WHITEPAPER

The Complete Guide to the NIST Cybersecurity Framework

imprivata®

Organizations of every size and across all sectors are at risk for a cyberattack. Digital transformation of manual processes and the cloud-enabled, decentralization of workforces and workplaces creates a nebulous system that makes organizations vulnerable to ransomware, bad actors, and other forms of cyber crime. We thought the world wide web was worldwide back in the 1990s, but the world is now more digitally interconnected than ever before. This means cyber risk is pervasive and unavoidable — and the proof is in the stats.

- There were 700 million attempted ransomware attacks in 2021 (up 134% from 2020)
- According to Cybersecurity Ventures, ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.
- 54% of organizations have experienced a cyberattack in the last 12 months

With so much risk comes much responsibility. Protecting assets, data, and information has become a mission-critical agenda item for more than just organizational IT and infosecurity teams. Cybersecurity is now a business, board-level priority — you can't separate the two. It's also caught the attention of policy makers and government agencies, which is why more policy has been created to protect the technology and infrastructure that can keep critical assets and access points safe.

NIST Framework

The National Institute of Standards and Technology (NIST), a part of the U.S. Department of Commerce, was built to support technological efforts of all scales, from the smallest nanotechnology to global innovations and infrastructure.

To support cybersecurity efforts, NIST created a set of guidelines and practices that better manage and reduce overall cyber risk. It's recognized as the gold-standard of cybersecurity, and the practices within the framework are all based on existing guidelines as well as industry best practices that have proven effective in combating cybercrime while minimizing risk.

The goal of the NIST Cybersecurity Framework is to give organizations an easy-to-understand, yet thorough, guide on how to build a cybersecurity structure that best fits an organization based on their level of risk.

The NIST Cybersecurity Framework is made up of three components:

- The Core
- Implementation tiers
- Profiles

Each component helps organizations determine where they're at in their cybersecurity maturity, where they'd like to be, and how to get there. While each component is important, the Core component holds five functions that serve as the standard for building an effective security model.

The five functions of the NIST Cybersecurity Framework

IDENTIFY

- Data, personnel, devices, systems, and facilities that keep businesses running and operating need to be identified and managed consistently to their importance and risk.
- The components of an organization's business environment, like mission, objectives, stakeholders, and activities are understood and prioritized so proper cybersecurity protocol can be established.
- Governance policies, procedures, and processes that manage and monitor an organization's regulatory, legal, risk, environmental, and operational requirements are understood and influence how cybersecurity risk is managed.
- Risk assessment is conducted so the organization understands the cybersecurity risk to operations like mission, functions, image, or reputation, org assets, and individuals.
- Risk management strategy is created, and priorities, restrictions, and all things risk-related are established.
- The organization has established and implemented processes to identify, assess, and manage supply chain risk.

PROTECT

- Identity management, authentication, and access control processes are established.
- Awareness and training for personnel and partners (third parties) is implemented and completed.
- Information and data are managed according to risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies are maintained and used to manage the protection of information systems and assets.
- Policies are established to protect the maintenance of industrial control and information system components.
- Protective technology solutions to ensure the security and resilience of systems and assets.

DETECT

- Information systems and assets are monitored to identify cybersecurity events.
- Detection processes and procedures are built, maintained, and tested to catch anomalous events.

RESPOND

- Response planning, processes, and procedures are put in place to detect cybersecurity incidents.
- Communications - response activities are coordinated with internal and external stakeholders.
- Analysis is conducted to ensure effective response and support recovery activities.
- Incidents are mitigated and vulnerabilities are identified and mitigated.
- Improvements are made from lessons learned and response strategies are updated.

RECOVER

- Recovery planning, processes, and procedures are conducted to restore systems affected by the incident.
- Recovery processes are improved by lessons learned.
- Communication is sent and internal and external stakeholders are updated on restoration/recovery activities, PR, reputation, etc.

Implementation tiers and profile

The next two components of the Framework help organizations understand their current cybersecurity posture and what they need to do to achieve the level of security needed.

PROFILES

Profiles are made up of an organization's business objectives, resources, and "risk appetite" — the amount of risk a business is willing to take on based on objectives they want to achieve.

Ideally, the Profiles are best used when held up against the Framework Core. Organizations should take their Profile — their current security posture — and compare it to the desired outcomes they'd like to achieve from the five Core functions. They can use this side-by-side comparison to identify opportunities to improve their security and risk practices and prioritize cybersecurity objectives and goals.

