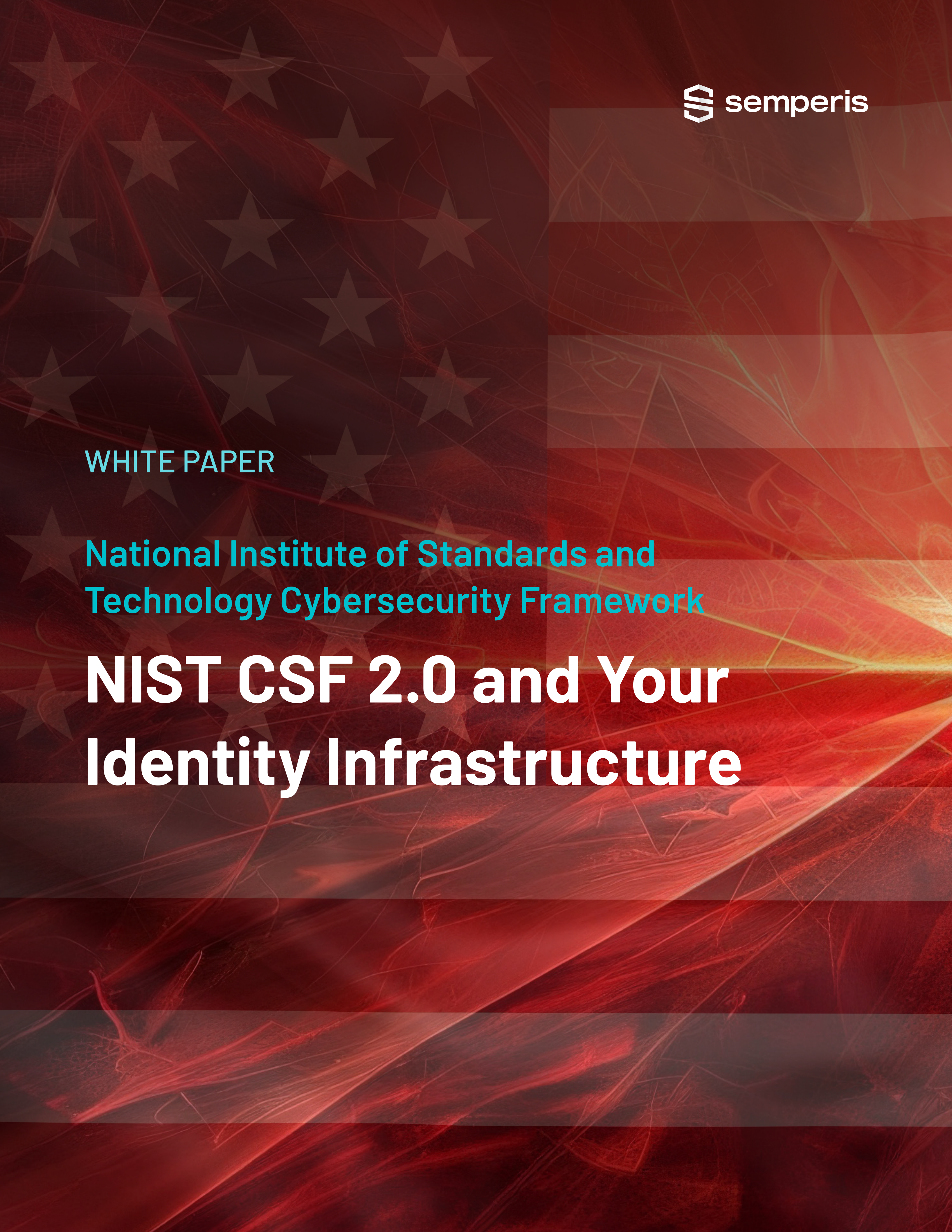


semperis

WHITE PAPER

National Institute of Standards and Technology Cybersecurity Framework

NIST CSF 2.0 and Your Identity Infrastructure

TABLE OF Contents

Introduction

In today's inherently complex digital environment, organizations of all sizes and types must understand and manage cybersecurity risks. Securing confidentiality, integrity, and availability for critical infrastructure and services, institutions, and enterprises is essential for national and global stability.

But effective cybersecurity is complex, demanding understanding of myriad assets, contextual factors, malicious actors, threat vectors, impacts, and mitigation tactics.

