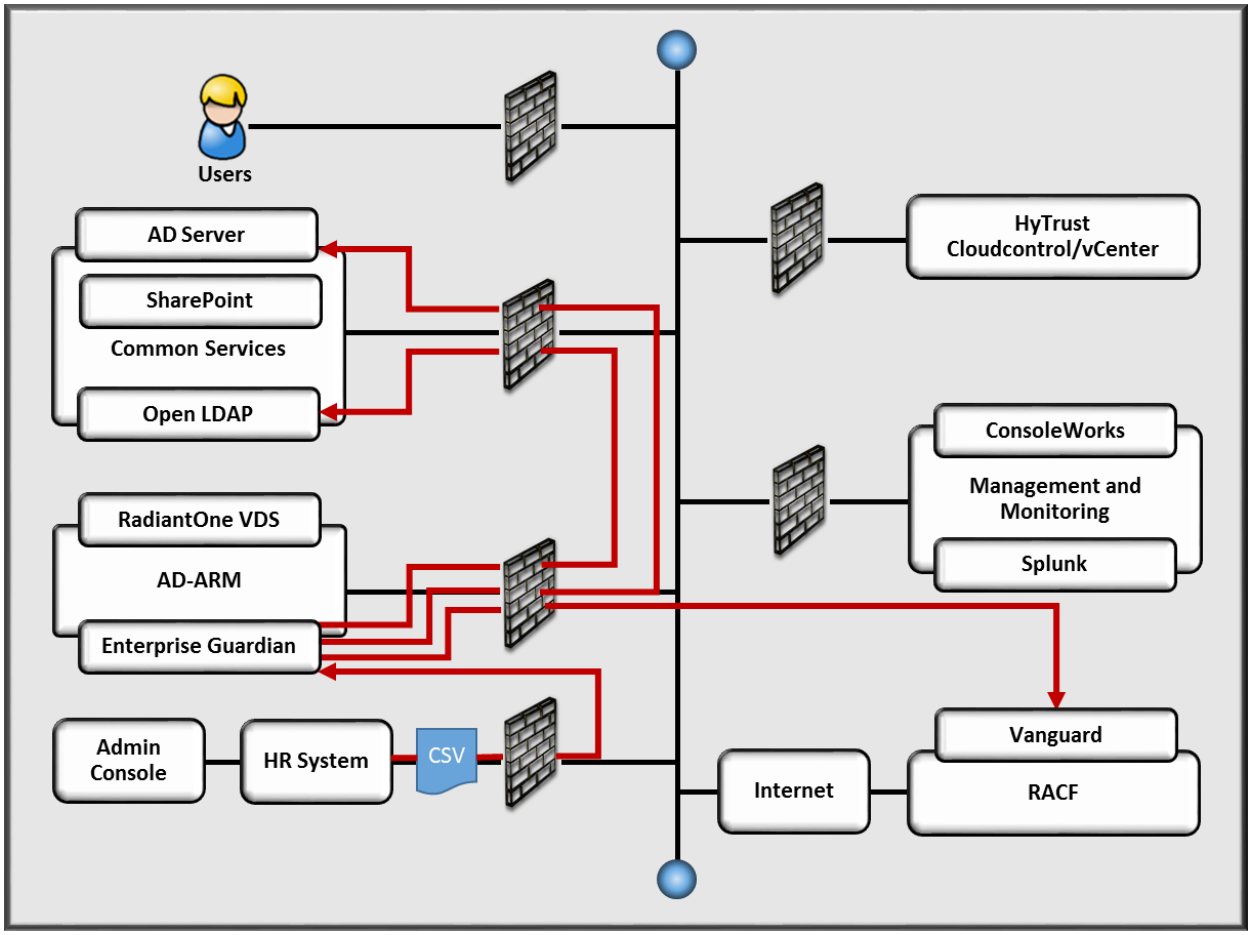
749 The NextLabs Entitlement Management product provides the attribute-based access control capability
750 for an instance of SharePoint. The NextLabs product provides the policy decisions for SharePoint when
751 determining access rights for any user attempting to log in to a SharePoint site. This functionality is used
752 in the demonstration of the example implementation.

753 5.2.4 Network Data Flows

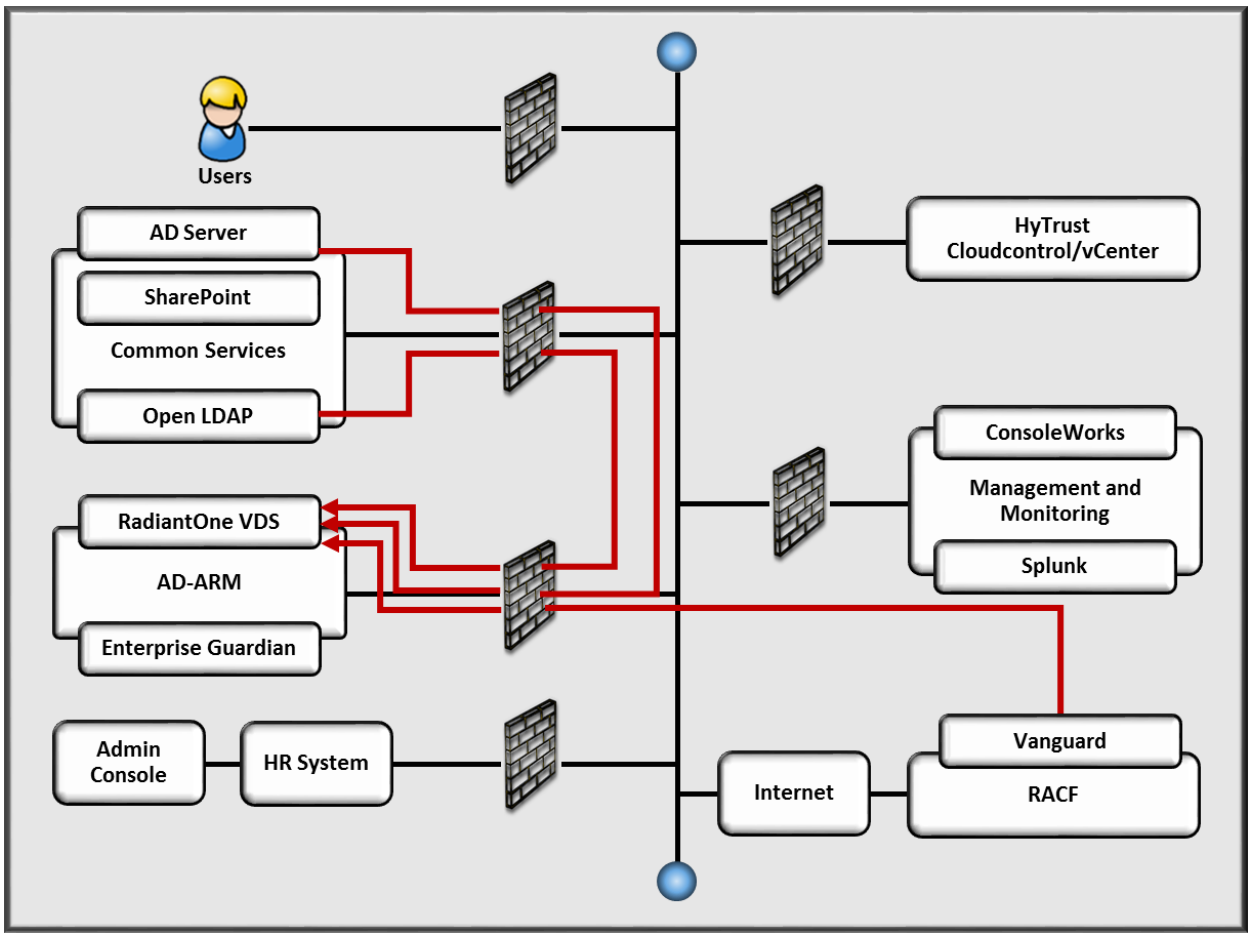
754 This section describes the data flows within the networks implemented in the example implementation.
755 Figures 5-7 and 5-8 depict data flows using red lines with arrows indicating the flow direction
756 superimposed on network diagrams. The steps are described in Section 5.1. Figure 5-7 depicts the flow
757 of user access information from the HR system to the Policy Administration and Provisioning systems
758 and into the directories. Figure 5-8 depicts the flow of user access information from the directories to

the VDS. Note that all data is routed among the ARM and shared services systems through the backbone network. The data-in-transit is protected using LDAPS.

Figure 5-7 User Access Information Network Data Flow (Steps 1 and 2 in Figure 5-2)



