PROJECT DESCRIPTION

PRIVILEGED ACCOUNT MANAGEMENT

Securing Privileged Accounts for the Financial Services Sector

James Banoczi

National Cybersecurity Center of Excellence

National Institute of Standards and Technology

Harry Perper and Susan Prince

The MITRE Corporation

DRAFT

October 2017

financial_nccoe@nist.gov

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE 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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes a particular problem that is relevant across the financial services sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the financial services sector and vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be used by financial services sector organizations.

Abstract

Privileged Account Management (PAM) is a domain within Identity and Access Management (IdAM) that focuses on monitoring and controlling the use of privileged accounts. Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and service accounts. These powerful accounts provide elevated, often non-restricted access to the underlying IT resources and technology, which is why attackers or malicious insiders seek to gain access to them. Hence, it is critical to monitor, audit, control, and manage privileged account usage. Many organizations, including financial sector companies, face challenges managing privileged accounts. In response to this potential threat, the Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool (CAT) has specified privileged accounts be tightly controlled.

The goal of this project is to demonstrate a PAM capability that effectively protects, monitors, and manages privileged account access to include their life cycle management, authentication, authorization, auditing, and access controls. This project will result in a freely available NIST Cybersecurity Practice Guide which includes a reference design, fully implemented example solution, and a detailed guide of practical steps needed to implement the solution.

Keywords

Access control, auditing, authentication, authorization, life cycle management, multifactor authentication, PAM, Privileged Account Management, provisioning 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.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

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

Public comment period: October 12, 2017 to November 13, 2017

Table of Contents

1 Executive Summary

Purpose

This document describes an NCCoE project focused on securing the use of privileged accounts for which we are seeking public feedback.

The purpose of this project is to provide guidance and demonstrate the secure use and management of privileged accounts also referred to Privileged Account Management (PAM). PAM is the aspect of identity and access management that addresses administrative accounts/users within an organization. Many privileged accounts provide the "keys to the kingdom" for attackers or malicious insiders as these accounts provide elevated, often unrestricted access to corporate resources and critical systems (e.g. "crown jewels"), beyond what a regular user would have. Many successful cyber-attacks have made use of privileged accounts to gain access to information or systems of interest resulting in data breaches. In response to these reported breaches, the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) has prescribed that privileged accounts be tightly controlled.

Many organizations, including financial services companies face challenges managing privileged accounts. These challenges include:

- controlling and monitoring (and auditing) use of these accounts
- ensuring personal accountability among privileged users
- enforcing least privilege and separation of duties policies

This project aims to help organizations in the financial sector design and implement a PAM system that controls access to and monitors privileged accounts, controls what users can do using privileged account access, and manage the lifecycle of privileged accounts.

The publication of this Project Description is the beginning of a process that will identify project collaborators, as well as standards-based, commercially available, and /or open-source hardware and software components. These products will be integrated and implemented in a laboratory environment to build open, standards-based, modular, end-to-end reference designs that will address the security challenges of privileged accounts. The approach may include architectural definition, logical design, build development, security analysis, test and evaluation, security control mapping, and future build considerations. The output of the process will be the publication of a multi-volume NIST Cybersecurity Practice Guide that will help financial sector companies implement stronger controls for privileged account security.

Scope

The scope of the project will include management and control of privileged accounts used to administer the IT infrastructure. The resulting example solution will include implementation of:

- applications, operating systems, database systems, network infrastructure, etc.
- cloud services (XaaS) (software, infrastructure, platform, etc. as a service)
- users with permission to perform transactions that can materially affect an organization's ability to operate (large financial transactions, large security trades, social media accounts, etc.)
- activity logging (textual and video)

- typical administrative users

Assumptions

The example solution of PAM will provide numerous security benefits including the reduction of privileged user access to sensitive information without compromising their ability to perform job tasks. The NCCoE assumes that organizations will perform a risk assessment to determine the risk reduction value of an investment in one or more of the PAM system capabilities included in the reference architecture.

A key assumption is that all potential adopters of this project or any of its components have polices describing the separation of duties and least privilege for administrative/privileged users.

Background

The project was chosen based on discussions with leaders from organizations within financial sector as well financial sector associations regarding the high priority cybersecurity issues they face. The lack of self-protection in the information technology infrastructure (IT) elements (networking systems, applications, and operating systems) forces organizations to limit access to these systems. Accounts (typically called privileged accounts) with access to these systems allow users to make changes (including file or system change, deletion, and creation) that can cause disruption within an organization. The accounts are typically referred to as administrators. Disruption can include, but is not limited to, data destruction, data exfiltration, and system failure. Any of these situations could significantly impact or eliminate the ability of the organization to continue operations. Because of the lack of self-protection within systems, organizations develop policies for separation of duties and least privilege. The policies apply to all users including privileged users. Because of the level of access administrators are trusted with, their access to the information technology infrastructure needs to be monitored and controlled.