Thus, regardless of whether your organization employs a basic or high level of technical sophistication, strengthening your cybersecurity posture requires a multi-pronged approach that includes:

- A well-planned strategy
- A comprehensive and robust framework
- Stringent mechanisms for testing and validation

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) provides such an approach. Developed in 2013 by the U.S. Department of Commerce, the Framework was created as an adaptable standard to encourage innovation and efficiency while helping organizations operate securely and protect business confidentiality and personal privacy.

NIST is not a regulatory agency, so most organizations that adopt the Framework do so voluntarily. Executive Order 13800[1] made the Framework mandatory for U.S. Federal Government agencies. Some organizations require the Framework for their customers or supply chain partners.

Because the NIST CSF is a comprehensive model that aligns with established informational sources such as NIST Special Publications and ISO standards, the Framework has gained international acceptance as a foundational standard,[2] and many of its components are referenced by cybersecurity regulations in other nations.

In February 2024, NIST released the latest version, CSF 2.0.[3]

[1] Federal Register: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

[2] Leveraging NIST CSF for Public Sector Cybersecurity | Semperis

[3] The NIST Cybersecurity Framework (CSF) 2.0

Cyber resilience and the NIST CSF

Cyber breaches from organized crime and nation states have tremendous negative effects on society. Estimates of the global impacts vary,[4,5] but in October 2023, Anne Neuberger, then the White House Deputy National Security Advisor for Cyber & Emerging Tech at the National Security Council, estimated cybercrime would cost the world $23 trillion in 2027.[6] Cyber-related events that cause significant industry-wide outages result in the highest costs. For example, the nation-state attack NotPetya had estimated total costs of $10 billion.[7]

Highly capable criminal actors have made extortion a major industry by scaling the destructive capabilities of data breaches through ransomware. The FBI has estimated that one ransomware organization—Akira—has breached and extorted more than 250 organizations, garnering revenues of more than $42 million.[8] Other high-profile examples include the Medusa[9] and Black Basta[10] ransomware operations. NCC Group tracked 94 active ransomware groups in 2024.[11]

The emergence of ransomware and threat actors at scale has moved cybersecurity from a focused activity in a few highly regulated industries and government agencies to a top concern for all industries.

In this landscape, the NIST CSF provides a roadmap for reducing cyber exposure for any organization.

Identity security and your cyber resilience

As the digital ecosystem of organizations has become more complex, the traditional perimeter-defense approach to cybersecurity has become less effective. Attackers know that when users log in from anywhere, the attack surface starts with users' account credentials.

Instead of breaking in, the malicious actor *logs* in. Thus, organizations are increasingly looking to identity security as a focal point for their overall cyber resilience.

Threat intelligence provides strong support for this approach. Microsoft data shows that of more than 600 million identity attacks per day on Microsoft platforms, more than 99% are password-based.[12] Meanwhile, IBM sees as many as 74% of breaches having a privileged compromise in an early stage of attack.[13]

[4] U.S. cost of cybercrime 2028| Statista

[5] the-cost-of-cyber-crime-full-report.pdf

[6] U.S. cost of cybercrime 2028| Statista

[7] Unexpectedly, the cost of big cyber-attacks is falling

[8] #StopRansomware: Akira Ransomware | CISA

[9] CISA: Medusa ransomware hit over 300 critical infrastructure orgs

[10] Black Basta ransomware gang's internal chat logs leak online

[11] Cyber Threat Monitor Report 2024 | NCC Group

[12] Microsoft Digital Defense Report 2024

[13] Cost of a data breach 2024 | IBM

Active Directory (AD), the identity system for 90% of global organizations, is at the heart of the vast majority of industry and government enterprises. However, ensuring AD's resilience is notoriously difficult. Not only is AD recovery a significant, multi-step activity,[14] it is fraught with difficulties[15] due to the high volume of daily changes and outbound dependencies for services such as certificate management, DHCP, and DNS.[16]

Let's explore how increased identity system security can strengthen your conformance with the NIST CSF—and your overall cyber resilience.

Developments in NIST CSF 2.0

The NIST CSF received a welcome update in 2024, adding a new core function, Governance, to the original five functions and updating the underlying categories that organize requirements.