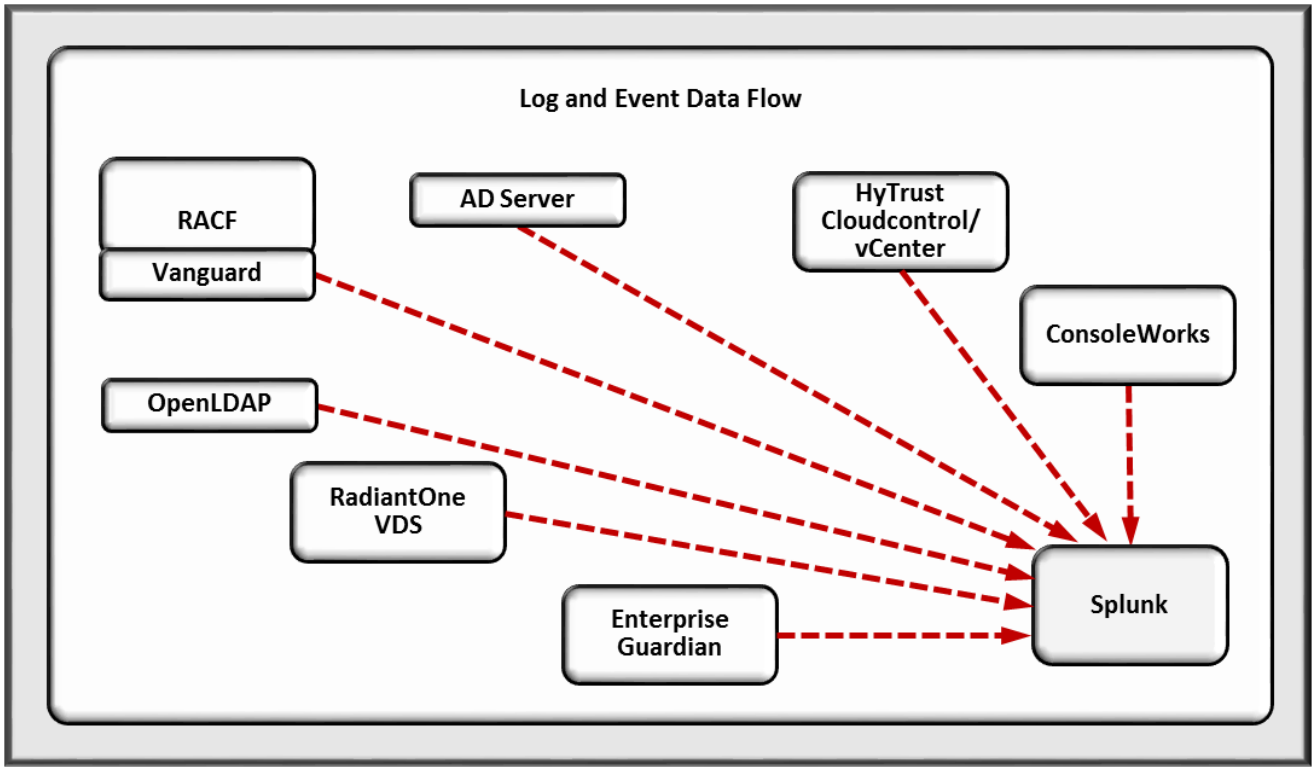
763 **Figure 5-8 User Access Information Network Data Flow (Step 3 in Figure 5-2)**



764

765 The system monitoring data (log and event data) flow occurs between each system and the security
766 monitoring system. Figure 5-9 depicts the data flows. All monitoring and management data are sent via
767 a separate management network segregated from the Backbone (production) network.

768 **Figure 5-9 Monitoring Network Data Flow**



769

770 *Note:* The red dashed lines depict data flows with arrows indicating the flow direction. The data-in-
771 transit is protected by encryption.

772 5.3 Data

773 The example implementation requires user dataset files (HR files) in a format similar to that typically
774 provided by human resource systems. Initially, we populated the HR file with user data from a synthetic
775 dataset designed to mirror a typical HR system dataset. We used a .csv file, which is a typical HR system
776 export file type. The data included user names, titles, access assignments, unique identifiers, and other
777 details required to complete valid directory entries. Each directory was pre-configured with the group
778 and attribute fields needed to support the example implementation. The details are included in NIST SP
779 1800-9C: *How-To Guide.*

6 Security Analysis

We organized the security analysis of the ARM reference design into three parts.

- Section 6.4, Analysis of the Reference Design's Support for CSF Subcategories, analyzes the reference design in terms of the specific subcategories of the CSF that it supports. It identifies the security benefits of each of the reference design capabilities and discusses how the reference design supports specific cybersecurity activities, as specified in terms of CSF subcategories.
- Section 6.5, Analysis of the Security of the Reference Design, reviews vulnerabilities and attack vectors that the reference design might introduce, as well as ways to mitigate them.
- Section 6.6, Security Evaluation Summary, highlights the results of the security assessment and the recommendations from Sections 6.4 and 6.5.

6.1 Assumptions and Limitations

The security evaluation has the following limitations:

- It is not a comprehensive test of all security capabilities, nor is it a red team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

6.2 Build Testing

The purpose of the security analysis is to understand the extent to which the example solution meets its objective of demonstrating access rights management functionality as defined in Section 3.2. In addition, it seeks to understand the security benefits and drawbacks of the reference design.

6.3 Scenarios and Findings

As we performed our security analysis, we assessed how well the reference design addresses the CSF subcategories it was intended to support. We used the CSF subcategories to structure the security assessment by consulting the specific sections of each standard cited for that subcategory. The cited sections describe the functions and controls the example implementation would be expected to include and perform. Using the CSF subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security functions and controls.

6.4 Analysis of the Reference Design's Support for CSF Subcategories

Table 6-1, ARM Reference Design Capabilities and Supported CSF Subcategories, lists reference design capabilities, their functions, and the addressed subcategories, along with the products that we used to instantiate each capability in the example implementation. The security evaluation does not focus on these specific products but on the CSF subcategories because, in theory, any number of commercially available products could be substituted to provide the CSF support represented by a given reference design capability.

The CSF subcategories column of Table 6-1 lists the CSF subcategories that each capability of the reference design supports. The references provide solution validation points in that they list specific security functions and controls that a solution supporting the desired CSF would include. Using the CSF subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports specific security activities and provides structure to our security analysis. The remainder of this subsection discusses how the reference design supports each of the identified CSF subcategories.

824 **Table 6-1 ARM Reference Design Capabilities and Supported CSF Subcategories**

Capability	Specific Product	Function	CSF Subcategories
Policy Management	AlertEnterprise Enterprise Guardian and NextLabs Entitlement Management	Stores access control policy rules as defined by administrators and delivers these rules to the Policy Administration capability. The access control policy rules define which users, roles, and groups have access to which enterprise resources, while also delivering access policy reports to administrators.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.
Policy Administration	AlertEnterprise Enterprise Guardian and NextLabs Entitlement Management	Manages user access-related attributes (e.g., identities, roles, groups) as specified by input from HR administrators. Combines these user access attributes with the access control policy rules that the Policy Management capability delivers to administer enterprise access policy (i.e., to determine which users, roles, and groups have access to which enterprise resources).	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.
User Access Information Provisioning	AlertEnterprise Enterprise Guardian	Automatically translates the enterprise access policy information that the Policy Administration capability delivers into the corresponding role, attribute, and other parameter values that need to be configured in each individual directory. In this way, the capability automatically provisions to all the directories based on the access information from this single, centralized location. LDAPS is employed to maintain confidentiality and integrity. Also, sends logs of all provisioning activity to the monitoring capability.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.DS-2: Data-in-transit is protected.

Capability	Specific Product	Function	CSF Subcategories
User Access Information Repository (also referred to as Directory)	Active Directory OpenLDAP Vanguard	Authoritative source for enterprise user identifiers and their associated roles and attributes. Organizations typically use several different such directories; the reference design integrates with each. These directories support access control to specific enterprise resources based on the user access (account) information stored in them. Each time a user access attempt is made, one or more of these directories is consulted and its contents are used to determine whether the access request will be granted. The directories also send logs of every change that is made to their user access (account) information contents to the monitoring capability. LDAPS is employed to maintain confidentiality and integrity.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.DS-2: Data-in-transit is protected. DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.
RACF Interface	Vanguard	Interface capability that translates between the RACF system to/from LDAP or LDAPS. The capability enables RACF to interface with both the User Access Information Provisioning capability and the Enterprise-wide Virtual Directory capability using LDAP or LDAPS.	PR.DS-2: Data-in-transit is protected. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.

Capability	Specific Product	Function	CSF Subcategories
Enterprise-wide Virtual Directory	RadiantOne VDS	Virtual Directory containing the aggregation of user access information from each of the several different directories in the reference design. It correlates and disambiguates different user accounts that may exist in various directories to create unique user identities and aggregate all the attributes that each user has in each of the directories. It provides a second, global view of the enterprise's access control information, in addition to the authoritative copy of user access information that is stored across the several different physical directories. It also sends logs of every change that is made to any user access information to the monitoring capability. LDAPS is employed to maintain confidentiality and integrity. Logs are reported to the monitoring capability.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.DS-2: Data-in-transit is protected.

Capability	Specific Product	Function	CSF Subcategories
Security Monitoring and Analytics (also referred to as Monitoring)	Splunk Enterprise	Receives security monitoring logs documenting all changes made to user access control and policy information at the User Access Information Provisioning capability, each of the directories, the Virtual Directory, the Privileged Access Management Capability, and the Virtual Environment Privileged Access Management capability. Performs analytics on the logs to detect potential inconsistencies and anomalies that might signal security concerns.	PR.DS-1: Data-at-rest is protected. PR.DS-2: Data-in-transit is protected. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. DE.AE-5: Incident alert thresholds are established.

Note: Table 6-1 describes only the product capabilities and CSF subcategory support that the reference architecture uses. Many of the products have additional security capabilities that are not listed here.

6.4.1 Supported CSF Subcategories

The reference design was created to identify a set of capabilities and their relationship to provide an ARM solution. The CSF includes functions, categories, and subcategories that define the capabilities and processes needed to implement a cybersecurity program. Within this practice guide, the NCCoE has identified the CSF subcategory capabilities and processes in Table 3-1 that are desirable to implement an ARM solution. Each of the following sections describes how the ARM reference design addresses the CSF subcategories, included in Table 3-1, with technical capabilities. Also included are the CSF subcategory processes from Table 3-1 that are beyond the scope of the ARM solution but are important for organizations to address. Some CSF subcategories are supported by individual capabilities of the reference design; others, by the reference design as a whole. Yet other CSF subcategories are relevant because the reference design is predicated on their being addressed by the enterprise-wide architecture.

6.4.1.1 ID.AM-3: Organizational communication and data flows are mapped

The reference design:

- Defines and identifies all ARM-related organizational communication and data flows.
- Defines each of the directories, as well as the flow of data and connectivity between these directories and other capabilities in the reference design.
- Supports CSF subcategory ID.AM-3 with respect to access control management information.
- Does *not* address organizational communication and data flows for any other types of information because they are unique to each organization.

By adopting the reference design, an organization thereby fulfills its support for CSF subcategory ID.AM-3 with respect to organizational communication and data flows that are related to access control management.

