CYBERARK®
The Identity Security Company™

Addressing the NIST Cybersecurity Framework 2.0 with the CyberArk Identity Security Platform

Table of Contents

Overview

The information provided in this document reflects CyberArk's opinion on the ability to leverage our products to comply with various industry requirements. CyberArk believes the content is accurate as of its publication date. However, it is provided for informational purposes only and is not intended as legal or other advice. It is provided without any express, statutory, or implied warranties and is subject to change without notice. Customers are advised to consult with their own professionals on the matter, including for specific guidance tailored to their unique circumstances. CyberArk shall not be liable for any direct, indirect, or consequential damages arising from the use of, or reliance on, this information.NIS2 applies to any entity providing critical services in an EU member country. All 27 EU member states must incorporate NIS2 into their own national laws by October 2024. The main directive goes into full effect in January 2025, categorizing organizations into two types of critical entities:

NIS2 covers a broader range of industries than the original directive. Here's an overview, color-coded to indicate which sectors are "essential" or "important."

What is the NIST CSF?

The National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity, commonly known as the NIST Cybersecurity Framework (CSF), is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk.

Developed through collaboration between industry and government, the framework was first published in 2014. It provides a prioritized, flexible and cost-effective approach for helping organizations manage cybersecurity risk, including those in sectors such as energy, water, finance, healthcare and transportation.

Version 2.0 was released in Feb 2024. This added a sixth core function and revised the controls to reflect the 10 years of success mitigating cybersecurity risk. It also expands the scopes from just critical infrastructure to any enterprise.

The NIST CSF 2.0 is structured around six core functions— govern, identify, protect, detect, respond and recover — which offer a comprehensive and outcome-based methodology for addressing cybersecurity threats.

These functions assist organizations in developing a holistic cybersecurity program that encompasses risk management practices and principles, aimed at protecting networks, systems and data from cyberattacks.

The framework's adaptability allows it to be implemented by organizations of all sizes, sectors and maturity levels, making it a widely adopted standard for cybersecurity risk management worldwide.

The Six Functions

Govern – A new addition in CSF 2.0, the Govern function focuses on establishing and monitoring the organization's cybersecurity risk management strategy, expectations and policy, highlighting the need for executive support and stakeholder engagement in a successful cybersecurity program.

Identify – Establishes an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. It involves inventorying resources to prioritize efforts, consistent with risk management strategy.

Protect – Focuses on safeguarding critical infrastructure services through appropriate safeguards. It involves implementing controls to limit or contain the impact of potential cybersecurity events.

Detect – Involves the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. It emphasizes timely discovery of cyber incidents to enable quick response.

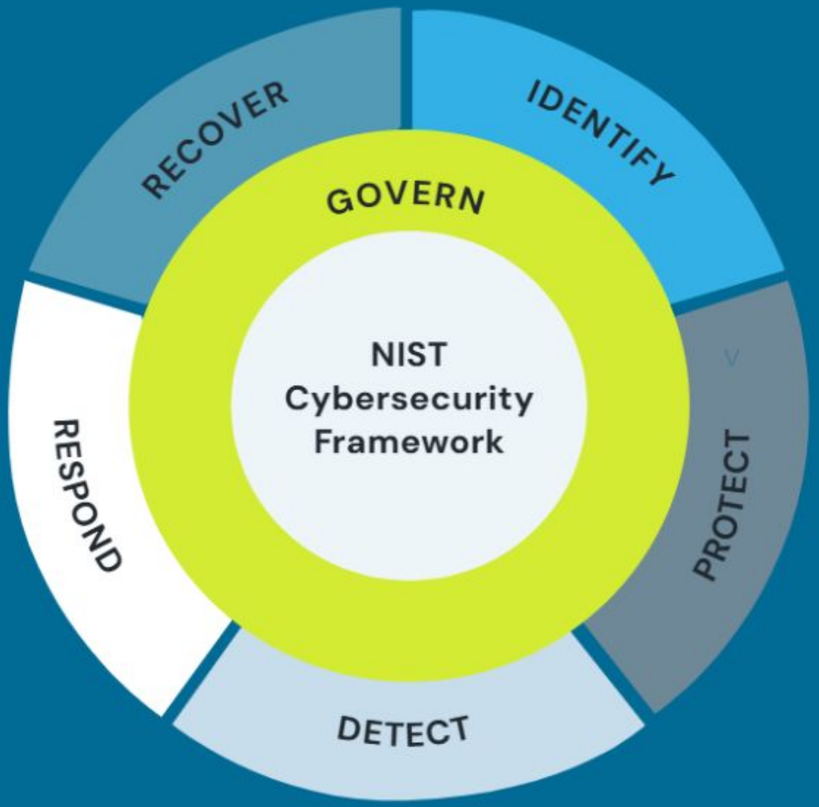
Respond – Addresses the actions to take after detecting a cybersecurity incident. It includes developing and implementing response planning, communications and analysis to manage and mitigate the impact of incidents.