The new Governance function helps organizations define how:

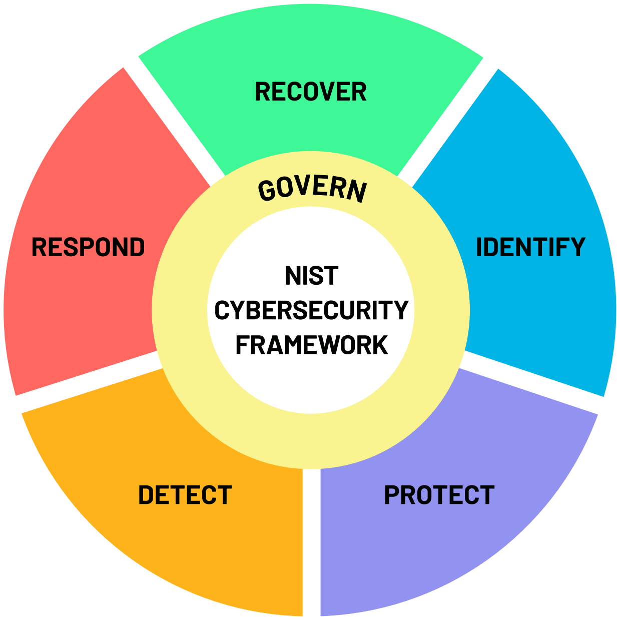
- Outcomes from security risk management relate to other enterprise functions
- Cybersecurity policies, oversight, and practices integrate with overall business strategy
- The organization can work to ensure that the controls are effective

The CSF aligns to a phased model of defense, typically illustrated as a wheel to show the ongoing and cyclical nature of cybersecurity practice (*Figure 1*). Governance overlays this model by unifying cybersecurity activities into a framework that supports defined purpose, objectives, measures, and ownership.

Let's dive deeper into the categories in each core function that relate to identity system security.

Figure 1: NIST Cybersecurity Framework

CSF functions are represented as a wheel to show that all core functions happen concurrently with Governance.



[14] Active Directory Forest Recovery Guide | Microsoft Learn

[15] The Guide to the Microsoft Active Directory Forest Recovery Guide - Semperis

[16] AD Forest Recovery - Configure the DNS Server service | Microsoft Learn

Govern

To meaningfully manage cyber risk, you need to understand who is responsible for risk management activities and what outcomes you're seeking.

Category	Focus areas of selected sub-categories
GV.OC **Organizational Context**	GV.OC-02: Identify internal and external stakeholders. GV.OC-04: Define critical objectives, capabilities, and services. GV.OC-05: Define required organizational outcomes.
GV.RM **Risk Management Strategy**	GV.RM-03: Integrate cybersecurity and enterprise risk management. GV.RM-06: Calculate, document, categorize, and prioritize cybersecurity risks.

When managing your identity infrastructure security, multiple considerations fall under categories in the Govern function.

- **Organizational Context (GV.OC):** You will need to be clear about who owns identity system cyber risk, how your identity system supports the critical services you depend on to run your business, and how ensuring identity system resilience supports the overall resilience of your business operations.
- **Risk Management Strategy (GV.RM):** You must clearly understand the risks and vulnerabilities of AD and Entra ID identity systems and how capabilities of other systems and services depend on identity security. If your identity systems are compromised or down, most of your enterprise operations will be affected. Thus, cybersecurity must be clearly integrated as part of your overall enterprise risk management.

To execute the specific actions for governance, NIST advises following a risk assessment standard such as those from the International Standards Organization[17] or the Information Security Forum.[18]

Identity-focused actions to consider for the Govern function

- Understand your identity system's role in the overall risk posture of the organization.
- Integrate identity security objectives into your strategic roadmap.
- Define ownership of identity capabilities.
- Understand which other critical services depend on your AD and Entra ID capabilities.
- Define assurance activities to ensure continuous monitoring and management of your identity system.

[17] ISO/IEC 27005:2022(en), Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[18] Information Risk Assessment Methodology 2 (IRAM2) - Information Security Forum

Identify

To meaningfully control your cyber risk, you need have a firm grasp on:

- The assets (physical, digital, or intangibles) you're tasked with managing
- Vulnerabilities, changes, and emerging threats that may cause failures or be exploited by malicious actors
- How to mitigate exposures and vulnerabilities to reduce your attack surface and risk of compromise

Category	Focus areas of selected sub-categories
ID.AM **Asset Management**	ID.AM-01 and 02: Inventory hardware, software, services, and systems. ID.AM-08: Manage risk of such assets throughout their lifecycles.
ID.RA **Risk Assessment**	ID.RA-01 to 04: Understand and manage vulnerabilities and threats and minimize their potential impacts. ID.RA-06: Determine and communicate appropriate responses and remediation for identified risks. ID.RA-07: Manage changes and exceptions and assess potential risk impact.
ID.IM **Improvement**	ID.IM-01: Use evaluations to identify risk management improvements. ID.IM-02: Test and practice risk improvement activities. ID.IM-03: Regularly review risks management processes, procedures, and activities to identify improvements. ID.IM-04: Establish, maintain, and improve incident response plans.