6.4.1.2 ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established

The reference design is predicated on there being a clearly defined set of roles and responsibilities for each user that determines that user's access control information (i.e., the roles, groups, and attributes that apply to that user and that thereby determine what resources he or she is authorized to access and at what level of privilege). The organizational access policy administrators define the roles and responsibilities of the entire workforce and describe these roles and responsibilities in terms of which employees have access to what resources (and at what level). They then populate this information into the Policy Management and Policy Administration capabilities of the reference design so it can automatically provision the user access information directories based on the roles and responsibilities that any given company will have defined for the workforce. Once these roles and responsibilities have

been established and provided to the reference design, the design then serves as the mechanism for enforcing the access control-related aspects of these roles and responsibilities.

The design does not include a capability that audits the user access information within the directories. The NCCoE determined that auditing of directory content was out of scope because the capability is well understood and widely adopted.

6.4.1.3 ID.BE-4: Dependencies and critical functions for delivery of critical services are established

With respect to the delivery of the critical service of access control, the reference design establishes the User Access Information Provisioning capability as a centralized source for managing and provisioning all user access control information, and it recognizes this capability as a new critical asset. It also recognizes the importance of each individual directory for storing authoritative user access information and supporting access control, identifying these directories as part of the critical infrastructure. The VDS and the Monitoring Capability are essential for ensuring the integrity of the information the directories store.

6.4.1.4 PR.AC-1: Identities and credentials are managed for authorized devices and users

Managing identities and credentials for authorized devices and users is inherent in and fundamental to the reference design. The objective of the design is to automate administering and provisioning user access changes throughout the enterprise for access control purposes.

6.4.1.5 PR.AC-3: Remote access is managed

To provide security to the reference design capabilities, the reference design does not permit any users, even privileged ones, to log in to the consoles of any reference design capabilities directly. It forces all console access to be performed via PAM systems for physical and virtual machines. In the reference design, PAM enables remote access to the capabilities, managing and logging privileged access to the consoles of physical reference design capabilities. Privileged access to virtual machines is managed by the Virtual Environment (VE) PAM capability. Section 6.5.3 discusses privileged access further.

6.4.1.6 PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

The main objective of the reference design is to manage access permissions for all enterprise resources and servers in a converged and automated fashion capable of supporting the principles of least privilege and separation of duties. Once corporate access policies have been defined and integrated with the reference design in the form of access policy updates, access information updates, and enterprise business rules/workflows, the reference design automatically and consistently provisions all the enterprise directories with the access information necessary to ensure that the directories enforce corporate access policies.

Access Rules administrators should base corporate access policies on the principles of least privilege and separation of duties. The principle of least privilege, defined as providing the least amount of access (to systems or data) necessary for the user to complete his or her job, and the principle of separation of duties, which restricts the amount of responsibilities held by any one individual, are important security tools. These tools help prevent fraud and abuse by limiting the amount of privilege that individual users have and requiring multiple individuals to collude to accomplish certain goals. The reference design, through its Policy Management, Policy Administration, and User Access Information Provisioning capabilities, ensures that the directories are provisioned based on these enterprise access policies. So, assuming access policies are designed to incorporate the principles of least privilege and separation of duties, the reference design will manage and enforce access permissions according to these principles.

In addition, to ensure the security of the reference design itself, typical enterprise users must not be authorized to create or modify user accounts on any enterprise machines. Nor should they be able to log in to any reference design capabilities. Only privileged users should be permitted to access reference design capabilities and the machines on which reference design capabilities run. Various levels of administrator privileges should be established and managed to administer the reference design capabilities themselves and the physical and virtual infrastructure on which the reference capabilities run. All privileged administrative activity must be performed through the PAM and VE PAM capabilities to ensure that all such activity is logged, with the logs being sent from the PAM and VE PAM to the Monitoring Capability for scrutiny. Still higher levels of administrator privileges must be established to administer the PAM and VE PAM capabilities themselves because PAM and VE PAM administrators have the authority to turn off logging and modify the privileges that administrators of other reference design capabilities have. Section 6.5.3 discusses privileged access management and the hierarchy of privileged users in more detail.

6.4.1.7 PR.DS-1: Data-at-rest is protected

User access information is not encrypted while stored at rest. However, this data is spread across the directories, and these directories are in their own security enclave. The security enclave consists of the physical directories only, without any other reference design capabilities, situated on their own subnetwork that is separated from the rest of the reference design by a firewall. The firewall is configured to permit communications using only the specific ports and protocols that are required.

Furthermore, although this information is not integrity protected while at rest, its integrity is monitored by the Monitoring capability. The Monitoring capability receives logs of user access information changes from the User Access Information Provisioning and VDS capabilities as well as each of the directories. The Monitoring capability correlates and compares the log information it receives from each of the above capabilities to ensure that the information is consistent across all sources. In this way, it is possible to verify that each change made to the directories is the result of a legitimate, corresponding event at the User Access Information Provisioning capability that resulted from input from the Policy Administration capability. If a change is detected to a directory that cannot be correlated with logs

signaling related events at these other capabilities, the Monitoring system generates an alert to signal that this change to the data-at-rest in the directory might be unauthorized. File integrity tools are available to monitor for loss-of-integrity events within systems like directories. These tools are not addressed in the reference design.

6.4.1.8 PR.DS-2: Data-in-transit is protected

LDAPS is used to encrypt user access information while it is in transit between reference design capabilities. In the example implementation, a single application is used to implement the Policy Management, Policy Administration, and User Access Information Provisioning capabilities so that all information flows between these capabilities remain inside the same application and are not transmitted over a network where they would be vulnerable to eavesdropping or tampering. If the reference design were to be built using separate physical components to instantiate the Policy Management, Policy Administration, and User Access Information Provisioning capabilities, messages exchanged among these capabilities would need to be provided with at least data integrity and preferably confidentiality protections. The User Access Information Provisioning capabilities encrypt all logs that they send to the Monitoring Capability. It would thus be very difficult to fake a log from one of these capabilities to the Monitoring capability with the aim of trying to trick the Monitoring capability into thinking that an unauthorized user is permitted to have access. Spoofing such a log would require that an adversary possess the keys used to encrypt the logs.

In the current example implementation (RFC 2830), LDAPS is used to perform read-and-write access to the directories and to the VDS capability, ensuring that user access information sent across a network to these remote capabilities is encrypted.

Also, when log information is sent to the Monitoring capability, it is encrypted using the Splunk connector application, resulting in protection from disclosure as well as unauthorized modification.

6.4.1.9 PR.DS-5: Protections against data leaks are implemented

The reference design itself, through its focus on management of access permissions, protects the enterprise in general against data leaks that might occur were someone to gain unauthorized access to resources on the production network. By preventing unauthorized access to information, the reference design protects against leaks of that information. The reference design, however, is not intended to protect against exfiltration of information by an authorized user; addressing such an insider threat is not within the scope of the guide. The reference design does, however, include some mechanisms to deter data leaks perpetrated by insiders. The fact that data flows within the reference design are encrypted serves to ensure that even if data-in-transit within the reference design were to be exfiltrated, this information would not be in plaintext form. Also, the PAM capability serves to limit which data privileged users can access, thereby limiting what privileged insiders can exfiltrate and copy. For example, administrators may be given access to administration and configuration directories and not to directories that contain sensitive data files. The PAM capability also logs all privileged user access,

ensuring that if a privileged user misuses his or her authority and leaks data, this activity would be recorded in log files.

6.4.1.10 PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Although it does not include an audit solution, the reference design supports auditing by aggregating all access-related log information in one location (the Security Monitoring capability), thereby enabling centralized accountability and tracking of access change activity. Locally, various events are monitored and logged at each reference design capability (see NIST SP 1800-9C: *How-To Guides* for a list of events logged). These logs are sent to the Security Monitoring capability. Security Analysts will typically be authorized to have read-only access to these logs to review and respond to potential security events. Monitoring and analytics tools will also have access to these logs for anomaly and potential security event detection. All system administrators or other privileged users are required to use the PAM system. Therefore, any actions they take, including abuse of their privileged access, will be monitored and logged. These logs will be sent to the Security Monitoring capability. Given that access to the logs in the Security Monitoring capability would enable an adversary to delete or modify logs that document adversarial activity, the ability to delete or modify such logs should, by policy, require the cooperation of multiple individuals.

6.4.1.11 PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

The reference design itself, through its focus on managing access permissions, inherently supports the control of access to all enterprise systems and assets. User access information, combined with access policies, can be configured to enforce the principle of least functionality.

6.4.1.12 PR.PT-4: Communications and control networks are protected

Network perimeter defense tools, including border routers and firewalls, are used in the reference design; the directories are isolated on their own subnetwork, separated from the rest of the reference design by a firewall that is configured to permit only ports and protocols required to store and retrieve user access information.

Similarly, other capabilities of the reference design are isolated on their own subnetworks, as shown in Section 5. For example, the Security Monitoring capability and PAM are isolated on their own subnetwork, the Policy Administration, Policy Management, User Access Information Provisioning, and VDS capabilities are isolated on their own subnetwork, and the VE PAM is isolated on its own subnetwork. Such separation ensures that if an intruder can gain access to one of these subnetworks, the resulting access does not provide the opportunity to eavesdrop on traffic that is being exchanged between reference design capabilities on other networks. Nor can the intruder use a capability on which he or she has gained a foothold in one subnetwork as a platform from which to launch an attack on

capabilities in another subnetwork if such an attack would require the use of ports or protocols that the subnetwork's firewall is configured to block.

A management subnetwork is implemented to segment log and administrator access to capabilities. This segmentation further isolates administrative and log data to reduce the potential of eavesdropping and rogue user access to administration interfaces.

6.4.1.13 DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed

Within the reference design, the directories constitute the authoritative repositories of user access information (accounts). The contents of these directories can be considered the baseline with respect to user access information. If user access (account) is changed in any of the following ways and is therefore inconsistent with the contents of the authoritative baseline (i.e., the contents of all the directories), the Monitoring capability detects this inconsistency and generates an alert:

- via direct manipulation of directory information such as an account change, addition, or deletion/deactivation by an insider or malware
- temporary removal of a directory from its network for offline manipulation
- administrative change mistake by a privileged user via the PAM system

The Security Monitoring capability can detect this inconsistency because every user access information update and every provisioning operation generates a log message that is sent to the Security Monitoring capability. For every valid account update, a consistent set of logs is expected to flow from each capability to the Security Monitoring capability, and the log messages received from all capabilities are checked for consistency.