Recover – Involves planning and implementing activities to restore any capabilities or services impaired due to a cybersecurity incident. It emphasizes resilience and recovery planning to minimize downtime and financial loss.

Informative References

It's no surprise that controls overlap between different frameworks. These are captured as Informative references within the NIST CSF. Each Informative reference covers standards, guidelines and practices that support the implementation of the framework's cybersecurity activities and outcomes associated with the functions above.

It can be a challenge for a layperson approaching a compliance framework implementing controls based off what sometimes feels like an arbitrary statement. These controls are often designed to address the different IT enterprises, environments and workloads as well as references describing how enterprises could approach a control.



Source: https://www.nist.gov/

The NIST CSF groups its controls in six clear functions, each offering a category and a series of subcategories under each. Each subcategory includes several informative references, as well.

Understanding Subcategories

Below is an example of a subcategory taken from NIST's CSF 2.0. This subcategory is taken from the Detect function and is part of the adverse event analysis category.

Sub-category

DE.AE-03: Information is correlated from multiple sources

Implementation Examples

- **Ex1 :** Constantly transfer log data generated by other sources to a relatively small number of log servers
- **Ex2 :** Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources
- **Ex3 :** Utilize cyber threat intelligence to help correlate events among log sources

DE.AE-03 Is the name of the subcategory

'Information is correlated from multiple sources' is the requirement of the subcategory.

Implementation example is where the implementation references exist. They are optional but practical views on how to achieve the intended outcome of the control. In this case the practical effort is addressed with the idea of implementing centralized log management and monitoring.

How CyberArk Can Help

The following are selected categories and subcategories of the NIST CSF where CyberArk can help your organization meet requirements.

Govern

The Govern section speaks to the need of strong governance and buy in from an enterprise's leadership team.

GV.RM-06	**A standardized method for calculating, documenting, categorizing and prioritizing cybersecurity risks is established and communicated.**

CyberArk offers the Blueprint methodology, a best practices framework for building identity security programs focused on risk reduction and aligning security controls to enterprise resources with a focus on risk and privilege. The CyberArk Blueprint can be used to quantify and understand the risks to be mitigated and their impact on a successful identity security program.

GV.SC-09	**Supply chain security practices are integrated into cybersecurity and enterprise risk management programs and their performance is monitored throughout the technology product and service life cycle.**
GV.SC-10	**Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.**

The implementation examples provided by NIST speak to discussion and policy third-party suppliers to ensure their security programs are up to standard. CyberArk Vendor PAM slutions allow you to isolate access to your infrastructure and resources from third-party vendors without allowing their security practices to increase your risk and exposure. This methodology also mitigates the risks of onboarding and offboarding of third-parties and external vendors.

Identify

Workloads cannot be secured if they're unknown. Identify forces an enterprise to ensure that processes are in place to make sure every component Is documented and understood.

ID.RA-03	**Internal and external threats to the organization are identified and recorded.**
ID.RA-04	**Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.**
ID.RA-05	**Threats, vulnerabilities, likelihoods and impacts are used to determine risk and inform risk prioritization.**

Both CyberArk Labs and the CyberArk Blueprint framework can support an enterprise in understanding and quantifying the actions of threat attackers. This can become another input into a risk assessment practice. CyberArk Labs is focused on identifying, documenting and mitigating new types of attacks. CyberArk Blueprint aligns security control recommendations to common enterprise resources and privileges, allowing security teams to quickly identify high-risk vulnerabilities and their impact. In addition, the CyberArk Red Team can support penetration testing opeations for organizations.

Protect

Protect covers the preventative controls that make up the technological backbone of many security programs. It is divided into each of the logical areas that cover the preventative controls of cybersecurity programs.

PR.AA-01	**Identities and credentials for authorized users, services and hardware are managed by the organization (formerly PR.AC-01).**
PR.AA-02	**Identities are proofed and bound to credentials based on the context of interactions.**

The CyberArk Identity Security Platform has strategic integrations with many human resources information systems (HRIS), serving as the fundamental first steps into building identity lifecycle management capabilities. It creates one identity your employee or contractor will use for their tenure within the enterprise. Shorter tenure access can be managed via CyberArk Vendor PAM. Both options leave the enterprise fully in control of the identity and credentials throughout their lifecycle.