Identifying and managing system vulnerabilities, threats, and risks is a constant challenge for most organizations. NCC Group reported more than 40,000 new vulnerabilities for 2024—an increase of 28% over the preceding year.[19] Of those, fewer than 1% were weaponized in the same year; however, an attacker needs only one opening to compromise your entire identity system.

In addition to inherent or emerging vulnerabilities, misconfigurations in the identity system can be a significant source of exposure, offering attackers pathways for lateral movement and privilege escalations. Splunk reported in their 2024 threat report that the biggest threat vector for initial compromise was misconfigurations (39%) with vulnerabilities in internally developed systems second (31%), zero-day vulnerabilities (30%) in third place, and known vulnerabilities fourth (29%).[20]

[19] Cyber Threat Monitor Report 2024 | NCC Group

[20] State of Security 2024

- **Asset Management and Risk Assessment (ID.AM, ID.RA):** To manage these risks, you need deep, expert understanding of both vulnerabilities and misconfigurations in AD and Entra ID.
- **Improvement (ID.IM):** To confidently build a risk reduction program, you must regularly test your incident response plan, including clean restore of AD backups.

Identity-focused actions to consider for the Identify function

- Integrate identity security best practices into your cybersecurity policies and processes.
- Understand and manage identity security assets and dependencies.
- Map identity security and cybersecurity outcomes.
- Establish a program to identify, evaluate, prioritize, and remediate cybersecurity vulnerabilities and indicators of exposure.
- For identity and access management (IAM) and identity security posture management, formulate a matrix to remediate your indicators of exposure and compromise, prioritizing fixes based on criticality and potential impact.
- Build a remediation program to patch vulnerabilities based on risk to services.

Protect

The CSF 2.0 Protect function enables organizations to reduce adverse cybersecurity events and impacts. The function covers multiple cybersecurity capabilities, including IAM, data security, platform security, awareness, and resilience.

Category	Focus areas of selected sub-categories
PR.AA **Identity Management, Authentication, and Access Control**	PR.AA-01 and 02: Manage and validate user and service identities and credentials. PR.AA-03: Authenticate users, services, and devices. PR.AA-04: Verify and protect assertions. PR.AA-05: Define and manage permissions and authorization.
PR.PS **Platform Security**	PR.PS-01 and 02: Establish configuration management and software maintenance practices. PR.PS-04: Generate logs for continuous monitoring.
PR.IR **Technology Infrastructure Resilience**	PR.IR-01: Protect networks and environments from unauthorized access. PR.IR-03: Employ mechanisms to ensure resilience in normal and adverse situations.

- **Identity Management, Authentication, and Access Control (PR.AA):** IAM is vital to establish a strong foundation for interconnected functions in the CSF. Once you've ensured the integrity of your identity system through management of vulnerabilities and exposure in your AD and Entra ID systems, the IAM practices recommended in the CSF function help ensure vital operational capabilities are all available and reliable.

- **Platform Security (PR.PS):** Identity and access risks remain some of the main threat vectors for organized crime. Attack techniques that take advantage of password spraying,[21] weak passwords,[22] unhardened access environments,[23] and vulnerabilities in multifactor authentication (MFA) configuration routinely give attackers the dreaded way in. In fact, in October 2024, Microsoft reported 7,000 identity-based attacks per secon—99% of them focused on passwords—up from 4,000 the year before.[24] The CSF stresses the need for hardening, robust maintenance, and configuration management on large cloud platforms (whether infrastructure or applications).

- **Technology Infrastructure Resilience (PR.IR):** Generally, you need to build resilient technologies where secure access is assured by your ability and capacity to plan, test, and successfully restore your technology services.