In addition, when user access updates are made to each directory, these changes are also propagated to the VDS, which also sends logs of these updates to the Monitoring capability. Hence, the Security Monitoring capability also checks to ensure that for each update that is logged at a directory, a corresponding update is logged by the VDS. The VDS functionality increases the effectiveness of a directory monitoring program through synchronization and change reporting. This increase will enable anomalous directory changes to be reported within seconds to minutes, depending on the VDS capability configuration.

This established set of log data flowing from reference design capabilities to the Security Monitoring capability is event-based, meaning that the data flow is initiated by specific activities that, once detected, generate logs (see NIST SP 1800-9C: *How-To Guides* for a list of events logged). The activity at the affected reference design capability must be identified and then reported to the Security Monitoring Capability. If the process that is supposed to detect the activity or generate or transmit the log to the Security Monitoring capability stops working temporarily and then resumes operation, whatever updates have occurred in the interim will not have generated any logs. In particular, if a change is made

to a directory while it is not connected to the network, no log event is generated at the time of the change. If the update was the result of a legitimate provisioning operation, the Monitoring capability detects an inconsistency in the logs received from various capabilities and it generates a false alarm. However, if the update was performed by an adversary who intentionally modified a directory while it was offline, this change to the directory could not generate a log, even though the directory contents would now be inconsistent with the contents of the Provisioning capability and of the VDS. This type of activity would be detected, and an alert noting that the directory connection was lost by the VDS would be sent to the Security Monitoring capability.

Monitoring directory update events is not the same as looking at the actual data in the directories. Log collection and transmission is typically performed as a best-effort process. Log collection agents sometimes go down, and they can be fragile, so there would be some risk inherent in relying solely on reference design capabilities to self-report activities and updates. If a directory update event were to somehow fail to reach the Security Monitoring capability, there would be no way to know that the change was made without looking at the information in the directory.

To mitigate the possibility that the best-effort nature of event-based reporting could be exploited to populate a directory with unauthorized information in this way, the VDS is configured to monitor the connections that it has with each of the directories, thereby ensuring that these connections are up. If any of the directories go offline or if its connection with the VDS goes down for any reason, this event would be signaled to the Security Monitoring capability. In addition, the VDS is configured to cache the directory information that it has stored. Once the cache has been initialized and caching has been turned on, the VDS monitors the user access information for any changes. When it detects a change or a connection being re-established to a directory that had been offline, the VDS compares the access information it has cached with the values present in the directories. If there are any discrepancies, it creates a log of these and sends the log to the Security Monitoring capability, enabling the Security Monitoring capability to detect unauthorized changes to the directories. If the reference design incurs too much of a performance hit because of the VDS cache information volume, a separate server can be set up to store the VDS's view of user access information for comparison with the actual contents of the directories. The reference design should not rely solely on the monitoring and flow of event-based logs to ensure that no unauthorized changes have been made to the directories; regular auditing of actual directory contents is also important to reduce risk and bring additional value.

In many cases, an organization's ARM system could have started out simply using a single directory, but, as a consequence of mergers and acquisitions, other applications, resources, and directories were added. As a result, an organization might not have complete awareness of the extent of any given user's access control authorizations across all appliances. Practically, an organization that deploys the reference design will want to ensure that it converts from the policies that it is enforcing at the time of adoption to the policies that it seeks to enforce. Simply adopting the reference design does not cause an organization to automatically begin enforcing its desired access control policy. The objective of reference design is to ensure the integrity of access changes as updates are applied. How well an

organization enforces the access control policies overall depends on the initial baseline contents of those directories. Certifying that these initial baseline contents are correct is not addressed in the design. Planning for deployment of the design gives an organization the opportunity to go back and audit the access control information in their directories and get a more global, correlated, disambiguated view of the user access roles and attributes that are currently in effect.

Ideally, in an operational deployment of the reference design, a separate system would also be deployed to periodically examine the directory contents to verify that they enforce enterprise policies as intended. Having such a system enables a security analyst to determine when an access control mistake is the result of a breakdown in business process as opposed to being the result of a security breach or technology failure.

6.4.1.14 DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

The Security Monitoring capability aggregates and correlates user access information change event logs from three types of sources:

- User Access Information Provisioning capability
- each of the directories (which, in aggregate, constitute the authoritative/baseline source)
- Virtual Directory capability

If any inconsistencies in the user access data changes across these sources are detected, an alert is generated. The Security Monitoring capability also receives log information from the PAM and the Virtual Environment PAM capabilities and generates an alert if it detects privileged user access attempts that are not consistent with the user access information that it has received from other reference design capabilities.

6.4.1.15 DE.AE-5: Incident alert thresholds are established

The alert thresholds are binary: if the user access information logs that the Security Monitoring capability receives from each of its sources are not consistent with each other, an alert is generated. If the user access information logs received from the various capabilities are consistent with each other, no alert is generated.

6.4.1.16 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events

All activity of privileged users on physical reference design capabilities is monitored and logged by the PAM capability for OSs and applications. Similarly, all activity that virtual machine (VM) Administrators perform on VMs (but not the activity that they perform on the OSs installed on those VMs) is logged by the VE PAM. The administrators of the OSs and applications running on VMs make use of the PAM capability for access. These capabilities log each administrator's activity on either the physical console or the VM and send the logs to the Monitoring capability. They also generate alerts when operations that

are not authorized are attempted. The Security Monitoring capability monitors the alerts generated by these physical and virtual PAM capabilities to detect potential cybersecurity events.

6.5 Security of the Reference Design

The list of reference design capabilities in Table 6-1 focuses on the access control capabilities of the reference design that are needed to enable it to meet its objective of automating the management of user access information (accounts). Table 6-1 does not focus on capabilities needed to manage and secure the reference design. However, the reference design itself must be managed and secured. To this end, this second part of the security evaluation focuses on the security of the reference design.

Measures implemented to protect the reference design from outside attack include:

- isolating certain capabilities on separate subnetworks protected by firewalls
- implementing a management network to isolate log and management traffic from the production (business operations) networks
- securing critical user access information and logs to protect them from unauthorized insertion, modification, or deletion
- logging of all privileged user access activities
- encryption and integrity protection of user access information and logs while this information is in transit between capabilities

Table 6-2, Capabilities for Managing and Securing the ARM Reference Design, describes the security protections each capability provides and lists the corresponding products that were used to instantiate each capability. The security evaluation focuses on the capabilities rather than the products. The NCCoE is not assessing or certifying the security of the products included in the example implementation. We assume that the enterprise already deploys network security capabilities such as firewalls and intrusion detection devices that are configured according to best practices. The focus here is on securing capabilities introduced by the reference design and minimizing their exposure to threats.

1134 **Table 6-2 Capabilities for Managing and Securing the ARM Reference Design**

1135 This table describes only the product capabilities and CSF subcategory support used in the reference architecture. Many of the products have
1136 significant additional security capabilities that are not listed here.)

Capability	Specific Product	Function	CSF Subcategories
Subnetting	N/A	Technique of segmenting the network on which the reference design is deployed so that capabilities on one subnetwork are isolated from capabilities on other subnetworks. If an intruder can gain access to one segment of the network, this technique limits his or her ability to monitor traffic on other segments of the network. For example, the enterprise's production network, on which user access information and decisions are conveyed, is separate from the reference design's monitoring and management subnetwork.	PR.DS-1: Data-at-rest is protected. PR.PT-4: Communications and control networks are protected.
User Access Information Repository Firewall	PFSense	Sits between one or more directories and the rest of the reference design, with one interface connecting to the subnetwork that is dedicated to the directories and a second interface connecting to the rest of the reference design. Monitors all traffic that flows to and from the directories. This firewall is configured to permit only the required ports and protocols (e.g., LDAPS) to be exchanged between the User Access Information Provisioning capability and the directory and between the VDS capability and the directory. Privileged user access to this firewall (i.e., access of all users authorized to change firewall rules) must be managed through the Privileged Access Management capability.	PR.PT-4: Communications and control networks are protected.

Capability	Specific Product	Function	CSF Subcategories
Privileged Access Management	TDi Technologies ConsoleWorks	Manages privileged access to the OSs of all physical reference design capabilities. This is the single portal into which all users with administrator privileges must log in; it defines what systems these administrators are authorized to access based on their role and attributes. It also logs every keystroke that is performed by users with administrator privileges, creating an audit trail of privileged user access to the OSs of the physical systems that are hosting reference design capabilities. Allowed commands can also be identified to further control administrator actions.	PR.AC-3: Remote access is managed. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.
Virtual Environment Privileged Access Management	HyTrust Cloud Control	Manages privileged access to the virtual environment (including machines, switches, and host hardware) that host reference design capabilities. Cloud Control is the single portal into which all users with administrator privileges to virtual environment systems must log in; it defines what VMs these administrators are authorized to access based on the user's role and attributes. It logs activity that administrators perform on VMs, but it does not log operations that are performed on the OSs that are installed on those VMs. These logs create an audit trail of privileged user access in the virtual environment that is hosting the reference design capabilities.	PR.AC-3: Remote access is managed. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.

Capability	Specific Product	Function	CSF Subcategories
Log Integrity	Splunk Forwarder	Forwards log information from each reference design capability to the Monitoring capability. This capability encrypts log files before sending them, thereby providing them with both integrity and confidentiality while in transit. If an alternative product were used to instantiate this capability, it could add a time stamp and hash/integrity seal to each log file instead, thereby providing the file with integrity, but not confidentiality, protections. However, if the hash/integrity seal were to continue to be stored with the log file at the Monitoring capability, it would provide a mechanism to detect unauthorized modifications made to the log file while stored there.	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. PR.DS-2: Data-in-transit is protected.