IMPLEMENTATION TIERS

The Implementation Tiers serve as an assessment to evaluate an organization's current level of security. The goal of these is to help organizations become aware of their security measures and where there can be improvements. Once an organization has identified its Profile, the Tiers matrix allows them to easily map out its level of cybersecurity and identify gaps or vulnerabilities. The higher the Tier, the more comprehensive a security strategy tends to be.

The Tiers rank three cybersecurity factors (risk management processes, integrated risk management programs, and external participation) on a scale of four "tiers": partial, risk informed, repeatable, and adaptive.

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk**[1.1] • benefits my sharing or receiving information from outside parties			

Tier 1: Partial

- **Risk management process:** Approaches are reactive, and cybersecurity risk management is not a high priority.
- **Integrated risk management program:** Little communication and risk management due to partial or lack of risk management processes — often dealt with on a case-by-case basis.
- **External participation:** Third parties (partners, consultants, vendors, supply chain, dependents) are generally unaware of risks.

Tier 2: Risk informed

- **Risk management process:** Risk processes are created and influence cybersecurity activity, but are not established or embraced.
- **Integrated risk management program:** Awareness, information, objectives, and assessments of cybersecurity and risk exist, but aren't standardized or embraced at an organization-wide level.
- **External participation:** External parties are aware of cyber risk but don't act on it.

Tier 3: Repeatable

- **Risk management process:** Formally approved risk management practices and policies are established and regularly updated based on threat and risk landscape.
- **Integrated risk management program:** There's an organization-wide approach to cybersecurity. Policies and processes are in place; employee training is performed so personnel know their role in cybersecurity activities. Communication is sent regarding cyber risk by senior and executive level.
- **External participation:** Third parties are aware of cyber risk and their role in the business ecosystem and/or supply chain as it pertains to risk and threats. They act on the risks by implementing written agreements, governance, policy, and monitoring activities.

Tier 4: Adaptive

- **Risk management process:** Cybersecurity and risk management is continuously improving by adapting security processes based on previous cyber incidents, current risk, and predictive factors. The business proactively adjusts to a changing threat landscape.
- **Integrated risk management program:** Cybersecurity risk awareness is implemented and integrated into organizational culture. It's seen in the same context as financial or other organizational risks — widely embraced and considered.
- **External participation:** External parties use current events and real-time information to understand and act on security risks. They receive, create, and contribute to the awareness and understanding around third-party cyber risk within the supply chain or business environment.

How to implement the NIST Cybersecurity Framework

The NIST Framework is voluntary, but it holds some of the best practices an organization can use to defend against bad actors. As organizations continue to implement more IoT devices and new technology to streamline operations and create more efficiency, it creates more access points for hackers to exploit. As a result, the potential attack surface continues to expand, which means cybersecurity needs to evolve and adapt right along with the new tech. The NIST Framework gives achievable action items that protect businesses from cyber threats, manage identities and user access, and meet compliance requirements.

CHECKLIST

How do you stack up against the NIST Framework?

IDENTIFY

- ☐ Inventory all business-related assets: data, physical devices and systems, software, applications, communication and data workflows, external information and systems
- ☐ Identify items within the business environment: objectives, stakeholders, mission, and roles in supply chain and/or critical infrastructure:
  - ☐ Objectives
  - ☐ Stakeholders
  - ☐ Mission
  - ☐ Role in supply chain and/or critical infrastructure
- ☐ Identify governance-related materials as it relates to cybersecurity:
  - ☐ Cybersecurity policy
  - ☐ Roles and responsibilities
  - ☐ Legal and regulatory requirements
  - ☐ Governance and risk management
- ☐ Assess and document cybersecurity risk, threats, vulnerabilities, likelihoods, impacts, and responses
- ☐ Establish risk management processes for organization and supply chain

PROTECT

- ☐ Restrict network access to only what's needed based on job function and implement zero trust network access to limit access at the application or protocol level
- ☐ Establish access policies for internal and external users
- ☐ Streamline remote access of employees and third-party vendors
- ☐ Identify, inventory, and manage all internal and external users
- ☐ Deploy multi-factor authentication for all users
- ☐ Implement credential management including password vaulting, rotation/randomizing, masking, and injection
- ☐ Provide cybersecurity awareness and training for employees
- ☐ Create and establish incident response plans and recovery plans in the case of cyber incidents
- ☐ Control and log all instances of remote maintenance

DETECT

- ☐ Establish workflows to detect and flag anomalous cyber events
- ☐ Monitor and track access and data usage across all systems for internal and external users
- ☐ Assess vulnerabilities within systems
- ☐ Detection processes are continuously evaluated, reviewed, and improved