[21] Password Spraying Explained | Semperis Identity Attack Catalog

[22] Missing or weak credentials is the lead compromise factor with 47.8% according to Google Cybersecurity Action Team, Threat Horizon, Apr 2023

[23] PaloAlto Unit42 found that 99% of cloud users, roles, services, and resources are granted excessive permissions

[24] Microsoft Digital Defense Report 2024

Identity-focused actions to consider for the Protect function

- Implement a least-privilege access model.
- Implement just-in-time and privileged access management principles to safeguard your Tier 0 assets, including AD.
- Review the Entra ID Connect synchronization rules to be sure proper segregation of access exists between AD and Entra ID, enabling syncing of only necessary principals.
- Execute active penetration testing, red teaming, or tabletop exercises to ensure the identity infrastructure is secure.
- Invest in automation of identification, scanning, and remediation for the identity infrastructure.

Detect

Because a high number of cyberattack methods focus on AD and Entra ID capabilities,[25] monitoring and active detection of identity threats and compromise is key to containment, recovery, and resilience.

Category	Focus areas of selected sub-categories
DE.CM **Continuous Monitoring**	DE.CM-03 and 09: Monitor personnel activities and technology use as well as hardware and software environments for potentially adverse events.
DE.AE **Adverse Event Analysis**	DE.AE-02 and 03: Analyze and correlate events across multiple sources. DE.AE-04: Understand the impact and scope of adverse events. DE.AE-06: Provide information about adverse events to stakeholders. DE.AE-07: Integrate cyber threat intelligence and contextual information into event analysis.

- **Continuous Monitoring (DE.CM):** To achieve awareness of the overall security posture and quickly detect potential risks, compromise, or attacks, security operations teams need to manage signals from a wide variety of log sources from on-premises and cloud environments and operational technologies.
- **Adverse Event Analysis (DE.AE):** Analyzing anomalies, indicators of compromise, and other potentially adverse events is difficult in large enterprises, where AD systems sprawl in scale, complexity, and configuration.

In addition, the teams managing operational services are often under significant pressure to keep services running without creating blockers for users.

For these reasons, when managing complex, hybrid identity infrastructures, robust and specialized automation solutions are essential to identify indicators of exposure and compromise and speed corrective actions while reducing the need for manual security development, configuration, and event triage.

Identity-focused actions to consider for the Detect function

- Configure and manage security measures on your identity infrastructure.
- Ensure logging is enabled and a trained team is monitoring suspicious and potentially harmful events.
- Enable secured logs on your identity infrastructure.
- Consider identity-focused analytics tools for a richer data set and scalability through automation.

[25] https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3917556/nsa-jointly-releases-guidance-for-mitigating-active-directory-compromises/

Respond

Threat actors are advancing their capabilities at breakneck speed. For defenders, this often means that prevention is not an option. Thus, the art of effective response to and containment of a cyber incident is essential for business resilience.

Category	Focus areas of selected sub-categories
RS.MA **Incident Management**	RS.MA-01: Execute incident response plans in coordination with relevant third parties. RS.MA-02 to 05: Triage, prioritize, escalate, and analyze incidents to prepare for recovery.
RS.AN **Incident Analysis**	RS.AN-03, 06, and 07: Analyze incidents to discover root cause, document response activities, and secure incident data.
RS.CO **Incident Response Reporting and Communication**	RS.CO-02 and 03: Coordinate incident response activities and share response information with relevant stakeholders.
RS.MI **Incident Mitigation**	RS.MI-01 and 02: Contain and eradicate incidents.

- **Incident Management (RS.MA):** When an incident occurs, time is of the essence. You must be prepared to swiftly mobilize teams and resources to manage your response to cybersecurity incidents, following structured incident management protocols to contain potential impact. It's essential to maintain readiness across distributed teams, ensuring all staff are familiar with their roles so they'll be effective during high-pressure situations.

- **Incident Analysis (RS.AN):** Effective incident analysis requires conducting thorough investigations to understand root causes, attack vectors, and compromised systems, thereby supporting accurate response and forensics. Practitioners often face the difficulty of gathering reliable evidence during ongoing attacks, especially when attackers use sophisticated evasion tactics. For example, an attacker who has gained privileged access may attempt to delete audit logs. Numerous threat actors, such as RansomHub, LockBit, and Ghost, have all used this technique.[26]

[26] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-050a

- **Incident Response Reporting and Communication (RS.CO):** To meet reporting requirements of the laws, regulations, and internal policies that govern your organization, you need to ensure response activities are clearly communicated and coordinated with internal and external stakeholders.
- **Incident Mitigation (RS.MI):** Your security teams must take decisive action to prevent the incident from spreading. To minimize harm, you'll want to be able to leverage containment strategies and mitigation techniques quickly and effectively, as incomplete containment or delayed response can result in further damage.