1137

6.5.1 Securing New Attack Surfaces

The reference design introduces new capabilities into the enterprise, and with any new capability comes the potential for new attack surfaces. Implementation of this reference architecture necessitates securing potential attack surfaces. To safeguard the internal systems covered under the proposed ARM system, the following steps can be taken:

1. ***Points of entry.*** The reference design enables employee access to be enabled, modified, and disabled from a single management system that provisions user access information changes to all directories within the enterprise. To prevent the reference design's converged provisioning capability from being transformed into an advantage for the adversary, the organization must secure logical and physical access to the Policy Management, Policy Administration, and User Access Information Provisioning capabilities, in addition to controlling access to the individual directories themselves.
2. ***Disabling monitoring.*** Consistency between the contents of this virtual directory and each of the individual physical directories is used to determine if any changes were made to the contents of the directories (and therefore unable to send log messages documenting these changes to the Security Monitoring capability). To ensure the reference design's Security Monitoring capability receives the proper log messages from the VDS, prevent unauthorized access to the VDS.
3. ***Sabotaging detection.*** Aggregation of user access information and logs in the Security Monitoring capability provides enormous potential in terms of anomaly detection. To prevent malicious changes to the security logs within the Security Monitoring capability, ensure unauthorized access to its contents is blocked.

6.5.1.1 Securing Access to the Policy Administration Capability

User access information changes are not typically made from within any user accounts on the Policy Administration capability, which could be misused to cause the unauthorized modification of user access information or workflows. Typically, user access information changes are initiated via a bulk update from a human resource system. User access information updates are input via .csv files that the Policy Administration capability receives from the HR system. HR administrators who are authorized to do so create .csv files and feed them into the Policy Administration capability. By policy, workflows, which are essentially business process rules that can be defined to enforce access (and other) policy, should be established to ensure that no single HR administrator can perform updates in isolation. Workflows based on the principles of least privilege and separation of duties should be defined that ensure that before updates are performed, multiple HR administrators and or multiple administrative approvals must be received. It should not be possible to submit a fake, unauthorized .csv file to the Provisioning capability; the Provisioning capability should only accept .csv files from the HR system with appropriate approvals in the context of a defined workflow.

6.5.1.2 Securing Access to the Policy Management Capability

The ability to create and modify user access policies within the Policy Management capability must also be carefully controlled. By policy, workflows should be established to ensure that no single administrator can create or modify policies in isolation. Workflows based on the principles of least privilege and separation of duties should be defined to ensure that before updates are performed, multiple administrators and or multiple administrative approvals must be received. It should not be possible to submit policies that have not been properly vetted and approved in the context of a defined workflow.

6.5.1.3 Securing Access to the User Access Information Provisioning Capability

The User Access Information Provisioning capability initiates provisioning activity on the various directories based on input that is received at the Policy Administration and Policy Management capabilities and that propagates to the User Access Information Provisioning capability. The provisioning capability should not accept direct input from any source other than the Policy Administration capability.

6.5.1.4 Securing Access to the Security Monitoring and Analytics Capability

If an adversary could modify the contents of the Monitoring capability without detection, it is essentially "game over" with respect to the ability of the reference design to monitor all access rights changes. By policy, only security analysts, whose role is to be notified of alerts and examine the logs pertinent to those alerts to determine if there is a genuine security event, should be able to view logs, and the logs should be only accessible via read-only access. Workflows based on the principles of least privilege and separation of duties should be defined to ensure that before any changes to the monitoring analytics are performed, multiple administrators and or multiple administrative approvals are received. It should not be possible to create or modify analytics that have not been properly vetted and approved.

As with other reference design capabilities, both policy and the fact that the Monitoring capability's console password is secured across multiple vaults should help ensure that the only way privileged users can access the Monitoring capability for administration is via the PAM capability. The PAM capability, as has been stated, logs all privileged activity that is performed on the Monitoring capability. However, it sends these logs to the Monitoring capability. If an inside adversary can misuse his or her privileges on the Monitoring capability to compromise that capability, it is likely that he or she can also configure the Monitoring capability to ignore, delete, or modify the logs that it receives from the PAM documenting this nefarious activity. To truly protect the Monitoring capability, it would be necessary to ensure that all PAM logs of activity performed on the Monitoring capability are sent to a separate "monitor of monitors" capability, rather than to the Monitoring capability. Such protection against privileged access management abuse is important, but it is not addressed in the reference design.

6.5.2 Ensuring Information Integrity

As mentioned earlier, access to each reference design capability must be secured to prevent unauthorized modification or deletion of access policies, user access information, and analytics information that is stored in these capabilities. In addition to preventing access to this information while it is stored in these capabilities, the information must be protected from modification while it is in transit between reference design capabilities. If user access or policy information were to be deleted, modified, or falsified while in transit between capabilities, the result would be a loss of confidence in the access authorization and authentication of users. It is essential that the user access and policy information have at least its integrity and ideally its confidentiality protected when in transit between capabilities. Securing communications among all capabilities is essential to securing the reference design. To provide this protection, all information sent to and from directories and the VDS is encrypted using the transport layer security (TLS) protocol.

All logs sent within the reference design are encrypted in transit to ensure the confidentiality and integrity of the log information while it is in transit from the reference design capability that is the source of the log to the Monitoring capability. Once the log file is transmitted to the Monitoring capability, it is stored in the clear (i.e., in plaintext form), where it would be vulnerable to modification or deletion if an adversary were somehow able to gain unauthorized access to the Monitoring capability.

6.5.3 Privileged Access Management

Ideally, as a basic security principle, the privileged user access information that is consulted to manage access to the reference design (i.e., to manage privileged access to reference design capabilities and the information they contain) should not be provisioned, stored, or managed by the reference design itself. Access information for privileged users should be managed by a system separate from the reference design, and all privileged access should be monitored and logged for auditing and accountability purposes. The responsibilities of controlling access to reference design capabilities and monitoring and logging privileged actions performed on these capabilities fall under the discipline of PAM.

6.5.3.1 Privileged Users

The access rules defined within the reference design should incorporate the principles of least privilege and separation of duties. Users should be given the authority to access only those resources that they need to access to fulfill their duties, and nothing more. As a result, unprivileged users can log in to their desktops and access specific resources on the production network that they need to do their jobs, but they are not authorized to log in to any of the capabilities in the reference design.

We would expect any organization that adopts the reference design to have several classes of privileged users who are authorized to access reference design capabilities or the machines on which they are running for the purposes of administering those capabilities and machines.

6.5.3.2 Insider Threat

The reference design securely provisions and stores user access information for unprivileged users, thereby ensuring that if an adversary gains insider access to the organization as an unprivileged user, the damage that he will be able to do will be restricted to only those resources to which his role gives him access and limited by what he is authorized to do with those resources. As an unprivileged employee, he will not have access to reference design capabilities or to the information stored on them, so the reference design itself should be secure from an unprivileged insider threat. The extent to which the reference design is protected against a privileged insider threat, however, depends on the privileged access management solution with which the reference design is integrated. Although comprehensive mitigation of the privileged insider threat is important, privileged access management is not addressed in this document.

6.5.3.3 Privileged User Access Information Storage

As mentioned earlier, the reference design includes PAM mechanisms for demonstration purposes, but these mechanisms are not intended to provide a comprehensive PAM solution. In particular, as one shortcut, the reference design stores the user access information that is consulted to determine who has privileged access to the PAM in the reference design itself (i.e., in the AD directory), rather than in a separate system for privileged user access information. This means that when a user logs in to the PAM capability, for example, the AD directory is consulted to determine if that user should be granted access and what privileges he or she should have. So, it is the contents of the AD that determine whether a user should have access to the PAM capability, but it is the PAM capability that determines whether a user should have the privilege to modify the content of the AD. As a result of this cyclical dependency, the Console Administrator for the AD directory could, in theory, log in to the console of the machine hosting the AD directory and add the necessary account and attribute information required to give himself PAM privileges that would enable him to access to all reference design machines via the PAM. It should be noted that the reference solution would detect these particular attacks because the Monitoring capability would generate an alert when it receives logs indicating that AD directory modifications occurred, when it does not receive corresponding logs from other reference design capabilities. In addition, policy and workflow precautions, such as requiring multiple parties to agree to changes to privileged accounts, could be implemented to try to mitigate the threat of such privilege escalation attacks. Solving these types of insider threats in general is beyond the scope of the reference design. However, they demonstrate the importance of integrating the reference design with a comprehensive PAM solution.

6.5.4 Isolating Reference Design Capabilities from Each Other

As mentioned earlier, each of the following sets of reference design capabilities is situated on its own separate subnetwork to isolate these capabilities from each other:

- Policy Administration, Policy Management, User Access Information Provisioning, and Virtual Directory capabilities
- Security Monitoring and Analytics capability and Privileged Access Management capability
- Virtual Environment Privileged Access Management capability
- Directories

Each of the reference design subnetworks is also isolated, via subnetting, from the enterprise's production network (backbone network).

Each subnetwork is separated from the rest of the reference design by a firewall that is configured to restrict the type of data that flow into and out of the subnetwork to the minimum set of necessary protocols. The ports and protocols to which each firewall restricts access are documented in NIST SP 1800-9C: *How-To Guides*.

6.5.4.1 Addressing Attacks

We used the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) model and framework developed by The MITRE Corporation to identify the following adversary tactics and techniques that the reference design protects against:

- Privilege escalation results when an adversary obtains a higher level of permissions on a system or network than he is authorized to have.
  - An adversary employing the tactic of privilege escalation might use the technique of trying to modify his user access information attributes that are stored in the enterprise directories so that these attributes permit him to have more access authority than he is entitled.

    The reference design protects against privilege escalation through its use of logging and monitoring, which enables it to detect unauthorized changes in user attribute information.
  - Alternatively, an adversary attempting to achieve privilege escalation could use the technique of creating an account for a new (nonexistent) user in one of the enterprise's directories and giving that new user the desired higher level of privileges.

    If such an account is created in a directory directly rather than being provisioned via the Policy Administration and Provisioning capabilities, the Security Monitoring capability is designed to detect that the account was not created using the converged provisioning system and generate an alert.
- Credential access results when an adversary obtains access to enterprise resources that he is not authorized to access. An adversary employing the tactic of credential access could use the technique of trying to obtain legitimate user credentials that belong to another user by eavesdropping on these credentials as they are sent to and from directories in the network.