PR.AA-03	**Users, services and hardware are authenticated.**
PR.AA-04	**Identity assertions are protected, conveyed and verified.**

The CyberArk Identity Security Platform has authentication at its core. Designed to support SAML, oAuth and other methods of integrating identity. Password rules can be configured centrally as part of SSO options. Extending strong SSO and MFA capabilities and additional controls or validations are available when required by either configuration or risk.

PR.AA-05	**Access permissions, entitlements and authorizations are defined in a policy, managed, enforced and reviewed and incorporate the principles of least privilege and separation of duties.**

The CyberArk Identity Security Platform supports a range of different ways to address this subcategory. Everything from risk-based authorization to account lifecycle management to recertification campaigns and Zero Standing Privilege-based access is supported. This gives the enterprise a diverse range of controls to address this subcategory regardless of the target environment.

PR.PS-02	**Software is maintained, replaced and removed commensurate with risk.**
PR.PS-05	**Installation and execution of unauthorized software are prevented,**

Endpoint privilege security is delivered from the CyberArk Identity Security Platform, allowing for the application of controls relevant to this subcategory for risk-based software control and access granted to software. These controls also cover the installation of software.

PR.IR-01	**Networks and environments are protected from unauthorized logical access and usage.**

CyberArk provides secure access controls to a diverse range of environments through the CyberArk Identity Security Platform. The platform can secure connections between segmented networks and act as a target for access as part of a Zero Trust strategy.

Detect

Detect covers the controls that allow organizations to understand an attacker has made it past the efforts made to prevent any breaches. As critical as Protect, this enables security teams to reduce the time and impact an attack might have for unauthorized access to systems in the enterprise.

DE.CM-03	**Personnel activity and technology usage are monitored to find potentially adverse events.**
DE.CM-06	**External service provider activities and services are monitored to find potentially adverse events.**
DE.CM-09	**Computing hardware and software, runtime environments and their data are monitored to find potentially adverse events.**

The CyberArk Identity Security platform is built around our market leading identity security intelligence capability. The platform is enhanced by insights from the platform's diverse SSO capabilities, adaptive MFA engine and information collected from session recordings in order to respond with remediation actions. The response actions can be either on-platform in the form of an account suspension or trigger a flow or off-platform using a webhook to initiate other automations (such as a ServiceNow event starting a security operations center (SOC) notification for investigation).

DE.AE-03	**Information is correlated from multiple sources.**

Acting either as the source or collector the CyberArk Identity Security Platform can contribute detailed logging to SIEMs or correlate logs into events using the integrated user behavior analytics (UBA) functionality that underpins identity security intelligence.

Respond

No cybersecurity program is complete without a clear incident response plan. The Respond section highlights the elements needed to have a successful incident response strategy and serves as the foundations of planning for the worst and thus minimizing the impact of an attack.

RS.MI-01	**Incidents are contained.**
RS.MI-02	**Incidents are eradicated.**

The CyberArk Identity Security Platform has successfully been used as part of many incident responses. Able to provide an environment for the purpose of containment, it provides a protocol break and credential boundary between systems under investigation that may have been compromised. The platform can also serve as a part of the eradication of a cybersecurity incident utilizing the credential rotation and discovery capabilities to bring systems back into control.

Recovery

Closing out the six sections of the NIST's CSF is Recovery. Focused on building the capability of incident recovery, this section serves to help enterprises build robust plans and get back to normal after the worst has happened.

RC.RP-05	**The integrity of restored assets is verified, systems and services are restored and normal operating status is confirmed.**

Further to the rotation capabilities discussed in **RS.MI-02**, the CyberArk Identity Security Platform monitors any bypass of controls, providing an essential function to continuously validate the integrity of recovered servers. Reporting is available to confirm the work and asset recovery now under management.

The Future of NIST CSF

The evolution of NIST CSF to version 2.0 addresses the rapidly changing cybersecurity landscape with fresh guidelines that reflect the latest threats and technological advancements.

The freshly released iteration aims to provide a more flexible and comprehensive approach to cybersecurity, ensuring organizations can effectively manage and mitigate risks in a dynamic digital world.

As cyber threats become more sophisticated, the framework will likely grow to incorporate new best practices for cloud security, supply chain risk management and the protection of critical infrastructure. It will also emphasize the importance of cyber resilience and the need for organizations to quickly adapt and recover from cyber incidents.

Going Further with CyberArk

CyberArk can help you achieve your identity security compliance goals. The CyberArk Identity Security Platform delivers a complete solution for securing your entire workforce.

Get a free 30- day trial of CyberArk Secure Cloud Access.

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

CYBERARK®
The Identity Security Company™