Identity-focused actions to consider for the Respond function

- Conduct a thorough security review and map attack paths leading to Tier 0 assets, including shadow administrators, nested groups, and local administrative rights, to understand your identity risk profile.
- Devise a detailed, out-of-band incident response plan that includes clearly defined roles and responsibilities for all stakeholder team members and secure access to critical response documents and information.
- Ensure the integrity of your identity infrastructure logs and monitor changes in AD in real time.
- Establish the ability to collect forensically sound data on your identity system and perform a forensic investigation to determine the origin and methods of attack.
- Ensure your identity forensics capabilities are integrated and tested as part of your broader incident response readiness plan.

Recover

Of course, the ultimate aim of incident response is to restore operational availability of your assets, services, and operations as quickly as possible. To achieve this resilience, you must ensure you can recover to a secure state and in a timely manner in case of an outage or cyberattack.

Category	Focus areas of selected sub-categories
RC.RP **Incident Recovery Plan Execution**	RC.RP-01 and 02: Execute recovery processes and actions from the incident response plan. RC.RP-03, 04, and 05: Before using restored backups, assets, or systems, ensure their integrity, security, and readiness for post-incident operations.

Your identity infrastructure is key for the use of most—if not all—digitally enabled services. Without an incident recovery plan for AD and Entra ID, you are unlikely to be able to restore your services and operations after a major destructive event.

However, identity infrastructure is highly complex, with many interdependencies. It is a core foundation of your technology-enabled services, so restoring it is also complex.

Legacy identity systems such as AD can be notoriously difficult to restore to a known secure state.[27] The official Microsoft guidance details the process to restore a single AD forest—requiring 28 steps covered in a 150-page document—and even a slight deviation will curtail a successful recovery.

For many organizations, recovery is further complicated because of other services (such as DHCP and DNS) running on AD, hybrid cloud and on-premises integrations, and the sheer number of changes that occur daily in a large AD forest.

Depending on backup frequency, AD backups may also be compromised. Thus, once an AD forest is recovered, it still cannot be trusted for use without extensive forensic analysis to remove persistence mechanisms that enable the attacker to retain a footprint.

A well-developed disaster recovery plan includes mechanisms for avoiding these onerous and devastating recovery delays, including:

- Frequent, immutable identity system backups
- Automated and timely AD forest recovery
- Thorough and rapid post-incident forensics

Such capabilities must be defined and tested for you to be able to rely on them during a cyber incident.

[27] Top Manual AD Forest Recovery Pitfalls | Semperis Guides

Identity-focused actions to consider for the Recover function

- Define a plan for identity system infrastructure recovery and restore, including specific team members who are assigned specific recovery tasks.
- Confirm measures to ensure clean-state recovery, including air-gapped, immutable backups.
- Establish a separate, non-production environment that mimics real-word use where you can perform frequent restore testing.
- Ensure identity recovery activities are implemented and integrated with broader business continuity and crisis management plans and activities.

Tool specialization

Managing the identity security of a large, complex organization is a major undertaking—even before your team performs hardening, security assessments, and disaster recovery planning. Because the availability of most of your operational services relies on AD or Entra ID services, you must ensure the operational team has the necessary time, skills, and incentives to manage identity cyber resilience.

To create the focus and capacity that enable your teams to reduce security risk, consider evaluating solutions that are purpose-built for identity security—such as those from Semperis, which offers community and paid tools that directly address the challenges of achieving a cyber-resilient enterprise.

How can Semperis help?

Below is a table highlighting the specialized capabilities that Semperis offers to support NIST CSF resilience outcomes. Semperis' products are enhanced by deep research from the identity security and AD-focused security research team.