Companies also face the following issues with respect to privileged accounts:

- regulatory compliance (monitoring, managing, and auditing activity)
- insider malicious activities
- abuse of rights
- employee mistakes
- securing administrative access to cloud infrastructure
- malware account escalation and account take over
- 3rd party access management

2 SCENARIOS

The following scenarios have been used to developed this project description. They will become the use cases for design of the reference architecture.

Scenario 1: Directory Administrator

From time to time directories need to be updated or modified. For example, a new application account may need to be added to support a new or modified application.

Scenario 2: Web Server Administrator

Web server administrator updating the server OS.

Scenario 3: Network Administrator

Network administrator making changes to a firewall.

Scenario 4: Security Analyst

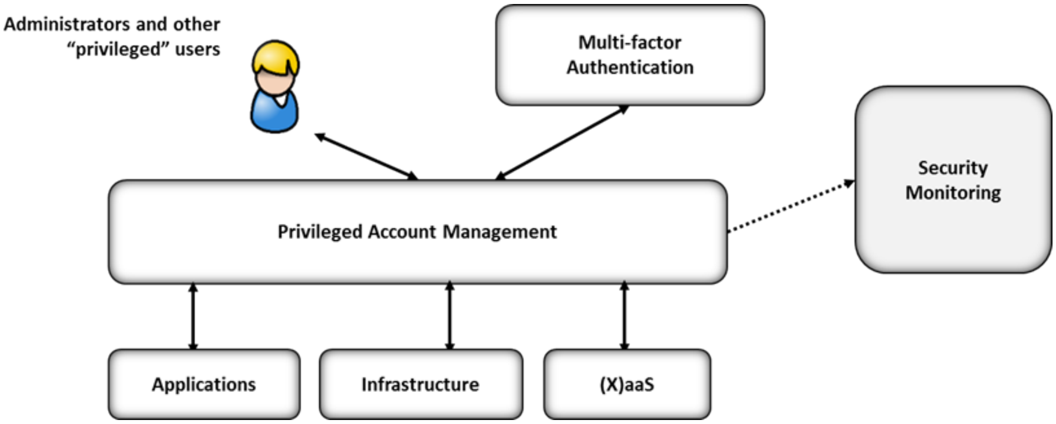
Security analyst accessing system logs as part of a security incident.

Scenario 5: High Impact System Access

Authorized Federal Reserve Discount Window transactions or any other exchange or financial transactions that have the potential for a significant impact to the organization's ability to operate normally. This could also apply to social media account access control.

3 High-Level Architecture

The high-level architecture diagram (below) introduces privileged account management into the information technology infrastructure of an organization between the IT elements and their privileged users (administrators). The reference architecture addresses the scope as noted in section 1 and the desired requirements noted below.


Administrators and other "privileged" users
Multi-factor Authentication
Security Monitoring
Privileged Account Management
Applications
Infrastructure
(X)aaS

Component List

The NCCoE has a lab environment for hosting development of the example solution including the following features:

- network with machines using a directory service
- virtualization servers
- network switches
- remote access solution with Wi-Fi and VPN

Collaboration partners (participating vendors) will need to provide specialized components and capabilities to realize this solution including, but not limited to:

- privileged account control
- privileged account command filtering (allow or deny specific commands, such as disk formatting)

- multifactor authentication capability
- access logging/database system
- password management
- separation of duties management
- support least privileged policies
- password obfuscation (hiding passwords from PAM users)
- temporary accounts
- Log management (analytics, storage, alerting)

Desired Requirements

The security capabilities, behaviors, and life cycle security requirements of the solution are identified in the following list[1]:

- easy to use for both PAM system administrators and PAM system users
- protection for data at rest and data in transit
- complementary to existing access management
- integrates with directories
- account use control (policy enforcement and decision making)
- system command control
- password obfuscation (hidden passwords)
- password management (vaults, changes, storage)
- activity logging (textual and video)
- real time activity monitoring
- support typical user
- privilege escalation management
- forensic investigation data management
- workflow management
- emergency (break glass) scenario support
- policy management
- single sign-on
- system and privileged account discovery

[1] Security Capabilities and Behaviors and Life Cycle Security are two of the major design principles described in the NIST Special Publication 800-130 *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.*