The reference design protects against credential access through its use of LDAPS (secure socket layer-based encrypted traffic between LDAP servers and clients), which prevents the network from sniffing another user's credentials.

6.5.5 Deployment Recommendations

When deploying the reference design in an operational environment, organizations should follow security best practices to address potential vulnerabilities and ensure that all assumptions on which the solution relies are valid to minimize any risk to the production network. Organizations leveraging the reference design should adhere to the following list of recommended best practices that are designed to reduce risk. Note that the laboratory instantiation of the reference design did not implement every security recommendation. They should not, however, consider this list to be comprehensive; merely following this list will not guarantee a secure environment. Planning for deployment of the design gives an organization the opportunity to go back and audit the access control information in their directories and get a more global, correlated, disambiguated, view of the user access roles and attributes that are currently in effect.

6.5.5.1 Patch, Harden, Scan, and Test [5]

- Keep OSs up to date by patching, version control, and monitoring indicators of compromise (e.g., performing virus and malware detection as well as keeping anti-virus signatures up to date).
- Harden all capabilities: all capabilities should be deployed on securely configured OSs that use long and complex passwords and are configured according to best practices.
- Scan OSs for vulnerabilities.
- Test individual capabilities to ensure that they provide the expected CSF subcategory support and that they do not introduce unintended vulnerabilities.
- Evaluate reference design implementations before going operational with them.

6.5.5.2 Other Security Best Practices [6]

- Install, configure, and use each capability of the reference design according to the capability vendor's security guidance.
- Change the default password when installing software.
- Identify and understand which pre-defined administrative and other accounts each capability comes with by default to eliminate any inadvertent back doors into these capabilities. Disable all unnecessary pre-defined accounts and, even though they are disabled, change their default passwords (just in case some future patch to the capability enables these accounts).

- Segregate reference design capabilities onto their own subnetwork, separate from the production network, either physically or by using virtual private networks and port-based authentication or similar mechanisms.
- Protect the various reference design subnetworks from each other and from the production network using security capabilities such as firewalls and intrusion detection devices that are configured according to best practices.
- Configure firewalls to limit connections between the reference design network and the production network, except for connections needed to support required internetwork communications to specific IP address and port combinations in certain directions.
- Configure and verify firewall configurations to ensure that data transmission to and from reference design capabilities is limited to only those interactions that are needed. All communications that are permitted should be restricted to specific protocols and IP address and port combinations in specific directions.
- Monitor the firewalls that separate the various reference design subnetworks from one another.
- NIST SP 1800-9C: *How-To Guides* contain the firewall configurations that show the rules that were implemented in each of the firewalls for the example implementation. These configurations are provided to enable the reader to reproduce the traffic filtering/blocking that was achieved in the implementation.
- Apply encryption or integrity-checking mechanisms to all information exchanged between reference design capabilities (i.e., to all user access, policy, and log information exchanged) so that tampering can be detected. Use only encryption and integrity mechanisms that conform to most recent industry best practices. Note that in the case of directory reads and writes, protected mode is defined as the use of LDAPS (RFC 2830).
- Strictly control physical access to both the reference design and the production network.
- Deploy a separate, complete system for PAM.
- Deploy a configuration management system to serve as a "monitor of monitors" to ensure that if any changes are made to the list of information logged and reported to the Monitoring Capability or to the analytics in the Monitoring Capability, notifications will be generated. Such a system could also serve to monitor whether reference design Monitoring capabilities such as log integrity capabilities or the Monitoring Capability itself go offline or stop functioning and generate alerts when these capabilities become unresponsive.
- Deploy a system that audits and analyzes directory contents to create a description of who has access to what resources and validate that these access permissions correctly implement the enterprise's intended business process and access policies.

6.5.5.3 Policy Recommendations

- Define the access policies to enforce the principles of least privilege and separation of duties.

- Equip the Monitoring capability with as complete a set of rules as possible to take full advantage of the ability to identify anomalous situations that can signal a cyber event. Define enterprise-level workflows that include business and security rules to determine each user's access control authorizations and ensure that enterprise access control policy is enforced as completely and accurately as possible.
- Develop an attack model to help determine the types of things that should generate alerts.
- Grant only a very few users (e.g., human resource administrators) the authority to modify (initiate, change, or delete) employee access information. Require the approval of more than one individual to be received to initiate employee access information updates. Log all employee access information modifications that are made. Define workflows to enforce these requirements.
- Grant only a very few users (e.g., access rules administrators) the authority to modify (initiate, change, or delete) access rules. Require the approval of more than one individual to be received to initiate access rule updates. Log all access rule modifications that are made. Define workflows to enforce these requirements.
- Grant only a very few users (e.g., security analyst) the authority to modify (initiate, change, or delete) the analytics that are applied to log information by the Monitoring capability to determine what constitutes an anomaly and generates an alert. Any changes made to the analytics should, by policy, require the approval of more than one individual, and these changes should themselves be logged, with the logs sent to a monitor-of-monitors system other than the Monitoring Capability and to all security analysts and other designated individuals. Define workflows to enforce these requirements.

6.5.5.4 Privileged Access Recommendations [7]

- Deploy a separate, complete system for privileged access management.
- Limit the number of privileged accounts on reference design capabilities to one or two specific console administrators (if the capability is on a physical machine) or virtual administrators (if the capability is virtual) and a backup administrator account. Limit the number of persons who serve as console administrator for more than one capability.
- Require all users logging in to any reference design capability to do so via the PAM (to ensure that all privileged user activity is logged and that these logs will be sent to the Monitoring capability). Forbid all reference design capabilities from having their consoles accessed directly in a way that bypasses the PAM.
- Ensure that any administrative changes to the PAM (i.e., the creation of any new privileged user accounts, the modification of privileges in privileged user accounts, or a change to the list of PAM activity that is logged) require, by policy, the approval of more than two individuals. Also, ensure that all administrative changes to the PAM are logged and will generate notifications.

- Require the PAM and VE PAM consoles to be accessed in person rather than permitting them to be accessed remotely.
- Configure the PAM to have an always-on connection to all devices in the reference design so that it can monitor each device's console port. This configuration ensures that all activity performed over the console port will be logged for monitoring and audit purposes. Configure the PAM such that if it's always-on connection to any device is disconnected, an alert is generated. This configuration ensures that security auditors can be aware of any times during which the console port of a device might have been accessed without the activity being logged or monitored.

6.6 Security Evaluation Summary

The security benefits of the reference design include:

- converged management of user access information and policy
- user access information provisioning that is governed by documented and repeatable business processes (workflows)
- rapid provisioning and de-provisioning using consistent, efficient, and automated processes
- centralized log storage to support the ability to apply monitoring and analytics across capabilities to detect potential security events, as well as to easily track and audit all user access information and policy changes, provisioning requests, and directory modifications.

These convergence, automation, and monitoring capabilities increase the security of organizations that adopt the reference design.

Automation of the administration and provisioning of user access information enables efficient, quick, and consistent enforcement of the principles of least privilege and separation of duties with respect to the access authority granted to each enterprise user. By performing administration and provisioning automatically, the reference design eliminates the need for individuals or groups of system administrators to manually modify, monitor, or audit the content of each of the enterprise's directories. Such automation improves security by reducing the possibility of human error being introduced during these processes. It ensures that when users are added or removed, or their responsibilities and the things they are authorized to do change, the modifications that need to be made to the user access information that determines what systems they have access to, when they have access to them, and what they can do on those systems can be provisioned from a single, converged location that automatically propagates these changes to all directories throughout the enterprise. These access information changes can be provisioned accurately and consistently throughout the enterprise instantaneously, ensuring that each employee's access permissions are synchronized across all enterprise directories. These capabilities help to reduce the so-called privilege creep that sometimes occurs as a user's role changes, and he or she is given access to additional systems without necessarily having his or her previous access privileges reduced or modified accordingly. Privilege creep can create

opportunities for insider threat attacks. These capabilities also help to reduce the possibility that a user's access permissions become inconsistent across directories.

The reference design also automatically monitors changes to the content of each directory and supports an audit system by sending logs from all reference design capability to a single location (the Monitoring capability). Consolidation of logs from all reference design capabilities at the Monitoring capability enables the reference design to correlate the logs of updates made to each enterprise directory with logs from the policy administration and provisioning capabilities and from the VDS in a way that is not possible when the logs generated by these capabilities are not consolidated at a single location. This consolidation enables the reference design to ensure that access information updates that are made to the enterprise's directories are in fact the result of personnel status information modifications input by HR, defined and approved according to business workflow rules and access policy, and provisioned via the reference design.

Use of the Monitoring capability has the potential to help eliminate access policy inconsistencies that could result from human error, as well as to detect security incidents that may be the result of a deliberate attack. Log consolidation, combined with the ability to monitor and apply analytics to the logs generated by all reference design capabilities, makes it possible for the reference design to automatically detect anomalous situations that can indicate a security breach that would be more difficult, if not impossible, to detect at any single user access information directory being considered in isolation. In addition, although it does not include an audit solution, the reference design enables access-related audits to be performed easily and efficiently by aggregating all log information in the Monitoring capability.

As with any solution, the reference design introduces new capabilities to the enterprise, and with any new capabilities come new threat surfaces. However, these threats can be mitigated using mechanisms designed to secure access to the new capabilities and to the user access information and logs that they exchange and store. In addition, the reference design's security monitoring and analytics capability also helps mitigate threats by systematically subjecting the logs from all reference design capabilities to anomaly detection analytics that ensure the authenticity of all directory entries and updates.

7 Functional Evaluation

We conducted a functional evaluation of the ARM example implementation, as implemented in our laboratory, to verify that it worked as expected. The evaluation verified that the example implementation could perform the following functions:

- Assign and provision access information to directories based on a set of organizational access policy rules.
- Create, modify, and deactivate/delete users in directories.
- Detect changes to user access information within directories.
- Generate a security alert when it detected anomalous activity—specifically, when it detected changes to any directory without also receiving logs corresponding to these changes from all other expected ARM capabilities.