Challenge	How Semperis can help	Solution
Govern To conform with NIST CSF requirements, it's vital that those responsible for cyber resilience have a strong understanding of the true risks associated with your identity system.	• Visualize identity security posture. • Identify risks to cyber resilience and compliance. • Map dependencies to enable AD restore. • Ensure a resilient identity system.	• Security Assessment services provide a clear view of identity and operational security posture and guidance for addressing security exposures at the strategic, operational, and tactical levels. • Purple Knight (no cost community tool) provides point-in-time security assessment of AD. • Forest Druid (no cost community tool) discovers and automatically maps attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit.
Identify Knowing your assets and their risks, vulnerabilities, and exposures is key to achieving a truly resilient enterprise.	• Map dependencies to enable AD restore. • Provide visibility into identity security posture. • Deliver semi-automated, research-led view of software vulnerabilities and misconfigurations. • Execute point-in-time vulnerability and misconfiguration scanning. • Provide ongoing risk identification and management.	• Active Directory Forest Recovery (ADFR) can map and automate forest recovery, including relevant dependencies. • Purple Knight provides point-in-time AD security assessment and recommends fixes for indicators of exposure and compromise. • Directory Services Protector (DSP) provides continuous threat and vulnerability detection and automative rollback of risky and malicious changes. • DSP provides comprehensive logging and highly specialized AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of SOC visibility through SIEM integration.

Challenge	How Semperis can help	Solution
Protect Establishing strong controls helps you ensure robust identity and technology resilience.	• Provide privileged access management and identity and access management for all users. • Enhance protections for identity security capabilities, including attack prevention and post attack recovery.	• DSP enables continuous monitoring of AD and Entra ID security posture, ensuring the underlying identity systems are secure and trustworthy. • ADFR reduces the time for a full AD forest restore by 90% compared to manual recovery. • The Forest Druid community tool discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit.
Detect Your identity infrastructure is a rich source of vulnerabilities and misconfiguration, requiring skill and dedication for meaningful detection.	• Provide AD and Entra ID monitoring to detect attacks and enable accurate incident reporting. • Comprehensively control the constantly changing AD environment with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities.	• DSP provides continuous threat and vulnerability detection, capturing every change made in AD, helping identify malicious changes, and automatically rolling back risky changes. • DSP provides comprehensive logging and highly specialized AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of SOC visibility through SIEM integration.
Respond Increasingly, large enterprises are required to be able to manage and report on incidents in short time periods.	• Secure your logs for forensic analysis. • Enhance ability to detect actions of a malicious actor and rapidly report incidents and attacks impacting AD and Entra ID.	• DSP provides comprehensive logging and highly specialized AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of SOC visibility through SIEM integration. • Identity Runtime Protection uses machine learning to perform attack pattern detection by capturing, analyzing, and correlating authentication activities with Semperis' identity threat intelligence to signal malicious behavior. • Ready1 centralizes and unifies all aspects of cyber crisis planning and incident response, ensuring seamless crisis response through preparation, collaboration, and enterprise-wide communications.

Challenge	How Semperis can help	Solution
Recover You need to be able to restore your identity system capabilities rapidly, to a known clean state—and have testing that proves you can.	- Enable early detection or avoidance of a security breach of your identity system and dependent technology-enabled services. - Provide proven, clean-state restore with validated recovery objectives. - Operationalize proven crisis and incident response frameworks, enhanced with expert playbooks—from preparation to after-action review.	- ADFR automates forest recovery, restoring AD quickly and safely without reintroducing malware. - ADFR also allows for post-breach forensics to identify persistence and recover AD to a trusted state. - Disaster Recovery for Entra Tenant (DRET) recovers Entra ID objects. - Ready1 centralizes crisis response, enabling teams to develop, test, remediate, and continuously improve incident response planning.

Conclusion

To build resilience in alignment with the NIST CSF, we recommend you establish six major capabilities for AD and Entra ID resilience, including:

1. Establish a program for asset and risk management and ownership for your identity system risk and resilience.
2. Establish a comprehensive and automated exposure, threat, and vulnerability monitoring program and integrate this capability with your security operations center.
3. Reduce the attack surface of your AD and Entra ID infrastructure through continuous monitoring and remediation of indicators of exposure and compromise.
4. Build and regularly test a comprehensive incident response plan for your critical technology and operations services, including your identity system, to enable rapid incident response, reporting, and forensic capabilities.
5. Develop and test an automated recovery process to enable rapid restore of your identity system to a proven, trusted state.
6. Establish a project of continuous improvement, including best practices from leading experts in the cybersecurity industry.

In our experience, achieving these capabilities is challenging. Sustaining them over time is not possible without significant automation. Semperis market-leading products and services can provide you with this threat-led, automated capability.