4 Relevant Standards and Guidance

- PCI/DSS version 3.2
  https://www.pcisecuritystandards.org/document_library
  Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT)
  https://www.ffiec.gov/cyberassessmenttool.htm
- NIST 800-53 rev 4
  http://csrc.nist.gov/publications/PubsSPs.html
- ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control
  http://csrc.nist.gov/groups/SNS/rbac/
- RFC 4245 The Secure Shell (SSH) Connection Protocol
  https://www.ietf.org/rfc/rfc4254.txt
- RFC 5246 Transport Layer Security Protocol
  https://tools.ietf.org/html/rfc5246

5 Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), and FFIEC guidance. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Table 1: Security Control Map

			Informative References					
Function	**Category**	**Subcategory**	**FFIEC CAT**	**CCS CSC 2016**	**COBIT 5**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**PCI-DSS 3.0**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-3:** Organizational communication and data flows are mapped	D4.C.Co.B.4 D4.C.Co.Int.1	1	DSS05.02	A.13.2.1	AC-4, CA-3, CA-9, PL-8	1.1, 1.2, 1.3, 2.4
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	D1.R.St.B.1 D1.TC.Cu.B.1		APO01.02, DSS06.03	A.6.1.1	CP-2, PS-7, PM-11	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-4**: Dependencies and critical functions for delivery of critical services are established	D4.C.Co.B.1 D1.G.IT.B.2			A.11.2.2, A.11.2.3, A.12.1.3	CP-8, PE-9, PE-11, PM-8, SA-14	
		ID.BE-5: Resilience requirements to support delivery of critical services are established	D5.IR.Pl.B.5 D5.IR.Pl.E.3		DSS04.02	A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1	CP-2, CP-11, SA-14	

			Informative References						
Function	**Category**	**Subcategory**	**FFIEC CAT**	**CCS CSC 2016**	**COBIT 5**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**PCI-DSS 3.0**
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	D1.G.SP.B.4		APO01.03, EDM01.01, EDM01.02	A.5.1.1	- 1 controls from all families	1.5, 2.1, 2.2, 2.5, 2.6, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 5.1, 5.2, 5.4, 6.7, 7.3, 8.1, 8.8, 9.6, 9.10, 10.7, 10.9, 11.6, 12.1, 12.3, 12.4, 12.5, 12.8
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	D1.G.SP.B.7 D4.RM.Co.B.2 D4.RM.Co.B.5		APO13.12	A.6.1.1, A.7.2.1	PM-1, PS-7	12.4
		ID.GV-4: Governance and risk management processes address cybersecurity risks	D1.G.Ov.B.1 D1.G.Ov.B.3 D1.G.Ov.E.1 D1.G.SP.E.1 D1.G.Ov.Int.1		DSS04.02		PM-9, PM-11	

			Informative References					
Function	**Category**	**Subcategory**	**FFIEC CAT**	**CCS CSC 2016**	**COBIT 5**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**PCI-DSS 3.0**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-6:** Risk responses are identified and prioritized	D5.IR.Pl.B.1 D5.DR.Re.E.1 D5.IR.Pl.E.1		APO12.05, APO13.02		PM-4, PM-9	
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	D3.PC.Im.B.7 D3.PC.Am.B.6	16	DSS05.04, DSS06.03	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-2, IA Family	8.1-8.7
		PR.AC-3: Remote access is managed	D3.PC.Am.B.15 D3.PC.De.E.7 D3.PC.Im.Int.2	12	APO13.01, DSS01.04, DSS05.03	A.6.2.2, A.13.1.1, A.13.2.1	AC-17, AC-19, AC-20	7.1, 7.2
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	3.PC.Am.B.1 D3.PC.Am.B.2 D3.PC.Am.B.5	5, 12, 14, 15, 16		A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	AC-2, AC-3, AC-5, AC-6, AC-16	3.5, 8.1-8.7

			Informative References					
Function	Category	Subcategory	FFIEC CAT	CCS CSC 2016	COBIT 5	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	PCI-DSS 3.0
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	D3.DC.Im.B.1 D3.DC.Im.Int.1	9, 11, 12, 13, 14		A.13.1.1, A.13.1.3, A.13.2.1	AC-4, SC-7	1.4
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	D1.G.IT.B.13 D3.PC.Am.B.14 D4.RM.Co.B.1 D3.PC.Am.A.1	14, 17	APO01.06, BAI02.01, BAI06.01, DSS06.06	A.8.2.3	SC-28	3.3, 3.4, 3.5, 4.1 - 4.3
		PR.DS-2: Data-in-transit is protected	D3.PC.Am.B.13 D3.PC.Am.E.5 D3.PC.Am.Int.7	13, 14, 17	APO01.06, DSS06.06	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8	2.3
		PR.DS-4: Adequate capacity to ensure availability is maintained	D5.IR.Pl.B.5 D5.IR.Pl.B.6 D5.IR.Pl.E.3 D3.PC.Im.E.4		APO13.01	A.12.3.1	AU-4, CP-2, SC-5	