Section 7.1 describes the format and components of the functional test cases. Each functional test case is designed to assess the capability of the example implementation to perform the functions listed above and detailed in the ARM use case requirements in Section 7.2. SharePoint is used for demonstration and testing purposes to simulate application and data resources for which access is managed. Access is controlled via attributes and group membership information stored in the directories.

7.1 ARM Functional Test Plan

This test plan includes the test cases necessary to conduct the functional evaluation of the ARM example implementation. The ARM example implementation is currently deployed in a lab at the NCCoE. The implementation tested is described in Section 5.

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 7-1 provides a template of a test case, including a description of each field in the test case

1502 **Table 7-1 Test Case Fields**

Test Case Field	Description
Parent requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
Associated Security Controls	The NIST SP 800-53 Rev. 4 controls addressed by the test case.
Description	Describes the objective of the test case.
Associated test cases	In some instances, a test case may be based on the outcome of another test case(s). For example, analysis-based test cases produce a result that is verifiable through various means (e.g., log entries, reports, and alerts).
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected results	The expected results for each variation in the test procedure.
Actual results	The observed results.
Overall result	The overall result of the test as pass/fail. In some test case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

1503 ## 7.2 ARM Use Case Requirements

1504 Table 7.2 identifies the ARM functional evaluation requirements that are addressed in this test plan and
1505 their associated test cases. The teller application access attribute is held in the OpenLDAP directory and
1506 the loan application access attribute is held in Active Directory. These applications will be referenced
1507 throughout the test plans to verify directory modifications. The NCCoE does not have a mainframe
1508 application that can be used for testing. Therefore, verification of RACF changes will be done manually
1509 through inspection of the directory contents.

1510 **Table 7-2 ARM Functional Requirements**

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 1	The ARM example implementation shall include an ARM workflow capability that can create users with policy-driven attributes and group memberships in the following directories:			
CR 1.a		Active Directory		ARM-1
CR 1.b		OpenLDAP		ARM-1
CR 1.c		RACF (via Vanguard)		ARM-1
CR 2	The ARM example implementation shall include an ARM workflow capability that can deactivate users in the following directories:			
CR 2.a		Active Directory		ARM-2
CR 2.b		OpenLDAP		ARM-2
CR 2.c		RACF (via Vanguard)		ARM-2
CR 3	The ARM example implementation shall include a workflow capability that can change an existing user's attributes and group memberships in the following directories:			
CR 3.a		Active Directory		ARM-3
CR 3.b		OpenLDAP		ARM-3
CR 3.c		RACF (via Vanguard)		ARM-3

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 4	The ARM example implementation shall include a security Monitoring capability that can detect changes to user attributes and group memberships in the following:			
CR 4.a		Active Directory (AD) via logs from:		
CR-4.a.1			AD	ARM-4
CR-4.a.2			Radiant Logic	ARM-4
CR-4.a.3			AlertEnterprise	ARM-4
CR 4.b		OpenLDAP via logs from:		
CR-4.b.1			OpenLDAP	ARM-4
CR-4.b.2			Radiant Logic	ARM-4
CR-4.b.3			AlertEnterprise	ARM-4
CR 4.c		RACF via logs from:		
CR-4.c.1			Vanguard	ARM-4
CR-4.c.2			Radiant Logic	ARM-4
CR-4.c.3			AlertEnterprise	ARM-4
CR 5	The ARM example implementation shall include a security Monitoring capability that will generate			

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
	an alert based on pre-defined anomalous (logged) activity for the following use cases:			
CR 5.a		Active Directory user changes with no correlated log received from:		ARM-5
CR-5.a.1			AD	ARM-5
CR-5.a.2			Radiant Logic	ARM-5
CR-5.a.3			AlertEnterprise	ARM-5
CR 5.b		OpenLDAP user changes with no correlated log received from:		
CR-5.b.1			OpenLDAP	ARM-5
CR-5.b.2			Radiant Logic	ARM-5
CR-5.b.3			AlertEnterprise	ARM-5
CR 5.c		RACF (Vanguard) user changes with no correlated log received from:		
CR-5.c.1			RACF (Vanguard)	ARM-5

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR-5.c.2			Radiant Logic	ARM-5
CR-5.c.3			AlertEnterprise	ARM-5

1511

7.3 Test Case: ARM-1

Table 7-3 Test Case ID: ARM-1

Parent requirement	(CR 1) The ARM example implementation shall include an ARM workflow capability that can create users with policy-driven attributes and group memberships in the following directories.
Testable requirement	(CR 1.a) Active Directory, (CR 1.b) OpenLDAP, (CR 1.c) RACF
Description	Show that the ARM example implementation can create users in the various directories with the appropriate access and permissions.
Associated test cases	N/A
Associated CSF Subcategories	PR.AC-1, PR.AC-4
Preconditions	HR representative .csv file is available. ARM example implementation is implemented and operational in the lab environment. Standard and privileged user sets are known to the testers. Privileged users are provisioned directly within the ConsoleWorks and HyTrust applications. A set of directories: AD, OpenLDAP and RACF (Vanguard) are operational.
Procedure	Activate ARM workflow engine and run command to read the HR .csv file. Verify that the AlertEnterprise system successfully processes the data. Query the directories to determine if the users are provisioned to the directories with the correct group memberships and attributes as specified by the .csv file. Query the Vanguard RACF system to verify that users are correctly provisioned as expected from the information included in the HR .csv file. At a workstation on the user network, attempt to log in to the teller application as a user known to have access to the teller application. The teller application control attribute is contained in the OpenLDAP directory. At a workstation on the user network, attempt to log in to the loan application as a user known to have access to the loan application. The loan application control attribute is contained in the AD directory.

	At a workstation on the user network, attempt to log in to the teller application as a user known to not have access to the teller application. At a workstation on the user network, attempt to log in to the loan application as a user known to not have access to the loan application.
Expected Results (pass)	Access Allowed (CR 1.a-c) Users with allowed access can log in to loan and teller demo applications. Access Denied (CR 1.a-c) Users without allowed access are unable to log in to loan and teller demo applications.
Actual Results	(example text) This system functioned appropriately and provided the expected results. Users that are known to not have access were unable to log in to the applications. Users that are known to have access to each application were allowed access.
Overall Result	Pass/Fail (with comments)

1514

7.4 Test Case ARM-2

Table 7-4 Test Case ID: ARM-2

Parent requirement	(CR 2) The ARM example implementation shall include an ARM workflow capability that can deactivate users in the following directories:
Testable requirement	(CR 2.a) Active Directory, (CR 2.b) OpenLDAP, (CR 2.c) RACF
Description	Show that the ARM solution can deactivate users in the appropriate directories.
Associated test cases	n/a
Associated CSF Subcategories	PR.AC-1, PR.AC-4
Preconditions	Successful completion of Test Case ARM-1. Create a new HR dataset that deactivates several users in each directory.
Procedure	Perform Test Case ARM-1 to ensure that user accounts have been created in the directories Read the new HR dataset (described in the pre-conditions) by AlertEnterprise. Verify that the AlertEnterprise system successfully processes the data. Query the directories to determine if the user changes are correctly provisioned to the directories. (deactivated) At a workstation on the user network, attempt to log in to the teller application as a user known to previously have had access to the teller application. (successful attempt in ARM-1). At a workstation on the user network, attempt to log in to the loan application as a user known to previously have had access to the loan application. (successful attempt in ARM-1). Query the Vanguard RACF system to verify the users are correctly deactivated as expected from the information included in the HR .csv file.
Expected Results (pass)	User accounts within the directories are deactivated preventing users from gaining access to resources. (CR 2.a-c)
Actual Results	(CR-2) The ARM example implementation shall include an ARM workflow capability that can deactivate users in the following directories: (CR 2.a) Active Directory: Users that previously had an active account are now in a deactivated account status.

	(CR 2.b) OpenLDAP: Users that previously had an active account are now in a deactivated account status. (CR 2.c) RACF: Users that previously had an active account are now in a deactivated account status.
Overall Result	Pass/Fail (with comments)

1517

7.5 Test Case ARM-3

Table 7-5 Test Case ID: ARM-3

Parent requirement	(CR 3) The ARM example implementation shall include a workflow capability that can change an existing user's attributes and group memberships within the following directories.
Testable requirement	(CR 3.a) Active Directory, (CR 3.b) OpenLDAP, (CR 3.c) RACF
Description	Show that the ARM solution can change user attributes and group memberships within directories.
Associated test cases	CR 1
Associated CSF Subcategories	PR.AC-1, PR.AC-4
Preconditions	Reuse ARM example implementation in the state after ARM-1 is completed. Create a new HR dataset that makes changes to the access permissions to the users in the original dataset. Change allowed to denied and denied to allow for all the users in the dataset.
Procedure	Operate the example implementation to read the new HR file. Choose a set of users with known access and a set of users without access for each of the loan, teller systems, and Vanguard RACF attribute. Use the ARM workflow to deny access for the set of users with known access chosen in 1 above. Use the ARM workflow to allow access for the set of users known to not have access chosen in 1 above. Process the HR dataset with the AlertEnterprise system. Verify that the AlertEnterprise successfully processes the dataset. At a workstation on the user network, attempt to log in to the teller application as a user known (from ARM-1) to have access to the teller application. At a workstation on the user network, attempt to log in to the loan application as a user known (from ARM-1) to have access to the loan application. At a workstation on the user network, attempt to log in to the teller application as a user known (from ARM-1) to not have access to the teller application. At a workstation on the user network, attempt to log in to the loan application as a user known (from ARM-1) to not have access to the loan application.