RESPOND

- ☐ Establish an incident response plan for all possible cyber incidents
- ☐ Incident response plans are initiated and executed during or after a cyber incident
- ☐ Personnel know their roles and responsibilities throughout incident response plans
- ☐ Communications are sent to all stakeholders regarding the incident and response plan activities
- ☐ Incidents are reported according to guidelines or policy
- ☐ Incidents are contained and any residual risks or incidents are discovered and mitigated
- ☐ Investigations and forensics are performed
- ☐ Response plans are adjusted and improved based on impact of cyber incident

RECOVER

- ☐ Establish a recovery plan
- ☐ Engage with public relations team to manage reputational and public impact
- ☐ Communicate to all parties involved or affected: internal and external stakeholders, supply chain, victims, customers, general public

Get started and implement the NIST Framework

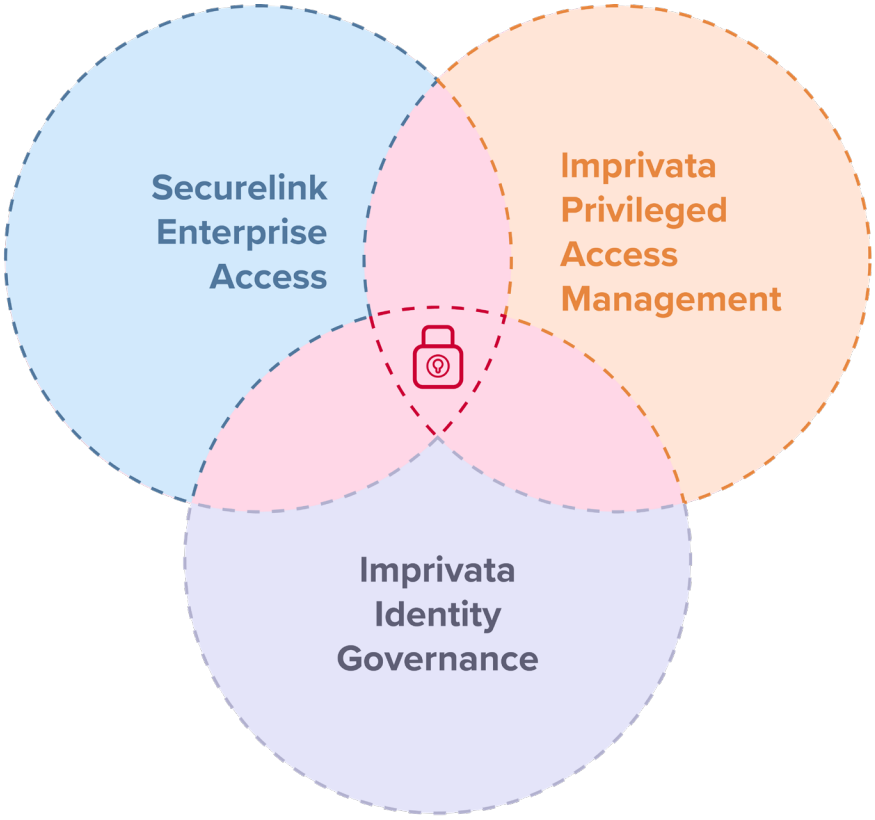
The goal of the NIST Cybersecurity Framework is to give businesses a set of best practices to build their own cybersecurity program, reduce risk, and improve communication between internal and external stakeholders when it comes to cybersecurity risk. It ensures cybersecurity risk is understood among all users and at all points in a supply chain and provides approachable and achievable methods of security to identify vulnerabilities and prevent threats.

The NIST Framework isn't a one-size-fits-all solution. Each organization is unique in its infrastructure, assets, access points, users, and cybersecurity budget. But no matter the size of the company or the budget, what matters most is that companies are proactive. The greatest downfall of an organization is staying stagnant and not proactively addressing security threats. The next steps are clear: compare your security structure to the NIST Framework and fill the gaps in your cybersecurity program.

Imprivata solutions to the NIST Cybersecurity Framework

You can start building out your NIST-approved cybersecurity program by implementing these streamlined solutions:

Secure vendor remote access and address third-party threats with Securelink Enterprise Access



Protect privileged accounts and credentials from unauthorized access with Imprivata Privileged Access Management

Accelerate secure role-based and least privileged access to systems and applications for all employees with Imprivata Identity Governance.

Working together, these privileged access management solutions help you meet the recommendations in the NIST Cybersecurity Framework and secure your most critical assets against attack.

LEARN MORE ABOUT IMPRIVATA'S ACCESS SECURITY SUITE ›

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow,security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform ofinteroperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage andsecure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

PAM-WP-GuidetoNISTCybersecurityFramework-0123