			Informative References					
Function	Category	Subcategory	FFIEC CAT	CCS CSC 2016	COBIT 5	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	PCI-DSS 3.0
		PR.DS-5: Protections against data leaks are implemented	D3.PC.Am.B.15 D3.PC.Am.Int.1 D3.PC.De.Int.1 D3.DC.Ev.Int.1	13, 17	APO01.06	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	1.3
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	D3.CC.Re.Int.5 D3.CC.Re.Int.6		BAI09.03	A.11.1.2, A.11.2.4, A.11.2.5	MA-2, MA-3, MA-5	5.2, 6.2

			Informative References					
Function	Category	Subcategory	FFIEC CAT	CCS CSC 2016	COBIT 5	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	PCI-DSS 3.0
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	D3.PC.Im.B.7	5, 12	DSS05.04	A.11.2.4, A.15.1.1, A.15.2.1	MA-4	6.2
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	D1.G.SP.B.3 D2.MA.Ma.B.1 D2.MA.Ma.B.2	6, 14	APO11.04	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	AU Family	5.2, 6.6, 9.6, 9.7,10.1-10.9

			Informative References					
Function	Category	Subcategory	FFIEC CAT	CCS CSC 2016	COBIT 5	ISO/IEC 27001:2013	NIST SP 800-53 Rev. 4	PCI-DSS 3.0
	policies, procedures, and agreements.	**PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality	D3.PC.Am.B.7 D3.PC.Am.B.4 D3.PC.Am.B.3: D4.RM.Om.Int.1	5, 14, 16	DSS05.02	A.9.1.2	AC-3, CM-7	1.3, 3.5, 7.1, 7.2

			Informative References						
Function	**Category**	**Subcategory**	**FFIEC CAT**	**CCS CSC 2016**	**COBIT 5**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**PCI-DSS 3.0**
		PR.PT-4: Communications and control networks are protected	D3.PC.Im.B.1 D3.PC.Am.B.11 D3.PC.Im.Int.1	7, 11	DSS05.02, APO13.01	A.13.1.1, A.13.2.1	AC-4, AC-17, AC-18, CP-8, SC-7	1.1, 1.2
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	D3.DC.Ev.B.1 D4.C.Co.B.4	9, 12	DSS03.01		AC-4, CA-3, CM-2, SI-4	1.1, 1.2, 11.4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	D5.IR.Pl.Int.4	19		A.16.1.1, A.16.1.4	AU-6, CA-7, IR-4, SI-4	10.4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	D3.DC.Ev.E.1	6			AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	10.1, 10.2, 10.3, 10.4

			Informative References					
Function	**Category**	**Subcategory**	**FFIEC CAT**	**CCS CSC 2016**	**COBIT 5**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**PCI-DSS 3.0**
		DE.AE-5: Incident alert thresholds are established	D5.DR.De.B.1 D3.DC.An.E.4. D3.DC.An.Int.3	19	APO12.06		IR-4, IR-5, IR-8	10.6
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events	D3.DC.An.A.3	19		A.12.4.1	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	10.1, 10.3
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	D3.DC.Ev.B.3	19			AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	5.1, 11.4
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-4:** Event detection information is communicated to appropriate parties	D3.DC.Ev.B.2 D5.ER.Is.B.1 D5.ER.Is.E.1	6	APO12.06	A.16.1.2	AU-6, CA-2, CA-7, RA-5, SI-4	

			Informative References					
Function	**Category**	**Subcategory**	**FFIEC CAT**	**CCS CSC 2016**	**COBIT 5**	**ISO/IEC 27001:2013**	**NIST SP 800-53 Rev. 4**	**PCI-DSS 3.0**
RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-2:** Events are reported consistent with established criteria	D5.IR.Pl.B.2 D5.DR.Re.B.4 D5.ER.Es.B.4	19		A.6.1.3, A.16.1.2	AU-6, IR-6, IR-8	

APPENDIX A – REFERENCES

[1] FFIEC Cybersecurity Assessment Tool (CAT)

[2] FFIEC Information Security Handbook

Appendix B - Acronyms and Abbreviations

CSF	Cybersecurity Framework
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
IdAM	Identity and Access Management
PAM	Privileged account Management
FFIEC	Federal Financial Institutions Examination Council
CAT	Cybersecurity Assessment Tool