	Query the Vanguard RACF system to verify the user accesses are correctly changed as expected from the information included in the HR .csv file.
Expected Results (pass)	(CR 3) The ARM example implementation shall include an ARM workflow capability that can change user attributes and group memberships in the following directories: (CR 3.a) Active Directory: Users that had previously had access to the loan application (from ARM-1) no longer have access. Users that had previous not had access to the teller application (from ARM-1) now do have access. (CR 3.b) OpenLDAP: Users that had previously had access to the teller application (from ARM-1) no longer have access. Users that had previous not had access to the loan application (from ARM-1) now do have access. (CR 3.c) RACF: User accesses are changed as expected.
Actual Results	This system functioned appropriately and provided the expected results. (CR 3) The ARM example implementation can change user attributes and group memberships in the following directories: (CR 3.a) Active Directory: Users that had previously had access to the loan application (from ARM-1) no longer have access. Users that had previous not had access to the teller application (from ARM-1) now do have access. (CR 3.b) OpenLDAP: Users that had previously had access to the teller application (from ARM-1) no longer have access. Users that had previous not had access to the loan application (from ARM-1) now have access. (CR 3.c) RACF: User accesses changed as expected.
Overall Result	Pass/Fail (with comments)

1520

7.6 Test Case ARM-4

Table 7-6 Test Case ID: ARM-4

Parent requirement	(CR 4) The ARM example implementation shall include a security monitoring capability that can detect changes to user attributes and group memberships in the following:
Testable requirement	(CR 4.a) Active Directory (CR-4.a.1) AD, (CR-4.a.2) Radiant Logic, (CR-4.a.3) AlertEnterprise (CR 4.b) OpenLDAP (CR-4.b.1) AD, (CR-4.b.2) Radiant Logic, (CR-4.b.3) AlertEnterprise (CR 4.c) RACF (CR-4.c.1) AD, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise
Description	Show that the ARM solution can detect when user changes occur within the directories.
Associated test cases	CR 1
Associated CSF Subcategories	DE.AE-1, DE.AE-3, DE.AE-5
Preconditions	Reuse ARM example implementation in the state after ARM-1 is completed.
Procedure	Process the HR dataset from Test Case 3 (the one that changes user access information in each of the directories). Check the security monitoring system to verify that the changes made are reported via logs from each of these systems for a change that occurs to a user in AD: AD, Radiant Logic, and AlertEnterprise. Check the security monitoring system to verify that the changes made are reported via logs from each of these systems for a change that occurs to a user in OpenLDAP: OpenLDAP, Radiant Logic, and AlertEnterprise. Check the security monitoring system to verify that the changes made are reported via logs from each of these systems for a change that occurs to a user in RACF (Vanguard): RACF (Vanguard), Radiant Logic, and AlertEnterprise.
Expected Results (pass)	(CR 4) The ARM security monitoring system receives and stores the logs indicating changes to the following directories: (CR 4.a) Active Directory from (CR-4.a.1) AD, (CR-4.a.2) Radiant Logic, (CR-4.a.3) AlertEnterprise (CR 4.b) OpenLDAP from (CR-4.b.1) OpenLDAP, (CR-4.b.2) Radiant Logic, (CR-4.b.3) AlertEnterprise

	(CR 4.c) RACF (Vanguard) from (CR-4.c.1) Vanguard, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise
Actual Results	This system functioned appropriately and provided the expected results. (CR 4) The ARM security monitoring system receives and stores the logs indicating changes to the following directories: (CR 4.a) Active Directory from (CR-4.a.1) AD, (CR-4.a.2) Radiant Logic, (CR-4.a.3) AlertEnterprise (CR 4.b) OpenLDAP from (CR-4.b.1) OpenLDAP, (CR-4.b.2) Radiant Logic, (CR-4.b.3) AlertEnterprise (CR 4.c) RACF (Vanguard) from (CR-4.c.1) Vanguard, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise
Overall Result	Pass/Fail (with comments)

1523

7.7 Test Case ARM-5

Table 7-7 Test Case ID: ARM-5

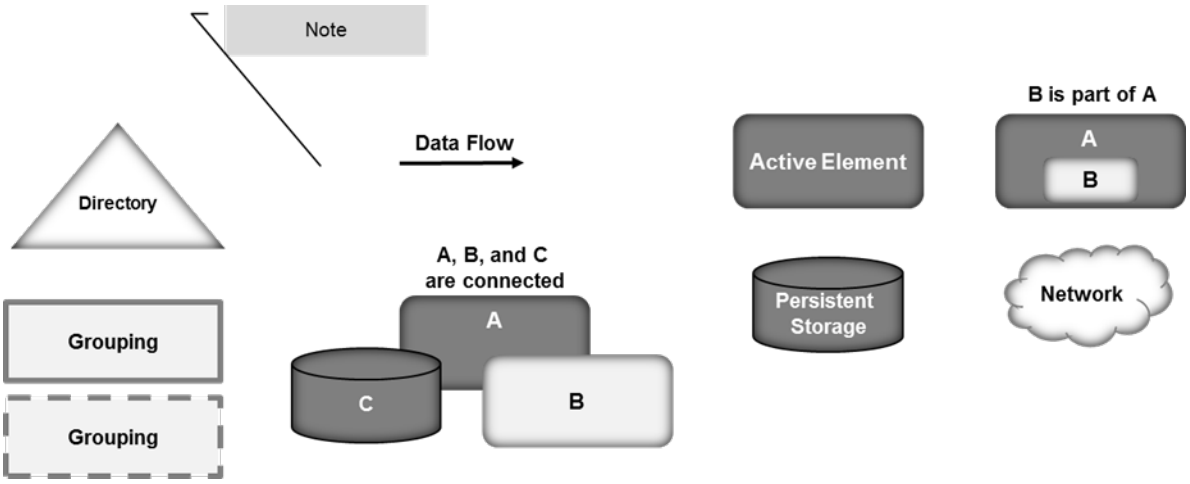
Parent requirement	(CR 5) The ARM example implementation shall include a security monitoring capability that will generate an alert based on pre-defined anomalous (logged) activity for the following use cases:
Testable requirement	(CR 5.a) Active Directory user changes with no correlated log received from: (CR-5.a.1) AD, (CR-5.a.2) Radiant Logic, (CR-5.a.3) AlertEnterprise (CR 5.b) OpenLDAP user changes with no correlated log received from: (CR-5.b.1) OpenLDAP, (CR-5.b.2) Radiant Logic, (CR-5.b.3) AlertEnterprise (CR 5.c) RACF (Vanguard) user changes with no correlated log received from: (CR-5.c.1) RACF (Vanguard), (CR-5.c.2) Radiant Logic, (CR-5.c.3) AlertEnterprise
Description	Show that the ARM example implementation can detect when anomalous user changes occur within the directories.
Associated test cases	CR 1
Associated CSF Subcategories	DE.AE-3, DE.AE-5
Preconditions	Reuse ARM example implementation in the state after ARM-1 is completed.
Procedure	Make a change to each of the directories without the AlertEnterprise provisioning system (anomalous activity) or the privileged account management system. This requires a privileged account on each directory system.
Expected Results (pass)	(CR 5) The ARM example implementation shall include a security monitoring capability that will generate an alert based on pre-defined anomalous (logged) activity for the following use cases: Alert generated for each of the following instances: (CR 5.a) Active Directory user changes with no correlated log received from: (CR-5.a.1) AD, (CR-5.a.2) Radiant Logic, (CR-5.a.3) AlertEnterprise (CR 5.b) OpenLDAP user changes with no correlated log received from: (CR-5.b.1) OpenLDAP, (CR-5.b.2) Radiant Logic, (CR-5.b.3) AlertEnterprise (CR 5.c) RACF (Vanguard) user changes with no correlated log received from: (CR-5.c.1) Vanguard, (CR-5.c.2) Radiant Logic, (CR-5.c.3) AlertEnterprise

Actual Results	This system functioned appropriately and provided the expected results. (CR 5) The ARM example implementation generates an alert based on pre-defined anomalous (logged) activity for the following use cases: Alert were generated for each of the following instances: (CR 5.a) Active Directory user changes with no correlated log received from: (CR-5.a.1) AD, (CR-5.a.2) Radiant Logic, (CR-5.a.3) AlertEnterprise (CR 5.b) OpenLDAP user changes with no correlated log received from: (CR-5.b.1) OpenLDAP, (CR-5.b.2) Radiant Logic, (CR-5.b.3) AlertEnterprise (CR 5.c) RACF (Vanguard) user changes with no correlated log received from: (CR-5.c.1) Vanguard, (CR-5.c.2) Radiant Logic, (CR-5.c.3) AlertEnterprise
Overall Result	Pass/Fail (with comments)

Appendix A List of Acronyms

AD	Active Directory
ARM	Access Rights Management
CAT	Cybersecurity Assessment Tool
CR	Capability Requirement
CSF	Cybersecurity Framework
.csv	Comma-Separated Value
DNS	Domain Name Service
FFIEC	Federal Financial Institutions Examination Council
FS-ISAC	Financial Sector Information Sharing and Analysis Center
HR	Human Resources
ID	Identity
IP	Internet Protocol
LDAPS	Lightweight Directory Access Protocol Secure
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OS	Operating System
PAM	Privileged Account Management
RACF	Resource Access Control Facility
RMF	Risk Management Framework
SIM	Security Information Management
TLS	Transport Layer Security
VE	Virtual Environment
VDS	Virtual Directory System
VLAN	Virtual Local Area Network
VM	Virtual Machine

Appendix B Legend for Diagrams



Appendix C References

[1] J. Saltzer, "Protection and the Control of Information Sharing in Multics," *Communications of the ACM*, 17 (7), 388-402 (1974).

[2] "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology Special Publication 800-53, Rev. 4, April 2013, http://dx.doi.org/10.6028/NIST.SP.800-53r4

[3] "Digital Identity Guidelines," National Institute of Standards and Technology Special Publication 800-63-3, June 2017, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[4] "Assessment of Access Control Systems," National Institute of Standards and Technology, NIST Interagency Report 7316, September 2006, http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[5] "Guide to Enterprise Patch Management Technologies," NIST Special Publication 800-40 Revision 3, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[6] "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology Special Publication 800-53, Rev. 4, April 2013, http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[7] A Report on the Privilege (Access) Management Workshop, National Institute of Standards and Technology Interagency Report 7657, March 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7657.pdf